ETAS



Cybersecurity Solutions

Empowering Tomorrow's Automotive Software
www.etas.com

Intrusion detection for vehicles **ESCRYPT CycurIDS**



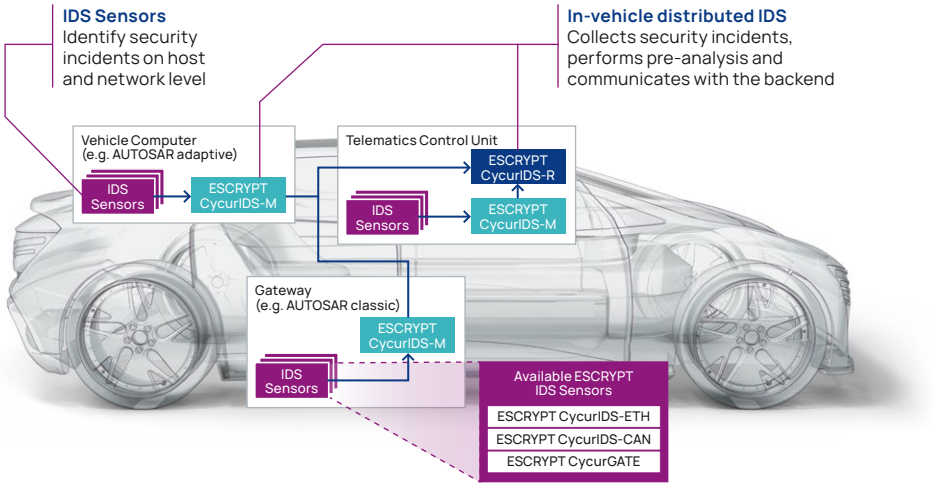
Continuous security monitoring with ESCRYPT intrusion detection solutions

With the increasing connectivity of vehicles, new vectors for cyberattacks are emerging and attackers are constantly perfecting their methods. This erosion of security concerns all building blocks of a connected vehicle fleet: the vehicles themselves as well as the corresponding vehicle backend services.

Ever since the recent enactment of UN R155, cybersecurity monitoring has become a top priority in the automotive industry. OEMs and fleet operators are required to provide effective security risk management for vehicles throughout their entire life cycle.

One of the key elements for achieving this is attack detection via intrusion detection systems (IDS) in the vehicle. But how does a viable IDS solution for the vehicle look like – given the challenges of a distributed E/E architecture with heterogeneous systems and communication protocols, the high performance requirements and the large limits on available computing resources and storage?

ETAS is offering a solution that is tailor-made for current and future vehicles with its ESCRYPT IDS senors CycurIDS-CAN for CAN/CAN-FD networks, CycurIDS-ETH for Ethernet networks, and host-based IDS tailored to automotive ECUs. The IDS manager ESCRYPT CycurIDS-M and the IDS reporter ESCRYPT CycurIDS-R complete the offer.



Distributed vehicle IDS architecture

- CycurIDS-CAN, CycurIDS-ETH and CycurGATE act as smart sensors aggregating and pre-selecting potential security events (SEV) to enable a fast and correct analysis
- Host-based IDS for risk-based monitoring of ECUs
- CycurIDS-M collects, analyses, aggregates, persists, and reports raised security events to the CycurIDS-R
- CycurIDS-R reports the security events from the vehicle to the VSOC

Components of the in-vehicle intrusion detection solution

ETAS offers a modular system of in-vehicle IDS products. The network IDS products ESCRYPT CycurIDS-CAN and ESCRYPT CycurIDS-ETH
- are fully interoperable with the IDS manager concept and can be incorporated as a "smart sensor" to detect intrusions on CAN and Ethernet
- offer graphical user interface based configuration tools providing automatic rule generation and simulation
- support reporting and logging of anomalies, either locally or to the Vehicle Security Operations Center (VSOC)

ESCRYPT CycurIDS-CAN
- Monitors forwarded CAN traffic and detects potential attacks (anomalies)
- Provides heuristic and signature-based detection on ECU

Exemplary detection features
- Allows to observe message frequency to detect message injection
- Makes it possible to compare all messages on the busses with a whitelist to detect unspecified messages
- Allows to detect malicious diagnostic requests while driving, e.g. detect attempts to shutdown certain ECU

ESCRYPT CycurIDS-M
- Acts as security event management for automotive ECUs
- Comes in two product variants:
  - for deeply embedded ECUs
  - for high performance ECUs
- Is an AUTOSAR compliant solution that is designed to be flexibly extended to cover any customer aggregation, persistence or reporting strategy
- Allows selection of relevant security events as early as possible to reduce storage and bandwidth cost
- Ensures an easy vehicle-wide configuration that can be adapted according to generated security events

ESCRYPT CycurIDS-ETH
- Monitors Ethernet traffic and detects potential attacks (anomalies)
- Enables in-vehicle intrusion detection for current and future Ethernet based E/E architectures
- Can run entirely on Ethernet switch as well as µC/µP

Exemplary detection features
- Covers specification, anomaly and signature based intrusion detection
- Allows to detect malicious attacks on application layer protocols like SOME/IP and DoIP, etc.
- Makes it possible to detect pattern of anomalies based on message frequency, sequence and vehicle state, etc.

ESCRYPT CycurIDS-R
- Acts as security event reporting for the vehicle
- Is a customized solution connecting the vehicle to the VSOC
- Ensures encapsulated provison of the IDS communication functionality
- Allows isolated deployments to fulfill security requirements
- Integrates seamlessly with the ESCRYPT CycurIDS components

Your benefits with ESCRYPT CycurIDS

- Timely detection of attacks in the field
- Field-proven ready-to-use solution
- Holistic offering that covers IDS sensors, security event management and reporting for in-vehicle intrusion detection
- In-vehicle IDS components are part of the ESCRYPT Intrusion Detection and Prevention Solution (IDPS), that includes also a VSOC as a managed security service
- Components are compliant to AUTOSAR, fulfill current automotive quality requirements, and are optimized for resource constrained ECUs
- A white-box, transparent security approach that enables you to realize and control your own cybersecurity policy
- Compliance to upcoming legal requirements, e.g. UN R155

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/CycurIDS

ETAS/COM2_AS/12/2022

Empowering Tomorrow's Automotive Software
www.etas.com

High-performance Automotive Ethernet/IP firewall and router **ESCRYPT CycurGATE**



Overview

With the automotive industry evolving to automated driving while getting more connected, cybersecurity threats can only be faced effectively with a holistic security approach.

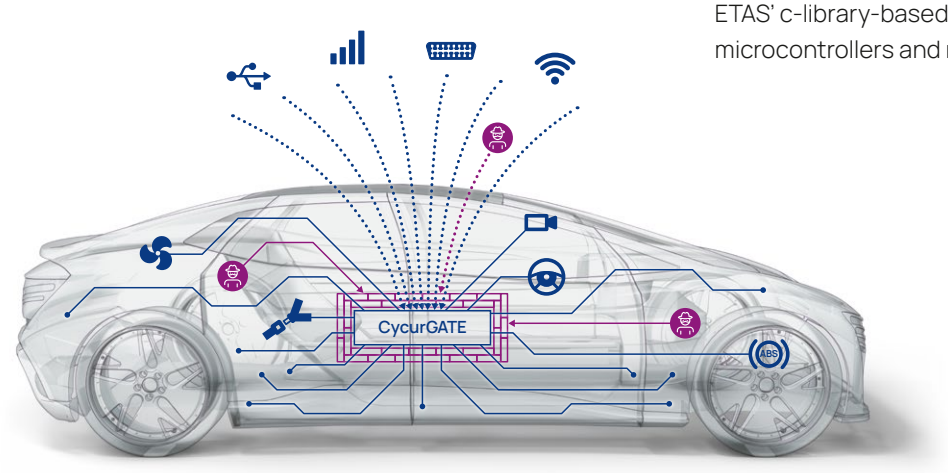
The automotive Ethernet firewall ESCRYPT CycurGATE is a market proven solution and indispensable to meet the increased security requirements of current and future gateways.

Perfectly balanced hardware-software co-design

The firewall is integrated directly into the Ethernet switch, where the entire packet flow is monitored and managed centrally – with no resulting interference with the host controller or individual ECUs. It can be used on the switch either as a library or as a stand-alone solution.

Thanks to balanced hardware-software co-design, the firewall solution makes the most of the hardware acceleration on the switch. The switch hardware and software are algorithmically so interwoven that the firewall can process the vast majority of data packets at wire speed.

ETAS' c-library-based firewall solution is tailored to run on microcontrollers and microprocessors.



Purpose of ESCRYPT CycurGATE

- Firewall to protect against a wide landscape of cyber attacks
  - Denial of service
  - Blocks illegitimate communication to individual ECUs or the entire network
  - Secure external interfaces
- Routing of data: effective control of data flow between network segments/domain

System solution

Security strategy for the entire vehicle life cycle

- Intrusion detection and protection calls for continuously effective, comprehensive security mechanisms.
- The ESCRYPT CycurIDS intrusion detection system monitors network traffic to detect and log anomalies and typical attack signatures. In addition, ETAS also offers a cyber-defense center backend: ESCRYPT CycurGUARD. This evaluates notifications from IDS components, detects new attack trends, helps determine the causes of security incidents, and defines countermeasures for distribution throughout the vehicle fleet.

Features

- Highly configurable and updatable
  - OTA-Update (over-the-air-update) ready: future-proof solution that can adapt to changing threat landscape
- Supports logging and statistics of suspicious data
- Provides all important filter mechanisms
  - Stateless-Packet-Inspection
  - Dynamic-Stateful-Inspection
  - Deep-Packet-Inspection
  - Black- and Whitelisting of messages
- Routing and firewall functionality
  - Also compatible with ETAS' Ethernet IDS features

Your benefits with ESCRYPT CycurGATE

- **Cost-effective, no additional hardware needed – easy integration**
  - Runs directly on the CPU of the switch, no resource consumption on host microcontroller
  - Software only version also available and can be integrated to any uC/uP
  - No changes needed to your current hardware/ software
- **Transparent**
  - Easy to configure according to your security standards
  - No black box security
- **Continually advancing and future proof**
  - More than three releases per year
- **Highest quality standards**
  - Developed according to the high ETAS quality standards

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/CycurGATE

ETAS/COM2_AS/12/2022

Empowering Tomorrow's Automotive Software
www.etas.com

ESCRYPT Vehicle Security Operations Center (VSOC)



Secure connected vehicle fleets

Increasing connectivity and automation of vehicles in combination with new regulations and standards like UNECE WP.29 and ISO/SAE 21434 requires OEMs and suppliers to monitor incidents and risks of their vehicle fleets over the entire life cycle. The threat landscape for connected vehicles is constantly evolving. Consequently, the security level of vehicles degrades over time as security measurements become ineffective and attackers learn to circumvent them.

This erosion of the security level concerns all building blocks of a connected vehicle fleet: the vehicles themselves as well as the corresponding vehicle backend services. Detailed knowledge on the security status and potential attacks is paramount. Two activities establish this knowledge and keep it up to date: threat detection and threat intelligence.

Threat detection

Timely detection and competent analysis of ongoing attacks to establish the appropriate measurements to maintain the security level.

Threat intelligence

Acquisition and collection of knowledge on known practicable attack patterns that may harm the security level of the connected vehicle.

ETAS develops and operates the ESCRYPT Vehicle Security Operations Center (VSOC) for connected fleets that enables manufacturers and fleet operators to establish a life cycle of continuous security improvements. This managed security service ensures permanent monitoring to identify rising security threats, establishes dedicated incident response, and keeps the security level stable over the entire life cycle.

We offer exactly the service you need to respond to the continuously evolving threat landscape for connected vehicles and to fulfill upcoming worldwide regulations, such as UNECE WP.29 and ISO/SAE 21434. With ETAS you have a competent partner at your side covering in-vehicle intrusion detection (IDS) and vehicle backend expertise with dedicated SOC services.

Our managed security service in detail

Open architecture approach

The ESCRYPT VSOC follows an open architecture approach and integrates all sensors in the vehicle that provide information relevant for cybersecurity monitoring. This includes: network-based intrusion detection for the CAN bus with ESCRYPT CycurIDS-CAN, automotive Ethernet firewalls and IDS with ESCRYPT CycurGATE and ESCRYPT CycurIDS-ETH, host-based intrusion detection for Linux, QNX, and Android ECUs and support for the complex distributed IDS architectures of modern E/E architectures.

SOC services

ETAS cooperates with leading IT security service providers on the commissioning, infrastructure, and services of a security operations center (SOC). In this way, it pools the skills and expertise for SOC-as-a-Service with its own specialist automotive know-how and portfolio. We have taken the existing SOC infrastructure and expanded it with trained automotive security analysts and specialized forensics experts, turning it into a highly professional, market-ready, and holistic solution.

Threat detection and response

ETAS' monitoring backend product ESCRYPT CycurGUARD collects and analyzes anomaly reports of vehicles in operation by interlocking of automated and manual analysis. Automatic classification of events and automated processing of known attack patterns are combined with the manual alert validation of automotive security forensic experts to identify emerging threats. This achieves event-based threat hunting, incident support and proactive response with network threat containment.

Your benefits with ESCRYPT VSOC

- Advanced security analytics by automotive forensic experts and security analysts
- Many years' operational experience from the SOC provider's IT security experts joined with ETAS' extensive expertise in vehicle cybersecurity
- Availability of as-a-service solution including operation, monitoring, and response
- Continuous monitoring of attacks in the field through market-ready and mature components that have been combined in collaboration with the SOC provider to form a complete and integrated solution
- Worldwide coverage and 24/7 availability
- Integration of and openness to all types of in-vehicle intrusion detection systems (IDS)

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/VSOC

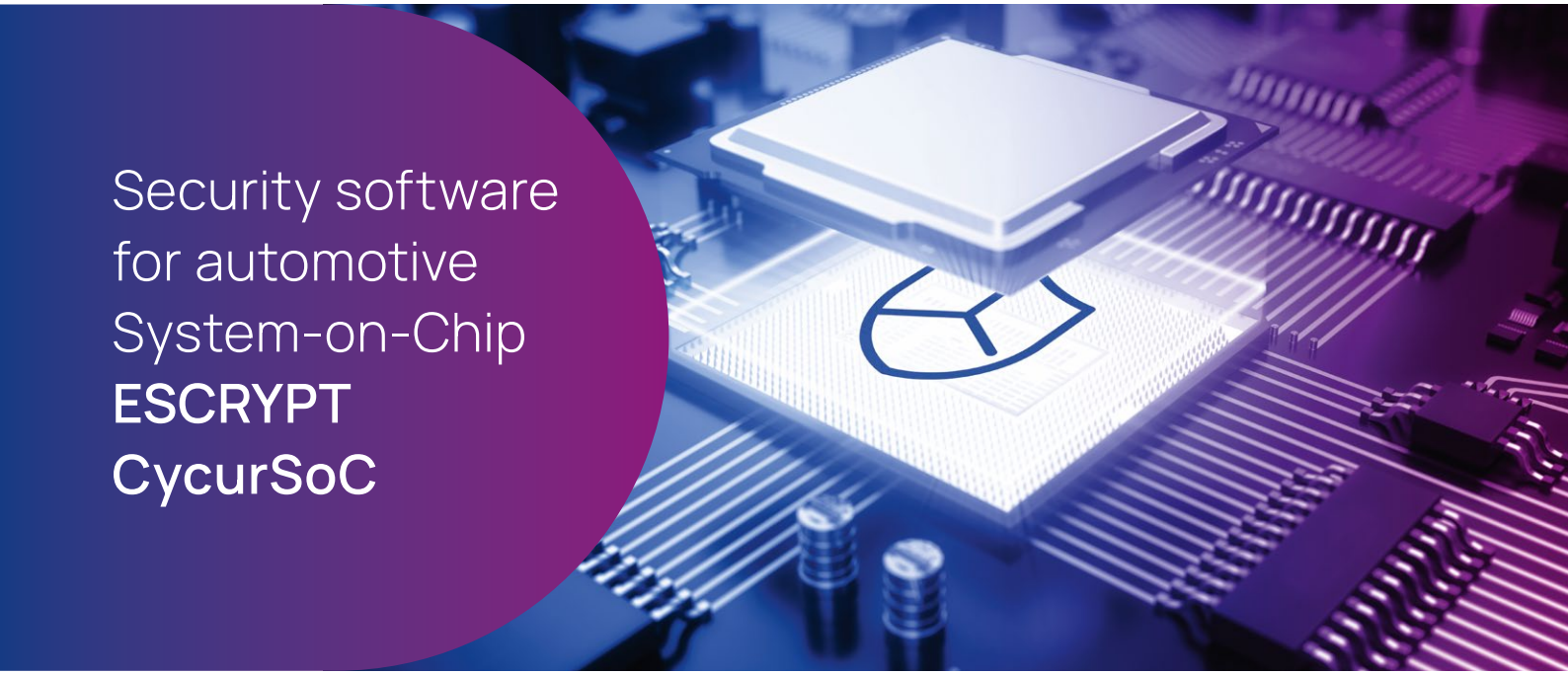
ETAS/COM2_AS/01/2023



Security Solutions : Crypto libraries & HSM stack

© 2023 ETAS K.K.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Empowering Tomorrow's Automotive Software
www.etas.com

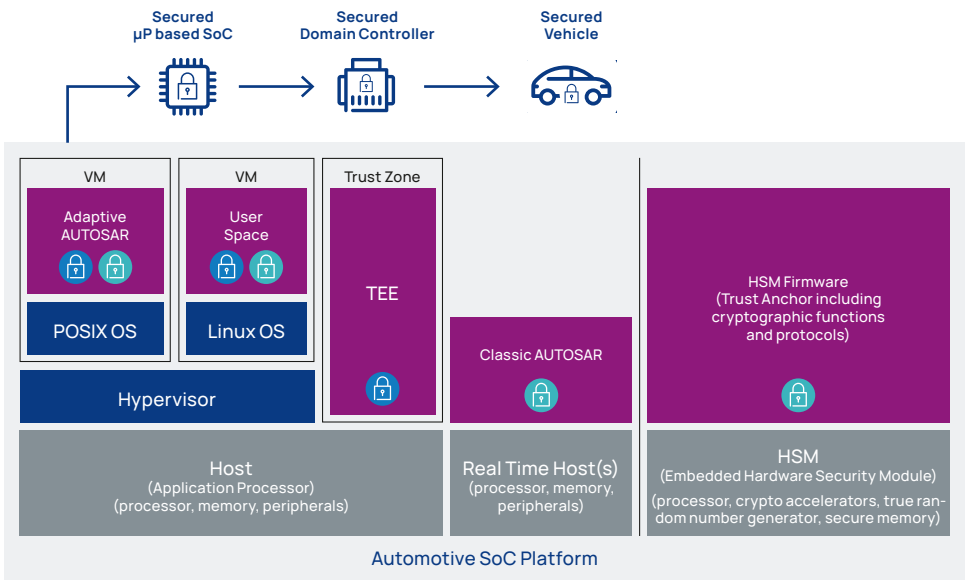


Security software for automotive System-on-Chip **ESCRYPT CycurSoC**

Enabling safety and trust for software-defined vehicles

Electrification, autonomous driving, Advanced Driver-Assistance Systems (ADAS) and infotainment systems are driving the emergence of powerful on-vehicle computing platforms. The key central component of each of these platforms is a microprocessor-based system-on-chip (SoC). These SoC platforms are enabling the vehicle E/E architecture evolution from traditional distributed ECUs to a more centralized domain architecture. Advanced E/E architectures host powerful software functionality that enhances customers' experience and increases automation. These benefits are, however, accompanied by newly-introduced cybersecurity vulnerabilities and threats.

ESCRYPT CycurSoC is an embedded cybersecurity software solution for contemporary and future SoC-based automotive ECUs. Designed for automotive security use cases, it provides a complete set of security building blocks for heterogenous SoC architectures utilizing an HSM core and any other SoC CPU cores. The security solution is optimized for efficiency with minimal impact on available system resources. While supporting open and standardized interfaces (e.g., SHE+, AUTOSAR Classic and Adaptive), it is flexible and integrable with different embedded technology solutions, including virtual machines and various host environments.



HSM & TEE variants

- **ESCRYPT CycurSoC-HSM** is an HSM core firmware variant of the microprocessor (µP) based SoC platform.
- **ESCRYPT CycurSoC-TEE** is a Trusted Execution Environment (TEE) software variant of the µP based SoC platform that may not have an HSM core.
- Both variants can be offered separately, or they can complement each other, depending on the platform and security use cases.
- Both variants are designed to act as root of trust, and utilize SoC resources efficiently to maintain security integrity, robustness and zero trust concept.

ESCRYPT CycurSoC-HSM Security Components

ESCRYPT CycurSoC-TEE Security Components

ESCRYPT CycurSoC – The de-facto standard for µP-based SoC

- Implements security functionality that is critical to the creation of a security enclave on the HSM core or TEE host
- Offers cryptographic protocols and algorithms to the application
- Helps to effectively fulfill complex automotive OEM security requirements, while ensuring a smooth integration into the overall system architecture
- Retains integrity of data and functionality to achieve reliability , safety and data protection
- Is abstracted from the requirements of an OEM and the underlying silicon, thus enabling sourcing one security solution that fits all and saves on cost

Cryptographic features

- CMAC and HMAC
- Hashing
- Key derivation
- TRNG and PRNG
- Digital signature algorithms; ECDSA, EdDSA, RSA
- Symmetric and asymmetric encryption
- Authenticated encryption and decryption
- SHE+ support
- Key exchange algorithms; ECDH, ECDHE, ECBD
- Key wrapping and transport
- Key encapsulation mechanism (KEM)
- Key storage management and trust management
- Certificate handling
  - Parsing
  - Signing request
  - Revocation and CRL handling
  - Chain verification

HSM & host core

- Secure storage of data and keys in external flash
- Secure access
- Establish trusted channel amongst different cores on the SoC
- Support for E/E architectures with large number of keys
- Support for multi-CPU tenancy
- Support for virtualized environment
- Responsive operations in multi-CPU use cases
- HSM lifecycle mode
- Support for secure boot, trusted boot, authenticated boot and other boot modes
- Trust anchor based on signatures
- Runtime manipulation detection

Trust zone

- Integration with TEE operating systems
- Establish trusted channel between trust zone and other cores on the SoC
- Automotive grade security functionality, supporting trusted applications (TA) and the non-secure world

Your benefits with ESCRYPT CycurSoC

- **User friendly**
  Can be seamlessly integrated in automotive ECUs
- **Fast**
  Allows to be easily integrated with POSIX and real time operating systems
- **Comprehensive**
  Encapsulates all required security functions needed to satisfy all OEM automotive security requirements
- **Quality and reliability**
  Is being developed to high quality standards (ASPICE, ISO-21434 CSMS, ISO-26262 ASIL B)
- **Secure**
  Offers a powerful hardware/software co-design platform for customer-specific applications with high-performance cryptographic demands
- **Flexible**
  Can be configured to meet automotive customers' specific needs

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/CycurSoC

ETAS/COM2_AS/12/2022

Empowering Tomorrow's Automotive Software
www.etas.com



Automotive-qualified Security Stack for HSMs **ESCRYPT CycurHSM**

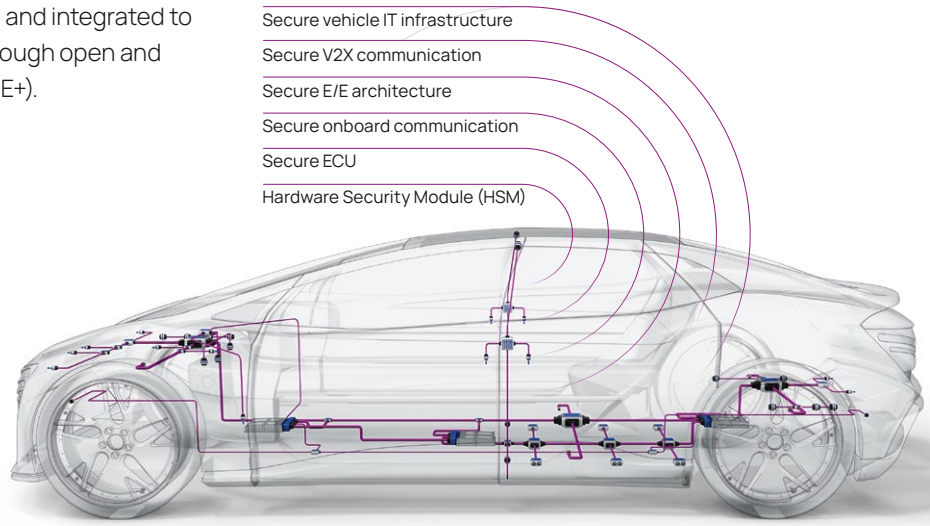
Overview

For security at ECU level, pure security solutions alone in software cannot sufficiently protect the integrity of a secure system. Hardware Security Modules (HSM) are a necessary prerequisite to harden embedded systems against attacks, to ensure confidentiality of data and provide protection to maintain the integrity and authenticity of the system.

ESCRYPT CycurHSM is a complete security software stack used in applications for HSM-embedded automotive microcontrollers. It is adapted to support a wide range of available automotive HSM implementations by different silicon manufacturers. ESCRYPT CycurHSM is a modular and flexible HSM firmware which can be easily customized and integrated to HSM-enhanced security applications through open and standardized interfaces (e.g. Autosar, SHE+).

ESCRYPT CycurHSM has been implemented in hundreds of successful projects with TIER-1s and OEMs worldwide, further underscored by a proven record in the field in millions of vehicles. ESCRYPT CycurHSM is a highly optimized HSM firmware implementation that ensures the highest level of ECU security.

ESCRYPT CycurHSM is accredited with the world's first ISO standard certificate for road vehicle cybersecurity "ISO/SAE 21434:2021 Road vehicles – Cybersecurity engineering" with the highest security level CAL4 (Cybersecurity Assurance Level 4).



Supported features

ETAS offers ESCRYPT CycurHSM with a comprehensive feature set:

Cryptographic and certificate features

- Asymmetric crypto algorithms:
  - RSA
  - ECDSA, ECBD, ECDH, ECDHE, EdDSA
- Basic cryptographic services
  - Symmetric ciphers (e.g AES)
  - MAC generation and verification (e.g. CMAC, HMAC)
  - Random number generation (e.g. TRNG, PRNG)
  - Hashing
  - Key derivation functions
- Certificate support (authenticity, parsing)
- Chinese algorithms
- Key exchange protocols (Diffie-Hellman)

Field return analysis and HSM debugging

- Fail-Safe HSM Update
- HSM-controlled Secure Access (Challenge Response Protocol)
- HSM Debug
- HSM Dump
- Secure Host Flashing
- Secure Logging

HSM core functionality and generic features

- Bank swap SOTA support
- Component protection (SHE+ support)
- EEPROM emulation to extend flash endurance
- HSM Lifecycle Mode
- HSM RAM mode
- Memory Unlock (flash password protection)
- Multi-core support
- Runtime manipulation detection
- Secure Boot / Trusted Boot / Authenticated Boot and other boot modes
- Secure storage of data and keys
- Support for systems with large number of keys (> 100)
- Trust Anchor based on signatures
- Preemptive, parallel job processing

OEM specific features

- Qualified OEM specific configurations including support for OEM specific protocols and functions

And many more!

Interested to know more or have a specific use-case? Please contact us.

ESCRYPT CycurHSM is a highly optimized and flexible security firmware that can be configured for your individual use case.

Your benefits with ESCRYPT CycurHSM

- **User friendly**
  Can be seamlessly integrated in non-AUTOSAR and AUTOSAR automotive applications
- **Fast**
  Based on a real-time operating system to ensure real-time HSM features
- **Trustworthy**
  Contains no open-source software in productive code
- **Comprehensive**
  Encapsulates all required security functions needed to satisfy OEM automotive security requirements
- **Future-oriented**
  Satisfies next-gen requirements and new cybersecurity regulations (ISO21434..)
- **Top quality**
  Has been developed to the highest quality standards (ASPICE, ISO 26262 ASIL D) and can be used in safety-criticial applications
- **Secure**
  Offers a powerful hardware/software co-design platform for customer-specific applications with high-performance cryptographic demands
- **Flexible**
  Can be configured to meet your specific needs and is free of hidden costs

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/CycurHSM

ETAS/COM2_AS/12/2022

Empowering Tomorrow's Automotive Software
www.etas.com

Cryptographic library for embedded systems **ESCRYPT CycurLIB**



Overview

Cryptographic protocols and algorithms provide the fundamental basis for most IT security applications and embedded security solutions. Typical applications include secure software updates, secure boot, encrypted/authenticated communication, and feature activation.

ESCRYPT CycurLIB is a cryptographic libraray that provides efficient implementations of cryptographic algorithms and security standards.

Additionally, it was designed especially for embedded systems where resources such as computational power and memory are particularly limited.

ESCRYPT CycurLIB has no dependencies on specific microcontrollers, operating systems or external libraries. This enables the use on any microcontroller with sufficient RAM/ROM.

ESCRYPT CycurLIB provides a comprehensive set of cryptographic algorithms including post-quantum algorithms together with supporting NIST and Chinese standards.

This enables its' use in many diverse and high-volume applications, especially the automotive industry.

This cryptographic library is geared for new cybersecurity regulations for which the security engineering process has been certified to be compliant to ISO/SAE21434-Road vehicles-Cybersecurity engineering

ESCRYPT CycurLIB is modular and easily integrable and is optimized for code-size while satisfying stringent performance-constraints. It can easily be used to make products secure, e. g., by verifying signatures to determine the authenticity and integrity of data and is highly configurable with an AUTOSAR compliant configuration tool).

Post-quantum algorithms supported

Proven and certified quality

Quality is deeply rooted in the business principles at ETAS and is a fundamental part of every product development. We are committed to offer customers only top-quality products and the quality of our cryptographic library has been proven in multiple ways.

ASPICE

The "Automotive Software Process Improvement and Capability dEtermination" (ASPICE) assessment rating is a widely adapted standard. Major OEMs use it to assess their electronic and software supplier's process quality and capability.

- ESCRYPT CycurLIB is developed by ASPICE compliant processes, capability level 2.

ASIL D

The automotive risk classification ASIL D is part of the larger ISO standard for functional safety ISO 26262 and represents the highest level of risk management. Components designed for ASIL D meet the most stringent safety requirements.

- The development of the cryptographic library follows ISO 26262 compliant processes, up to ASIL D.
- ESCRYPT CycurLIB can be implemented in safety-critical applications.

FIPS and CAVP

The "Federal Information Processing Standard" (FIPS) 140-2 by the National Institute of Standards and Technology (NIST) specifies the security requirements that will be satisfied by a cryptographic module.

The NIST "Cryptographic Algorithm Validation Program" (CAVP) provides validation testing of cryptographic algorithms and their individual components.

- FIPS-certified variant available
- CAVP validation will be available soon

Testing

ESCRYPT CycurLIB is continuously and rigorously tested with about 15.000 unit, integration and qualification tests performed with a passing rate of 100%. The cryptographic librarys' high-quality has further been underscored by its' proven record in the field, in millions of vehicles and applications worldwide.

Comparison freeware vs. ESCRYPT CycurLIB

Freeware cryptographic library	Our cryptographic library
? May be well tested	✓ Rigorously tested
? May be licensed under GPL	✓ No open-source included (GPL-free)
× No product support	✓ Long-term product support and maintenance
× No customer incident handling and support	✓ Customer incident handling and support
× Not qualified for automotive systems and microcontrollers	✓ Qualified for automotive systems and microcontrollers
× Does usually not cover safety use-cases	✓ Qualified for safety critical applications

Available cryptographic algorithms

Category	Algorithms
Symmetric Block Ciphers	AES SM4
Modes of Operation	CBC CCM CTR GCM
Authenticated Encryption	ChaCha20-Poly1305
Symmetric Stream Ciphers	ChaCha20
Digital Signatures	RSASSA-PSS RSASSA-PKCS1-v1_5 ECDSA EdDSA SM2 Digital Signature
Post Quantum Algorithms	CRYSTALS-KYBER CRYSTALS-DILITHIUM
Asymmetric Encryption	SM2 Encryption ECIES ECIES DHAES RSA-OAEP
Hash Functions	SHA-2 SHA-3 SM3
Message Authentication Codes (MACs)	CMAC HMAC Poly1305 SipHash24
Diffie-Hellman Key Exchange	Curve25519 ECDH FFC DH
MQV Key Exchange	SM2 Key Exchange
Key Derivation Functions	KDF2 / ANSI X9.63 KDF Hash-based KDF according to NIST SP800-56C HKDF according to RFC5869 KDF in CTR mode with AES-CMAC according to NIST SP800-108
Key Wrap	NIST AES Key Wrapping
Pseudo-Random Number Generators	HMAC_DRBG Hash_DRBG
Certificates	X.509 parsing and chain validation OCSP response parsing and validation
Password-Authenticated Key Exchange	SPAKE2+

Details

General

- Implemented according to MISRA-C:2012, ANSI-C standard and Cert-C
- HIS Source Code Metrics compliant components
- No external library required, in particular no OSS is included
- No dynamic memory allocation
- Optimized for code size while satisfying stringent performance constraints
- Modular structure to directly adapt the software
- GUI supported configuration
- ASPICE (level 2) compliant development processes
- ISO 26262 compliant development processes, up to ASIL D
- AUTOSAR compliance
  - AUTOSAR compliant configuration tool
  - AUTOSAR compliant memory mapping
- FIPS certified variant available
- Well-documented
- Intuitive API
- Easy to integrate in your product
- No dependencies on specific microcontrollers

Supported platforms

- Any platform providing an ANSI-C conform compiler – from 8 bit to 64 bit

Outlook

- Components: AUTOSAR CryptoDriver
- Post-quantum algorithms optimization
- EdDSA extension

Your benefits with ESCRYPT CycurLIB

- Seamless integration in existing products
- Supports all common cryptographic algorithms and certificate standards
- Implemented to account for highest quality standards
- Low footprint
- Modularity
- Runs on all platforms
- High level of customer support
- **Continuous enhancement and adaptation:** Extensions/Modifications – enhancement based on market trends and customer requirements
- **Customization:** Please contact us for questions regarding extensions and modifications.



Security Development Tools

© 2023 ETAS K.K.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Empowering Tomorrow's Automotive Software
www.etas.com

Software tool for Threat Analysis & Risk Assessment **ESCRYPT CycurRISK**



Uncover the vulnerable points of your automotive systems

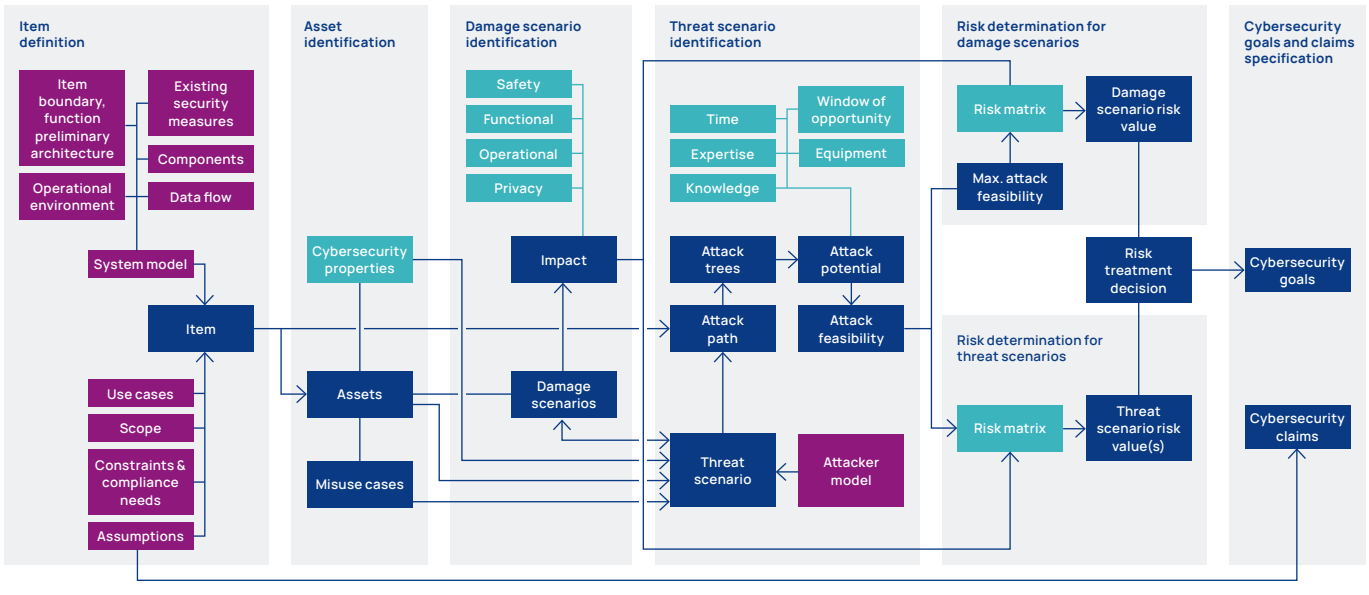
UN R 155 and other international regulations have made a risk-based approach to vehicle architecture development a prerequisite for type approval. In addition, ISO/SAE 21434 sets the framework for the implementation of these guidelines. Threat Analysis and Risk Assessment (TARA) has thus become an indispensable part of automotive system design and development processes.

ESCRYPT CycurRISK is a TARA software tool that helps you uncover and evaluate potential attack surfaces in automotive systems and architectures at an early stage.

ESCRYPT CycurRISK allows you to systematically identify and analyze threats via attack feasibility (based on attack potential) using attack trees. Damage scenarios are used to assess the impact on road users and your business. The tool provides a structured documentation of threat scenarios and risks to a given system.

Thus, this TARA software tool enables you to prioritize risks and countermeasures and to create a security concept that complies with the requirements of security engineering processes, ISO/SAE 21434, and UN R 155.

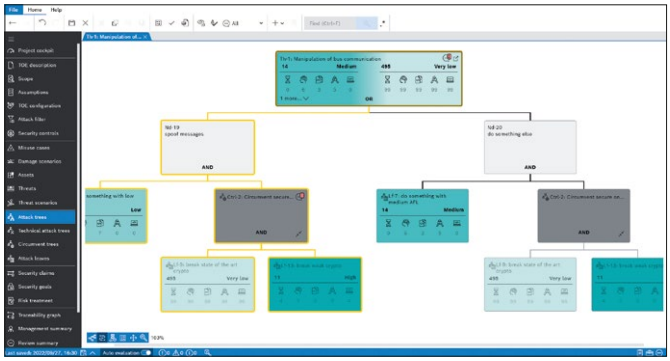
Threat Analysis & Risk Assessment methodology



Features

Creating TARAs efficiently

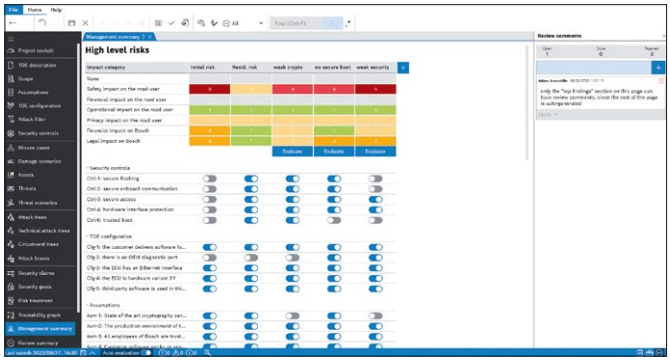
- Workflow-oriented guidance
- User-friendly GUI
- Direct comparison of initial and residual risks
- Automatic management summary
- Integrated attack tree editor
- Support of attack potential method with automatic attack potential computation
- Dedicated mode for reusing TARA
- Sophisticated functionality for variant handling and configuration



Creating attack trees via drag-and-drop in a user-friendly attack tree editor

Working together

- Configurable PDF report generation
- Catalog function for reuse and knowledge sharing
- Collaboration on TARAs on on-premises servers
- Review functionality



Comparing variants of item configuration and security controls to decide on an economical risk treatment

Your benefits with ESCRYPT CycurRISK

- Established tool widely used in the automotive industry
- Professional maintenance and support
- Updates and improvements based on our long-standing experience in automotive security
- Fully compliant with ISO/SAE 21434
- Backed by ETAS security consulting experience and services
- On-premises server hosting
- Fully configurable report templates
- Tool classification according to ISO 26262 available and tool qualification for all use cases for tool confidence level (TCL) 2/3 performed
- Mapping to ISO/SAE 21434 tool requirements available

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/CycurRISK

ETAS/COM2_AS/12/2022

Empowering Tomorrow's Automotive Software
www.etas.com

Smart fuzz testing for automotive systems **ESCRYPT CycurFUZZ**



Ensure compliance with UN R-155 and ISO/SAE 21434

Increasing complexity coupled with international regulations like UN R-155 and ISO/SAE 21434 make cybersecurity testing mandatory for the development and validation of automotive systems. Fuzzing is one of the test methods explicitly recommended in ISO/SAE 21434 for validating the robustness and cyberresilience of automotive systems and identifying weaknesses at an early stage. A smart automotive fuzz testing tool allows you to customize, automate, and accelerate the test procedure, while constantly improving and embedding it efficiently into your development process.

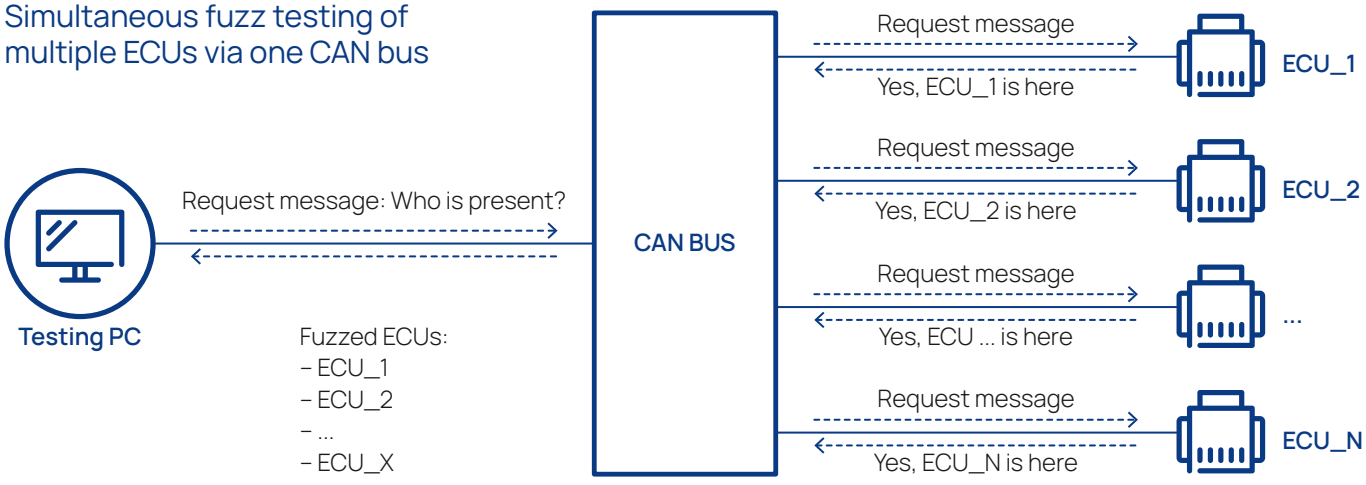
Improve the quality of your automotive software

ESCRYPT CycurFUZZ is a state-of-the-art fuzz testing tool that helps you meet current regulations and standards. With built-in automotive cybersecurity testing knowledge, ESCRYPT CycurFUZZ enables you to assess the security maturity of your automotive systems and to improve the software quality of your products throughout the development and validation process.

Unique defect detection rate and execution speed

ESCRYPT CycurFUZZ covers pre-dominant automotive protocols and takes customer specific demands, e.g., ARXML files, into consideration. Due to the dynamic timing feature, a particularly high test performance is achieved: ESCRYPT CycurFUZZ performs a unique defect detection rate at an execution speed much faster than other fuzz testing tools.

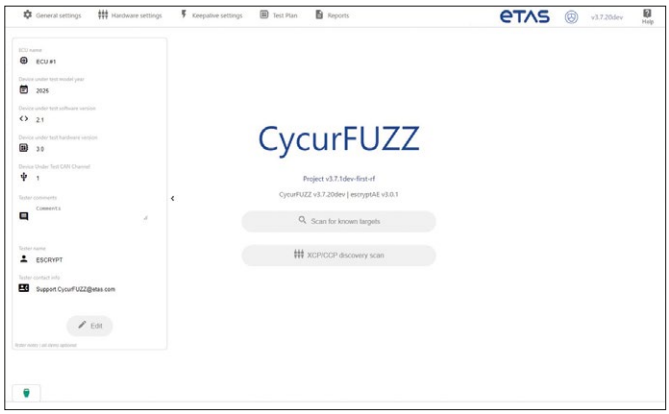
Simultaneous fuzz testing of multiple ECUs via one CAN bus



ESCRYPT CycurFUZZ at a glance

Setups & use cases

- System or integration tests to identify weaknesses/ vulnerabilities of a physical or virtual ECU
- Single virtual or physical ECU tests with easy setup (ECU, hardware connector, PC)
- The following test setups are possible:
  - SiL setup on component level in a single level 3 vECU
  - SiL Setup on system level with multiple ECUs on a PC (see front page)
  - HiL setup with integration of ESCRYPT CycurFUZZ to increase the speed of fuzz testing
- Professional fuzz testing services from ETAS: Fuzz testing, result reports, analysis and interpretation of findings and proposal for remediation.



Web-based GUI of ESCRYPT CycurFUZZ

Features & supported protocols

- Coverage of pre-dominant automotive protocols
  - CAN
  - CAN-FD
  - ISO-TP
  - J1939
  - UDS
  - DoIP (upcoming)
  - SOME/IP (upcoming)
- Support for various fuzzing modes: UDS, Inverse UDS, ISO-TP, ARXML, DBC, Random, and Monitor Mode
- Easy-to-use local PC and cloud-based version
- Vehicle-level fuzz testing: simultaneous fuzzing of multiple ECU targets via one CAN bus
- Full-headless mode: supports all common tools for bus access (DB9, USB connector), REST API for external integration

Your key benefits with ESCRYPT CycurFUZZ

- High-speed test execution, enabled by the dynamic timing feature of fuzzing messages
- Unique defect detection rate compared to competitor tools
- Built-in and continuously improved automotive security testing knowledge due to ESCRYPT professional security testing services
- Compliance to automotive cybersecurity regulations and standards, including ISO/SAE 21434 and UN R-155
- Straightforward local fuzz testing setups and considerably lower switching costs from competitor solutions
- Component-, system-, vehicle-level fuzzing
- Cross-platform support (Windows, Linux, Docker container)

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/CycurFUZZ

ETAS/COM2_AS/04/2023

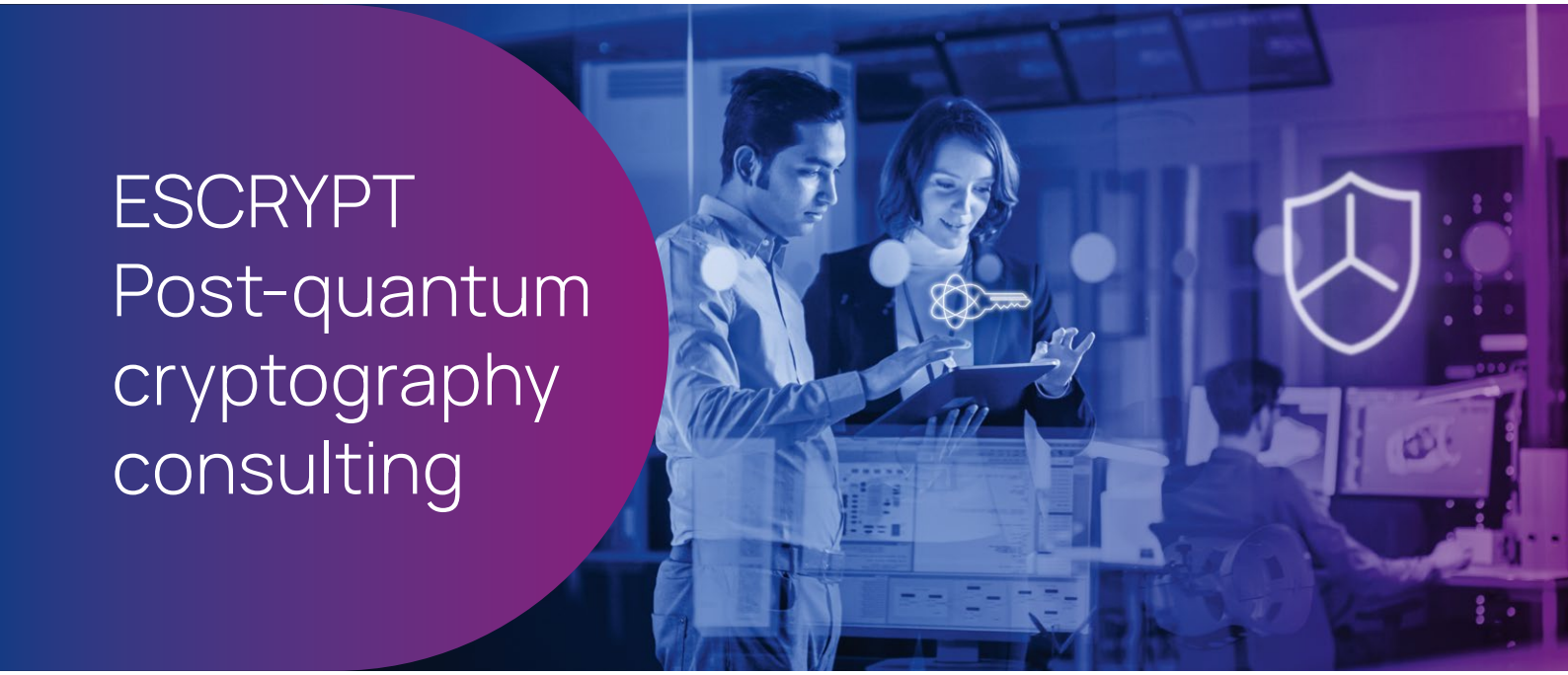


Professional Consulting Services

© 2023 ETAS K.K.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Empowering Tomorrow's Automotive Software
www.etas.com

ESCRYPT Post-quantum cryptography consulting



Are you post-quantum ready?

Asymmetric cryptography is now in widespread use, but algorithms that are secure today will be broken by the quantum computers of tomorrow. Although a breakthrough in quantum computing might be some years away, companies need to prepare for the smooth transition to quantum-secure systems in good time. Finding suitable post-quantum algorithms and migrating to quantum-secure systems can pose many challenges.

In addition to our proven expert knowledge in developing secure automotive architectures, ETAS has gained extensive experience in post-quantum cryptography (PQC) as a partner in FLOQI (full lifecycle post-quantum PKI) – a funded project that focuses on developing a post-quantum PKI for automotive use cases, among others.

The challenge

There have been huge advances in quantum computing in recent years and the first computer capable of breaking today's asymmetric cryptography may be here less than ten to fifteen years. Companies using asymmetric cryptography to secure products with long lifecycles need to start looking for secure alternatives now.

Impacts for automotive security

Most of todays and upcoming automotive security measures (e. g. ECU integrity protection, secure onboard communication, V2X, access control etc.) rely on classical cryptography that will be vulnerable to quantum computing.

OEMs in particular need to think about post-quantum cryptography solutions now if they want to avoid disruptions and comply with future standards and legislation applicable to automotive security (e. g., BSI, UN-R 155).

Our recommendations

- Be prepared for the post-quantum world early, before scalable quantum computers exist
- Develop crypto agility and migration solutions (e. g. hybrid PQC solutions), identify suitable algorithms for every use case
- Use existing PQC expertise & implementations, available with trainings, consultations, testing and products like ESCRYPT CycurLIB

ESCRYPT post-quantum cryptography consulting – service overview

Guidance for management

- We offer customer workshops that aim to raise awareness of the problems arising from the development of quantum computers.
- We give specific recommendations on points of action and prioritization, and help you establish a timeline.
- We perform an analysis of the state-of-the-art regarding standardization activities for post-quantum algorithms.

Specific technical quantum-safe solutions

- Our post-quantum cryptography experts analyze specific systems (e. g. function or function clusters) that use asymmetric cryptography in order to identify the changes necessary for migration to post-quantum solutions, taking specific requirements into consideration.
- We design migration and transition solutions, e. g. for the PKI or key management.

Integrating post-quantum solutions into E/E architectures

Our post-quantum cryptography experts analyze post-quantum algorithms with respect to

- Key and signature sizes
- Performance of signing and verifying algorithms
- Memory consumption
- Confidence in security of algorithms
- Use case requirements

We compare resources of deployed ECUs with available benchmarks in order to identify suitable algorithms for different targets/use cases and we offer an analysis of adjacent IT systems (e. g. PKI, backend) with respect to the changes required for post-quantum security.

Your benefits with ESCRYPT PQC consulting

- **Proven expert knowledge:** benefit from years of experience in PQC and automotive security.
- **Latest research insights:** as part of FLOQI, ETAS works together with the project partners on defining a quantum-secure PKI, taking into consideration the needs and specific requirements of the automotive industry.
- **State-of-the-art:** use existing PQC implementations for testing & benchmarking quantum-safe security for embedded & backend systems such as ESCRYPT CycurLIB.
- **Field-proven solutions:** we provide tested and proven solutions to make your systems quantum-secure.

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/pqc-sonsulting

ETAS/COM2_AS/12/2022

Empowering Tomorrow's Automotive Software
www.etas.com

ESCRYPT AUTOSAR security consulting service



The ESCRYPT AUTOSAR security consulting service provides expertise in securing the vehicle using existing AUTOSAR modules and supports customers in adding their own features to AUTOSAR.

AUTOSAR for holistic vehicle protection

On the way to connected, automated driving, the number of security relevant in-vehicle functions is increasing. This means it is becoming more important than ever to have more elaborate security measures and a high security level in place for vehicle platforms.

AUTOSAR has extended its security portfolio by more and more components and nowadays incorporates various security applications, making it the ideal technological answer to the increasing security requirements. ESCRYPTs AUTOSAR security consulting service provides expertise in securing vehicles using existing AUTOSAR modules and supports customers bringing their own features into AUTOSAR.

AUTOSAR as enabler for the UN-R 155

AUTOSAR enables an adequate solution for regulations like UN-R 155 and paves the way for implementing the new security requirements relevant to type approval.

Our expertise

ETAS is a member of the AUTOSAR consortium since many years and we have successfully completed numerous projects with various OEMs and Tier1s regarding AUTOSAR security consulting.

Available AUTOSAR security building blocks

AUTOSAR incorporates various security applications, for instance for securing invehicle communication and for protecting confidential data. However, due to their different architectures, AUTOSAR Classic and AUTOSAR Adaptive offer partly identical and partly different security applications.

- Crypto stack for access to cryptographic primitives and key management
- Secure communication via TLS, IPSec and SecOC
- Secure diagnostic access via the UDS services 0x27 (Secure Access) and 0x29 (Authentication)
- Access protection to critical resources via Identity & Access Management
- Detection and reporting of security events via IdsM
- Secure updates of individual applications or the whole platform parallel
- Authenticated software by continuing the chain of trust within Trusted Platform

	AUTOSAR Classic R20-11	AUTOSAR Adaptive R20-11
Crypto stack	✓	✓
Secure communication	✓	✓
Secure diagnostics	✓	✓
Identity and access management	×	✓
Intrusion detection	✓	✓
Secure updates	×	✓
Trusted platform	×	✓

ESCRYPT AUTOSAR security consulting – service overview

AUTOSAR security concepts

This consulting service supports you in the review of existing and the design of new security architectures using AUTOSAR security modules, e.g. the creation of security concepts for secure in-vehicle communication using SecOC/TLS/IPSec.

Our AUTOSAR experts support you in identifying the correct usage of existing AUTOSAR security modules and offer:

- Analysis of your use case, current environment and architectures
- Identification of corresponding AUTOSAR security modules (e.g. IdsM for distributed IDS)
- Support for correct usage of the AUTOSAR modules (e.g. AUTOSAR IDS sensors, IdsM filter chain configuration etc.)

Our AUTOSAR security consulting service encompasses design and requirements engineering of security modules according to your application that make use of the AUTOSAR interfaces, e.g. the design of a SecOC Freshness Manager including requirements engineering.

Strategic AUTOSAR consulting & consortional work

- AUTOSAR experts compare your requirements with the AUTOSAR specification and identify the missing aspects by performing a gap analysis
- We offer independent representation in the AUTOSAR consortium according to your individual strategy
- We perform strategic consulting towards new developments, especially with regards to currently ongoing specification activities within AUTOSAR

Your benefits

- **Field-proven industry standard:** AUTOSAR has been used in the industry for over a decade.
- **Not reinventing the wheel:** we provide expertise in securing the vehicle using existing AUTOSAR modules and we can support you in bringing your own features into AUTOSAR.
- **Prepare in time for the new regulations:** use AUTOSAR security building blocks to achieve adequate security.
- **Proven expert knowledge:** benefit from our years of experience in AUTOSAR, the AUTOSAR consortium and automotive security.

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/autosar-consulting

ETAS/COM2_AS/12/2022

Identify the vulnerabilities of your embedded system **ESCRYPT security testing services**



Understand how hackers work

Keeping data secure is one of the top priorities for companies today. Unfortunately, new vulnerabilities are discovered every day and it is nearly impossible to keep pace with all of them. That is why it is essential to test your embedded system with seasoned security experts. The professionals from ETAS will dig deep to uncover the security weaknesses that can cost you time, money and reputation. With several test methods they simulate the strategical and technical actions of a real world attacker with the goal of finding the security vulnerabilities and providing comprehensive assistance in how to fix them.

Available ESCRYPT testing methods

Code review

In some cases a code review is the only efficient way that several key security controls can be verified including access control, encryption, data protection, logging, back-end system communications and usage.

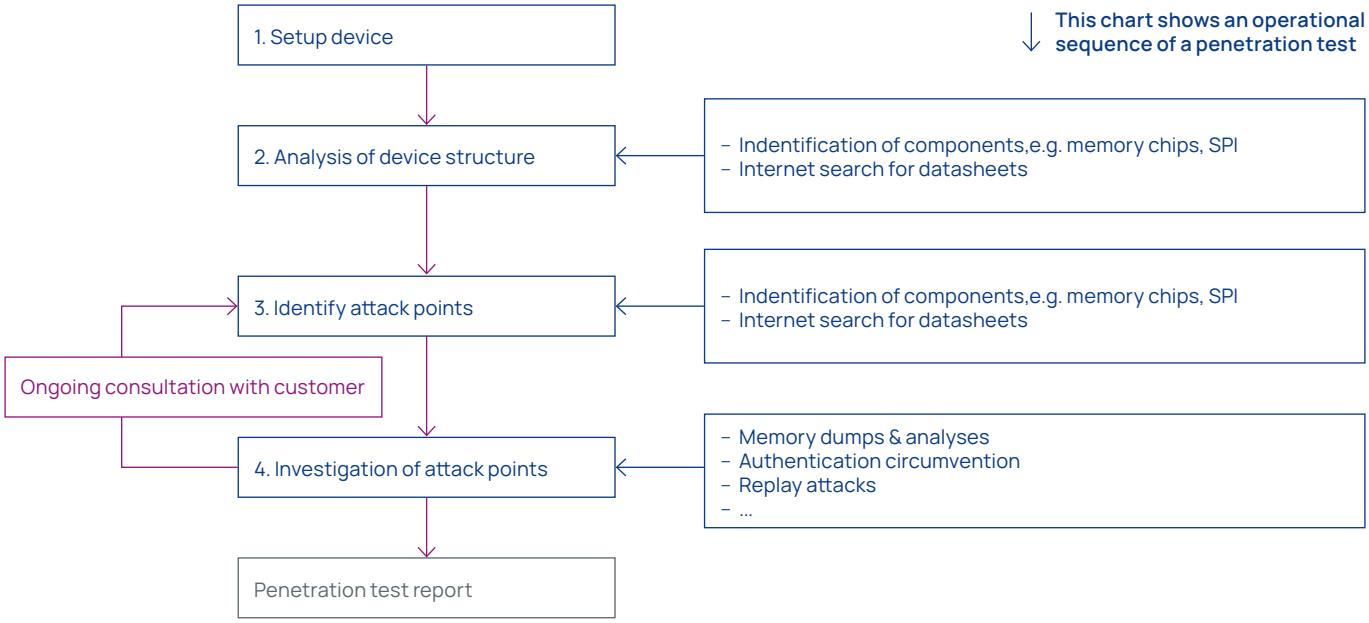
Penetration testing

Penetration tests turn known attack theories or newly identified vulnerabilities into real proof-of-concept attacks to fulfill a realistic attack goal and identify physical weaknesses often not covered by other security tests. A penetration test can include following modules:

- Vulnerability scans
- Systematic fuzzing
- Exploration/exploitation tests
- Reverse engineering
- Implementation attacks

Functional testing

With functional security tests the good performance, correctness and robustness of already implemented security functionality can be verified (e.g., encryption algorithms, security protocols).



Our service at a glance

- Identification of critical security threats of your embedded system at implementation and deployment level before it leads to real safety or financial or PR damage
- Demonstration of how difficult or how easy it is to break into your embedded system based on realistic proof-of-concept attacks
- Check existing protections in your embedded system if they are (still) capable to defend actual security attacks
- Detailed documentation describing the result of every attack
- Accurate evaluation and risk assessment for each finding by the experienced testing team
- Risk assessment based on CVSS possible
- Detailed recommendations of state-of-the-art protection mechanisms, which reduce identified security risks to an acceptable level in order to enable economic security

Testing packages

ETAS offers individual testing packages tailored to the special requirements of the embedded system. All available testing methods and modules can be combined and the testing scope can be adapted accordingly. A typical penetration testing package for embedded devices consists of the modules vulnerability scanning, fuzzing, and exploration & exploitation. Optionally this can be expanded by other test modules, e.g., reverse engineering. Or the penetration test can be conducted together with a code review of critical code parts or functional testing.

A special testing trial package gives a quick overview about potential security risks and potential attacks for your product (if any) and suggests where further investigations might become necessary in order to ensure a cost-efficient, result-oriented testing approach.

Your benefits with ESCRYPT security testing services

- Prevent hacker attacks that put your organization's reputation and trustworthiness at stake
- Ensure a cost-efficient risk management
- Avoid the cost of system downtime
- Meet regulatory requirements and avoid fines
- Maintain positive corporate image and customer loyalty

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/security-testing

ETAS/COM2_AS/12/2022

Unmask hidden security risks in your system **ESCRYPT fuzz testing service**



Introduction

With each passing year, vehicles become more complex and connected. In fact, International Data Corporation predicts that by 2023, nearly 70 % of worldwide new light-duty vehicles and trucks will have embedded connectivity. In the U.S., the number is even higher – 90 %.

While this connectivity provides consumers the driving experience they demand, it also significantly increases the vehicle's attack surface – USB connections, connected entertainment, navigation systems and wireless systems. This makes vehicle cybersecurity testing even more critical to prevent criminals from stealing the vehicle and compromising vehicle systems, privacy, and safety of occupants.

A powerful testing technique to check software and system robustness is fuzzing. Fuzzing tests the target's reaction to randomly generated invalid or unexpected input in such a way that it triggers hidden bugs in the implementation. These bugs can lead to insecure and undefined behavior – leaking of secrets and crashes.

Your fuzz testing benefits

- Address bugs before release
- Reduce number of open vulnerabilities
- Reduce bugs in carry over software

ETAS – your fuzzing partner

ETAS' security testing experts are providing fuzz testing to customers for over five years. They use commercially available and with ESCRYPT CycurFUZZ in-house fuzzers for automotive and OEM specific protocols, such as UDS and J1939.

By this, they have already discovered weak points and implementation errors in numerous customer projects – up to and including the sudden crash of safety-relevant ECUs.

Our services at a glance

Holistic fuzz testing service suited for your needs

- Commercially available and in-house fuzzers for automotive and OEM specific specifications, such as GM CG4579
- In-house R&D including several patents
- Support of system level and Software-in-the-Loop (SiL) fuzz testing
- ECU reponse monitoring on several layers (protocol specific, amperage, power cycles, camera detection, ...)

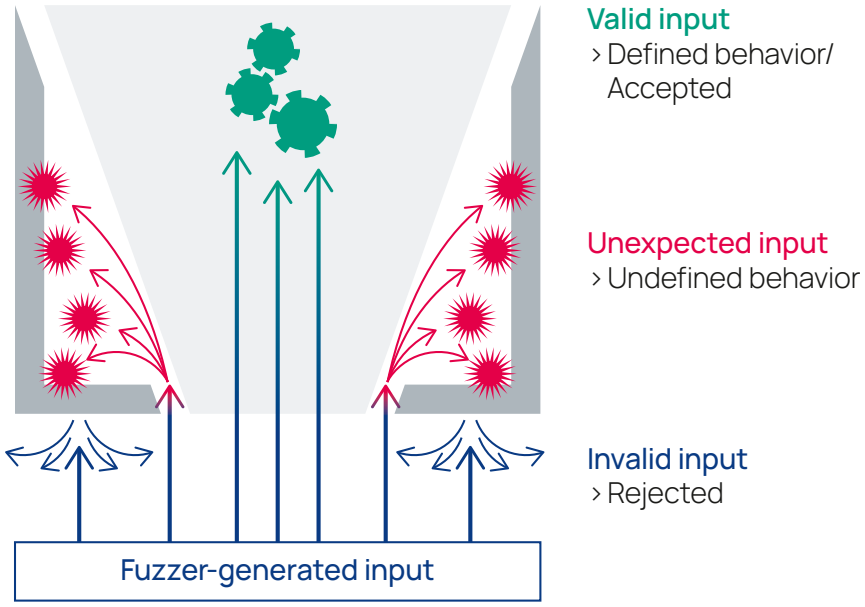
All relevant protocols & applications supported

The ESCRYPT fuzzing service is available for CAN-based protocols, Ethernet-based protocols (TCP, TLS, etc), automotive connected ECU protocols (WIFI, BT, USB, etc.) and many more.

Please contact us for a full list, covering more than 40 protocols!

Fast, informative and reliable test results

Pre-notification of findings and comprehensive report with management summary, carried out tests, list of findings with severity assessment and suggested mitigations.



Your benefits with the ESCRYPT fuzz testing service

- Support via experienced testing team and fully equipped testing lab
- We align our testing portfolio with all major OEMs to cover their fuzz testing requirements
- Comprehensive report with management summary, carried out tests, list of findings with severity assessment and suggested mitigations
- Pre-notification of findings

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Weitere Produktinformationen:
www.etas.com/fuzz-testing

ETAS/COM2_AS/12/2022

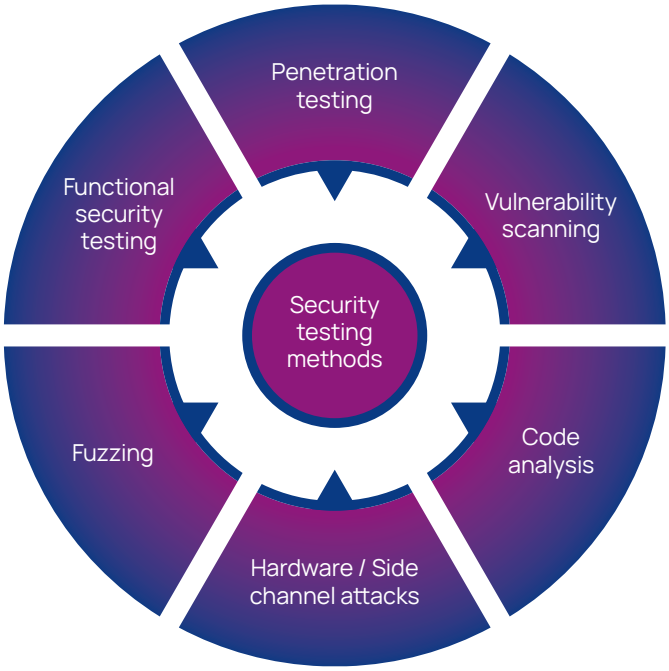


Finding the best security testing strategy **ESCRYPT security test consulting**

Introduction

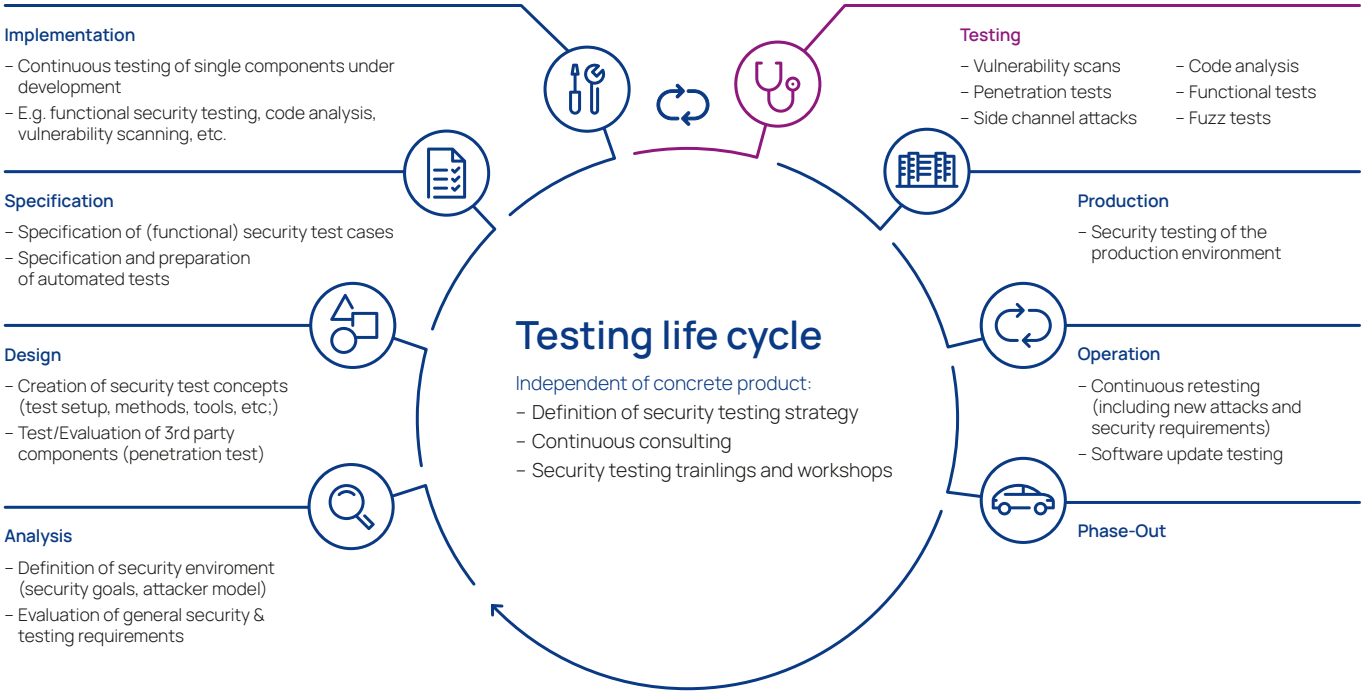
With increasing connectivity and automation, IT security functions have long become a critical business success factor. Security testing is one of the key components of a solid, holistic cybersecurity approach. It uncovers exploitable flaws and vulnerabilities in the hardware or software implementation of a target and reduces safety, financial, operational, and legal risks.

Code review, penetration testing, fuzzing, automated vs. nonautomated, blackbox, greybox and whitebox – there are many approaches, tools and techniques to consider once it comes to identifying a suitable security testing method for a product. The ESCRYPT security test consulting supports you in understanding security testing better and finding the most appropriate testing strategy for your needs.



Consulting tailored to your needs

The ESCRYPT security test consulting will answer your questions about security testing and the best strategy for your product. Depending on your requirements our experts will recommend methods and tools and make recommendations on the best time frame to implement security testing. The scope of this service will be tailored to your needs, so contact us to talk about your project.



Questions you might have asked yourself

- What kind of testing methods should I consider for my product?
- What are the advantages and disadvantages of a certain method?
- When in the product development process should I do what kind of security testing?
- Which components should I test? How to prioritize?
- What can be automated?
- What about the economic side - how much security testing is really needed?

Security test consulting at a glance

- Individual consulting in the area of security testing (e.g. methods, tools, expertise etc.)
- Support with continuous integrated security testing
  - Integration of security testing into the existing product development process (processes, work products, roles, etc.)
  - Recommendation of methods and tools
  - Interpretation of security testing results
- Internal security testing strategies, processes, standards and requirements
- Creation of security testing artefacts
  - Technical security testing guidelines
  - Creation of security test concepts and specifications (test setup, test cases, test steps)
- Depending on customer requirements ETAS offers different security testing workshops and security testing trainings

Your benefits with ESCRYPT security test consulting

- Save time, money and resources with efficient security testing
- Increase the security of your products by finding loop-holes, before someone else does
- Learn to understand and manage the complexity of security testing
- Define your own security testing strategy for your specific needs

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/security-test-consulting

ETAS/COM2_AS/12/2022