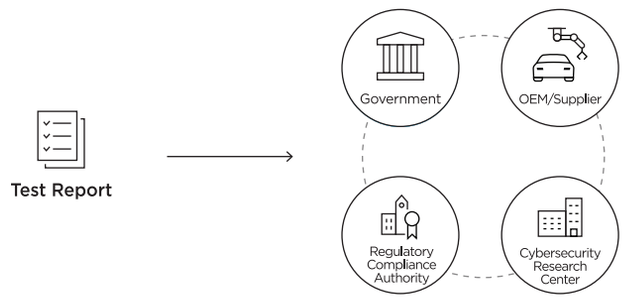
AutoCrypt CSTP

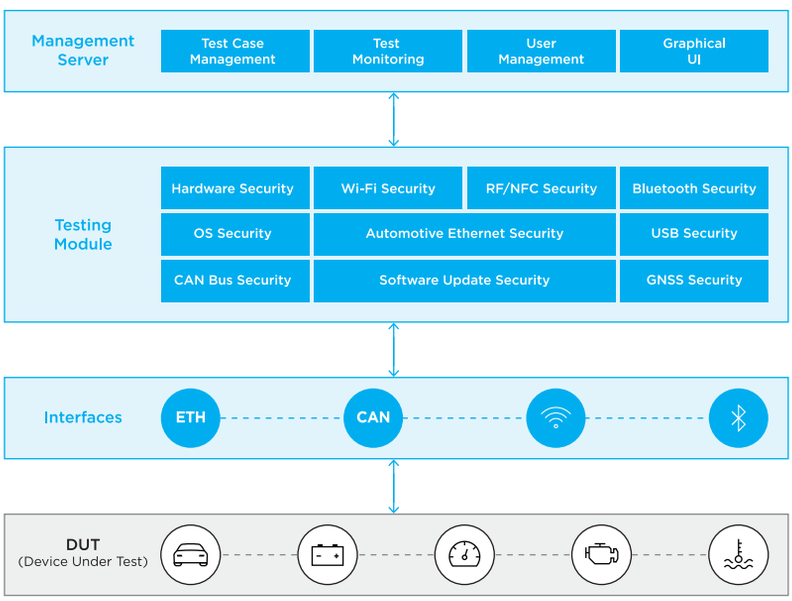
Comprehensive cybersecurity testing platform

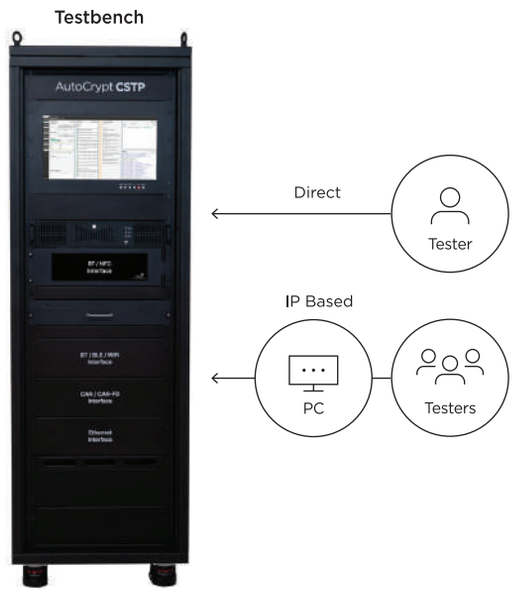
AUTOCRYPT provides an advanced and integrated platform with proprietary test cases tailored to UN R155/156 and GB compliance, enabling a streamlined process for regulatory compliance.

AutoCrypt® CSTP (Cybersecurity Testing Platform) is a highly versatile and automated platform that runs a full range of automotive cybersecurity tests in accordance with the requirements of UN Regulation 155/156 and SAC's GB standard. It is designed to support a full range of ECU types and communication protocols including CAN, Ethernet, Wi-Fi, USB, and Bluetooth.

The platform generates comprehensive reports that group testing results by test cases, allowing for easy result sharing with suppliers and **regulatory compliance** authorities.







Supported Tests

- Security Validation Testing
- Functional Testing
- Penetration Testing
- Fuzz Testing
- Vulnerability Testing

Professional Services

- Engineering Service

AutoCrypt CSTP offers **proprietary test cases** mapped out for UN R155/156 and GB requirements. Users can select individual test cases from the list provided, based on their vehicle type, system type, specifications, and environments.

AUTOCRYPT provides automated and manual test cases optimized for the client's systems and environment.

The automated testing feature enables **uninterrupted testing** throughout the entire test project.

For test cases that are difficult to automate, AUTOCRYPT offers a **manual test case engineering service.** Our engineers visit the clients' site to establish test case criteria, implement streamlined testing, and assist with reporting processes for regulatory compliance.

AUTOCRYPT

APAC Autocrypt Co., Ltd | Seoul, Korea
NORTH AMERICA Autocrypt Inc. | Irvine, CA, USA
EUROPE Autocrypt Technologies GmbH | Munich, Germany

CONTACT global@autocrypt.io

AutoCrypt IDS & vSOC

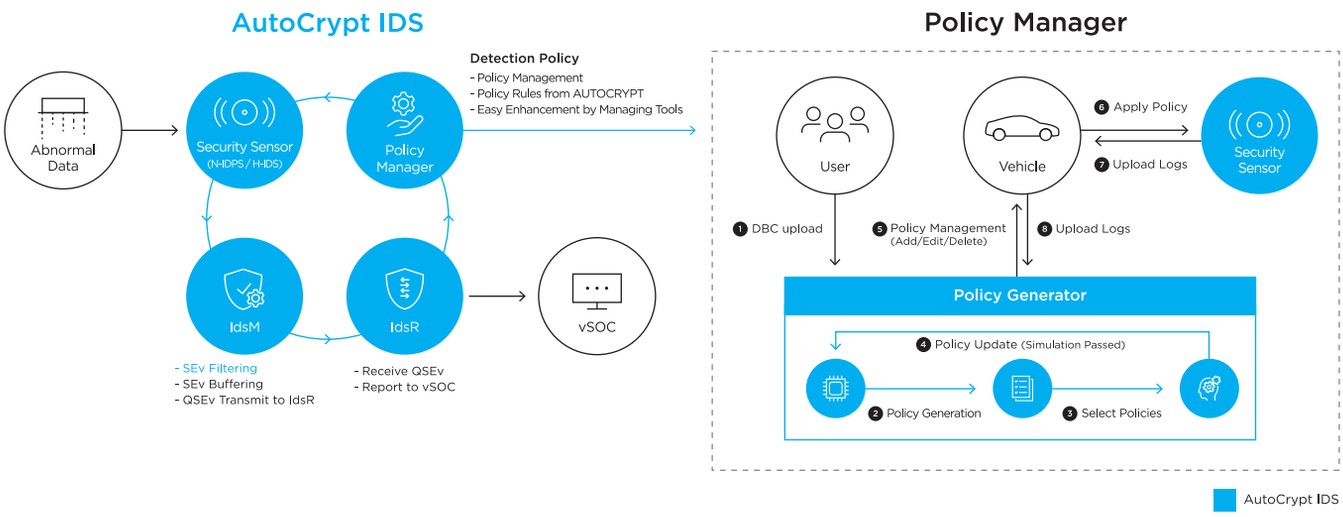
Intrusion detection and threat monitoring

AUTOCRYPT provides a vehicular intrusion detection solution that detects, filters, and prevents cyberattacks against in-vehicle systems.

AutoCrypt® IDS

Intrusion detection system and smart policy management

AutoCrypt® IDS is an advanced automotive intrusion detection system running AUTOCRYPT's proprietary Security Sensor, readily implementable in both AUTOSAR and proprietary environments.



Security Sensor

N-IDS (network IDS) detects abnormal data in the network; **H-IDS** (host IDS) identifies abnormal behaviours within the ECUs.

Evaluation and Reporting

IDS Manager (IdsM) evaluates detected security events (SEv) and sends qualified cases (QSEv) to the **IDS Reporter** (IdsR).

Automated Policy Generation

Newly reported intrusions are sent to the **Policy Manager**, which utilizes data from the DBC to automatically generate detection policies, refine them through simulations, and apply them to the Security Sensor.

Policy Simulation

Smart Policy Simulator runs simulations to evaluate policy effectiveness and provides policy enhancement recommendations based on their importance to vehicle functionality.

AutoCrypt® vSOC

Vehicle security operations center

To monitor and manage threats of a fleet in real-time, AutoCrypt IDS can be paired with AutoCrypt vSOC or VSOC solutions from third-party providers.

AutoCrypt® vSOC provides an intuitive, real-time dashboard with a graphical UI, allowing OEMs to monitor their vehicle fleet for potential cybersecurity risks, view real-time detection logs, analyze results, as well as manage and update detection policies.

AUTOCRYPT

APAC Autocrypt Co., Ltd | Seoul, Korea
NORTH AMERICA Autocrypt Inc. | Irvine, CA, USA
EUROPE Autocrypt Technologies GmbH | Munich, Germany

CONTACT global@autocrypt.io