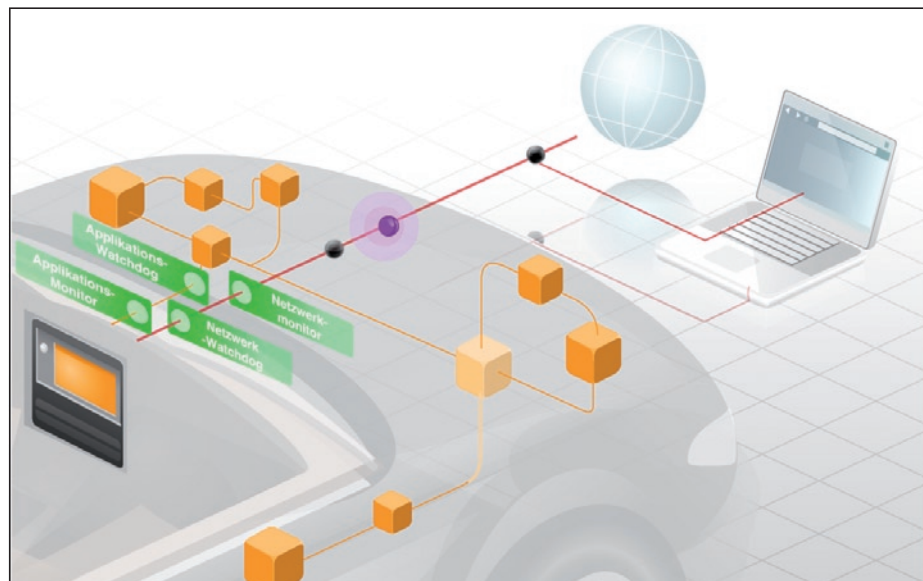


# White Paper

Version: August 2009

## Towards a Secure Automotive Platform



<b>1</b>	Introduction . . . . .	3
<b>2</b>	Use Cases . . . . .	5
<b>3</b>	Technical Overview of MOBICORE4 Runtime. . . . .	6
<b>4</b>	Technical Overview on secunet Technology . . . . .	8
<b>5</b>	Value Proposition of the Secure Automotive Platform . . . . .	11
<b>6</b>	Glossary . . . . .	14

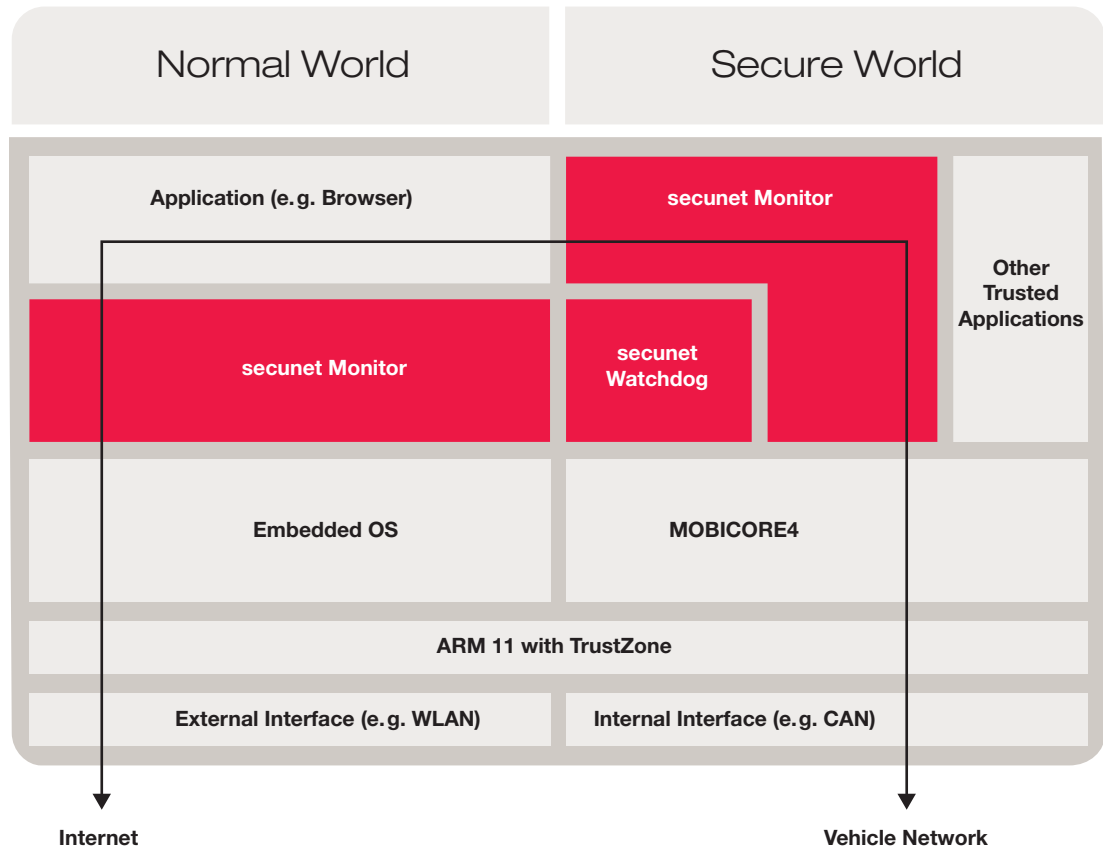
# 1 Introduction

Future automotive infotainment platforms are characterised by the following features:

- Use of web services from the Internet
- Utilisation of public communication infrastructure
- Third party applications
- Connectivity to in-vehicle networks

Many applications will be based on the Internet. Such services require a car to go online immediately at any time to deliver a superior user experience for the driver or the passengers of a car. Such a scenario on the other hand implies the usage of public communication infrastructure to enable a car to use any available connectivity to be online all the time. As a consequence, the communication of the car with any backend infrastructure will use public networks. Cars will then be visible in the Internet by its Internet address and therefore exposed to Internet attacks. Moreover, future automotive infotainment platforms have to support third party applications like YouTube. They have to create an ecosystem for a plethora of application developers to deliver a rich offering of services to car passengers. As a consequence, not only the control over the communication infrastructure but also the control over the applications themselves do shift from carmakers to application providers being new players in the automotive market. For this reason, third party applications like e. g. facebook and car related functions like Local Danger Warning (C2C applications) will run on the same platform. The latter requires access to in-vehicle bus systems in both directions. That means that third party applications might also access the vehicle bus systems. If those applications are not monitored and controlled and bus systems and electronic control units are not protected against attackers, malicious applications and attackers might compromise the safety of the car. Due to the open interfaces, a hacker from the Internet might even get remote access to vehicle bus systems just like a hacker of a company's LAN.

To thwart these threats secunet, Giesecke & Devirent (G&D) and ARM joined forces to deliver an open secure automotive infotainment appliance to the automotive market. It addresses the resulting risks for vehicle networks while enabling car manufactures to offer any kind of web based applications based on a secure and future ready infotainment platform as outlined in the following picture:



In order to separate the Internet from the vehicle networks, G&D MOBICORE4 enables the secure automotive platform to create and monitor runtime environments on the embedded platform, that are securely shielded against each other to execute security-critical applications in a trustworthy environment (Secure World). Third party applications can be run in a more open environment (Normal World). MOBICORE4 is designed for ARM® processors with TrustZone® thus leveraging the security potential of ARM TrustZone hardware virtualisation technology.

This combination of ARM TrustZone hardware virtualisation and G&D’s secure operating system MOBICORE4 assures protection, control, monitoring and remote management of security critical processes on the secure automotive appliance. At the same time, it provides secure interfaces between the separated environments based on ARMs TrustZone API.

While G&D MOBICORE4 isolates safety critical applications from third party applications and provides well defined communication channels between the different runtime environments, secunet modules monitor the communication and data that are exchanged via the interfaces between the two runtime environments. They take proper action to remove the car from an attack. Thus safety critical data can be identified and neutralised. The monitoring is done at interface driver level, network level and application level. The monitoring utilises firewall techniques, intrusion detection mechanisms and scanning methods. It provides reports about safety critical incidents to other applications.

Leveraging the security of MOBICORE4 an automotive specific watchdog module (WM) in the secure runtime environment receives the incident reports via the hardware secured ARM TrustZone APIs from the monitoring modules. It checks the integrity of the monitors during runtime. It takes proper action to hide the platform from a detected attack, neutralises erroneous or malicious applications and blocks unwanted communication towards the vehicle bus systems. ARM TrustZone based MOBICORE4 together with the secunet modules guarantee that full reliability of the secure automotive platform and the safety of the vehicle bus systems are maintained throughout the whole lifecycle of the infotainment appliance.

## 2 Use Cases

The secure automotive platform assures system security for the vehicle network while empowering a wide range of new services for connected vehicles. MOBICORE4 technology, combined with secunet technology, enable the following areas of use:

- Seamless, controlled and secure integration of additional external devices such as mobile devices, smart phones, MP3 players or navigation devices into the vehicle network. Particular attention is given to the isolation and protection of the vehicle networks against external interfaces or unintended communication with external devices. Malicious code for example designed to interfere with in-car networks can be blocked.
- Enhancement of authenticity and integrity in remote diagnostics of in-car systems. Such diagnostics continuously provide data for current system and application configuration and status.
- Implementing Car2Car use cases in the presence of third party applications.
- Utilisation of Internet based web services that require communication with the vehicle network.
- Enabling financial services in a secure manner, such as the billing and payment of road charges or entertainment content. Secure feature enablement would allow customers to purchase upgrades without needing to return to the place of purchase.

### 3 Technical Overview of MOBICORE4 Runtime

In the Automotive context, MOBICORE4 runtime provides the separation technology to create isolated runtime environments – one for third party applications and one for safety relevant applications.

With MOBICORE4 runtime, safety-relevant processes are encapsulated in a Secure World by hardware based mechanisms of ARM® TrustZone® technology extensions.

In technical terms, the concept of ARM TrustZone (TZ) involves two separate execution modes isolated by hardware security mechanism such as an extra security bit on the AMBA bus. Therefore an ARM TZ processor enables the two processor “worlds”:

- Normal World with any Embedded OS e. g. Android OS.
- Secure World with the G&D MOBICORE4 runtime environment.

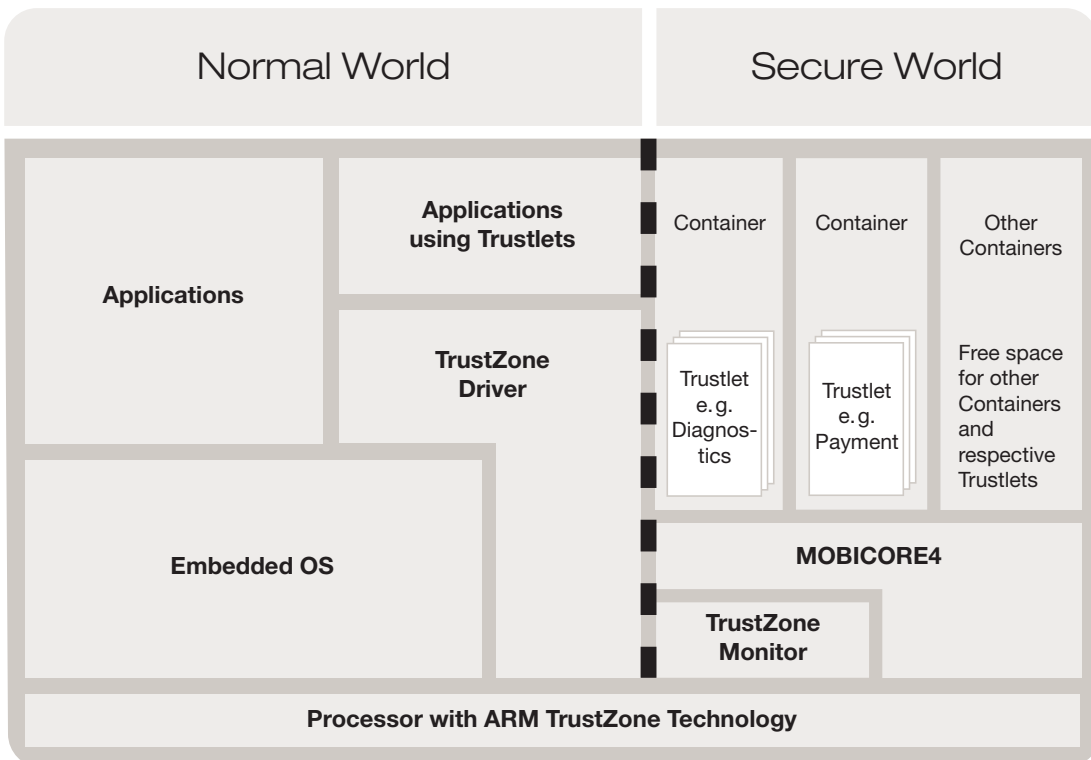


Figure 1: Security relevant applications, i. e. ‘Trustlets’, can be distributed in one or more separate ‘containers’, isolated within the ECU via ARM® TrustZone® technology.

The TZ Monitor mode enables a switch between the Secure World and the Normal World (see figure 1). The TZ Monitor controls the secure state of an ARM1176 or ARM Cortex-A TrustZone enabled processor by transferring control from one world to the other. This secure TZ Monitor processes switches to and from the Secure World. In order to switch to the Secure World, a special Secure Monitor Call (SMC) instruction is used to execute the secure TZ Monitor. Any Normal World application is able to initiate this switch. From a security standpoint the initiation of a SMC is not critical, because it is just a call to the Secure World without any information leakage from the Secure to the Normal World.

Tasks within the Secure World are separated by the MOBICORE4 Runtime. The MOBICORE4 Runtime is executed within the Secure World. Different service providers can claim processor space within the Secure World, so called 'containers'. Inside their containers they can then provide numerous service Trustlets for their security sensitive applications.

The separation and isolation of Trustlets, within the Secure World is a core security functionality of MOBICORE4. The MOBICORE4 Runtime guarantees that memory, which was assigned to one "Container", e. g. containing cryptographic keys, can never be used or modified in an unauthorized manner by Trustlets running in other containers. Thus, applications are protected, separated and even erroneous or malicious code cannot damage other applications. This protection is supported by the ARM TrustZone processor hardware.

The communication between a Trustlet in the Secure World and the Normal World Operating System is enabled via a standardised interface, the 'TrustZone Application Programming Interface (API)'. The TrustZone API is a communication interface enabling Normal World applications to exchange data with Trustlets executed in the Secure World.

## 4 Technical Overview of secunet Technology

Leveraging the MOBICORE4 Trustlet Technology and ARM TrustZone Application Programming Interface, secunet technology protects the cross linking of the secure automotive appliance with a vehicular network infrastructure. The secunet technology provides device-, network- and application level modules that monitor and filter the communication from external systems into the vehicle network. Moreover the unauthorised manipulation of data and code of the automotive platform, especially of the monitoring modules, is detected and set back to a safe state. This is done by a watchdog module that is independent from the Normal World (cf. figure 1). It collects information from the monitoring modules and the MOBICORE4 runtime about incidents. If the watchdog considers the incidents safety-relevant proper action is taken to bring the car out of reach of the attack. The following picture shows the architecture of the secure automotive appliance:

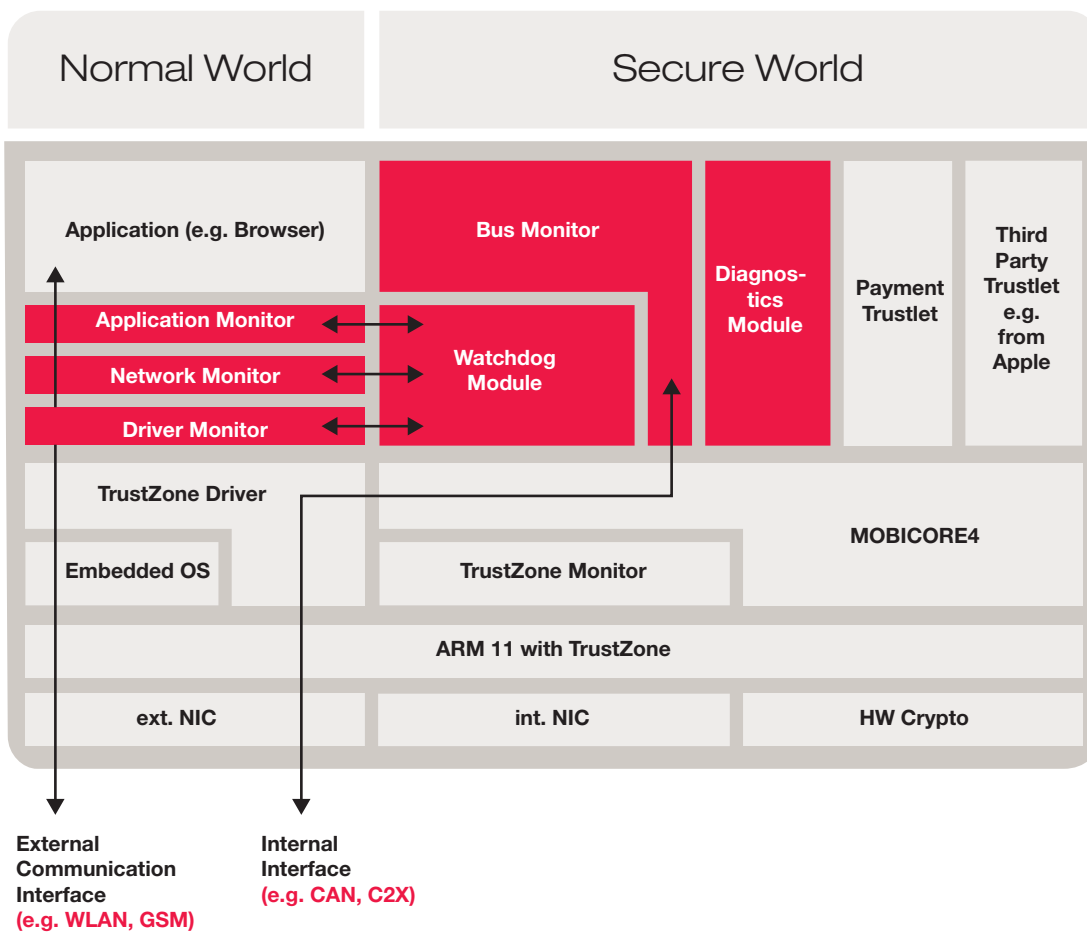


Figure 2: Integration of secunet technology with MOBICORE4

- Driver Monitor (DM)
  - The DM monitors the number of packets that are transmitted via the external interface and checks if a certain threshold is exceeded. Thus it is guaranteed, that any flooding of the appliance is detected as long as enough cpu resources are still available.
  - Moreover the DM provides an IPSec tunnel to a trustworthy environment of an OEM that terminates in the Normal World. This function uses the Truszone API to access the crypto resources in the secure zone.
  - Malicious events are provided to the watchdog module (cf. below) using the TrustZone API.
  
- Network Monitor (NM)
  - The NM detects attacks on network layer, i. e. attacks based on tweaking the TCP/IP headers or the IP-protocols; it utilises information gained from the TCP/IP Stack and Firewall.
  - Malicious events are provided to the watchdog module (cf. below) using the TrustZone API.
  
- Application Monitor (AM)
  - While the network monitor filters information and protocols, which are transmitted at the TCP/IP level, the AM scans protocols, e. g. HTTP, IRC, and data on application layer that are transmitted in the payload of the IP packets.
  - Using heuristics it monitors events that are related in time like intrusion detection systems (IDS) and data like a malware scanner.
  - Malicious events are provided to the enforcement watchdog (cf. below) using the TrustZone API.
  
- Bus Monitor (BM)
  - Any information that has to be transmitted from the Normal World to the vehicle network has to pass the BM. Based on the ARM Trustzone HW MOBICORE runtime environment guarantees, that the network interfaces (NIF) can be accessed only via the Secure World.
  - The BM detects the flooding of vehicle networks, i. e. if too many messages are transmitted to the vehicle network.
  - Moreover the BM keeps a white list what kind of messages, e. g. CAN message identifiers, and what kind of respective payload, e. g. range of a certain value, is admitted to enter the vehicle network.
  
- Watchdog Module (WM)
  - The WM is the core component of the secunet technology. It is an independent active component to take proper action to neutralise remote attacks.
  - Using the MOBICORE4 technology the WM monitors the driver-, network- and application monitors during runtime to ensure that the integrity of these modules is never compromised and that they are always alive. Thus it can be detected if e. g. the network monitor code was

manipulated by a virus before start-up or during runtime or if too much cpu time is consumed due to a SYN-attack.

- This protection can be applied to any application in the Normal World.
- The WM collects the safety relevant incidents detected by the monitors mentioned above and by the runtime environment itself.
- Upon detection of a compromised monitor or a safety relevant incident in the platform itself the WM takes proper action to remove the car from the attack:
  - Shut-downs or restarts external interfaces with a different network ID, e. g. IPv6 address or different MAC.
  - Switches to other interfaces to hide from an attacker. E. g. switching from WLAN to HSDPA.
  - Blocking or confining the bandwidth the internal interfaces in case of an alert from the bus monitor.
  - Re-establishing the integrity of the monitors or the above mentioned white list applications, e. g. by restarting from a trusted memory using secure boot mechanisms of the MOBICORE4.

#### ■ Diagnostics Module

- Configuration parameters of the secunet monitors such as the acceptable bandwidth for an external interface are set via the diagnostics modules.
- The parameters can be set remotely using an IPSec tunnel starting from the OEM systems and terminating in the Secure World leveraging MOBICORE secure update mechanisms.
- Using the TrustZone API dedicated applications can re-set the parameters dynamically e. g. to increase the acceptable bandwidth during runtime if necessary.
- The diagnostics module also provides information about the security incidents to applications in the Normal World via the TrustZone API in order to guarantee a seamless operation of an application after the EW has taken actions to neutralise remote attacks. Such information could also be provided to the OEM using an IPSec tunnel starting from the OEM systems and terminating in the Secure World leveraging MOBICORE secure update mechanisms.
- The DM itself can be updated using an IPSec tunnel starting from the OEM systems and terminating in the Secure World leveraging MOBICORE secure update mechanisms.

The automotive industry moves towards ever more sophisticated, open software applications and increased collaboration with a growing number of external application partners and providers. Against this background, secunet's experience in implementing security in automotive systems and processes, combined with G&D's expertise in providing trusted technologies for ARM TrustZone processors and services, offers a highly valuable solution to the automotive industry.

## 5 Value Proposition of the Secure Automotive Platform

The secure automotive platform is based on G&D's and secunet's experience with trusted devices, trusted services and security certification. MOBICORE4 provides additional security to automotive communication modules, which is also beneficial for reliability. Based on a thorough security analysis of automotive systems by G&D and secunet, the secure automotive platform offers the following value propositions:

- **Secure Boot Process:**
  - The OS start-up is executed without any interference from untrusted code. The OS start-up is not part of MOBICORE4 itself, but inherent for the security of the whole system and therefore also designed and implemented by G&D.
  
- **Secure Communication API between normal and secure Execution Environment:**
  - Of course, communication interface from Normal World to Secure World provides risks for data leakage and for malicious intrusion. MOBICORE4 therefore incorporates a security model to confine these risks. Moreover, the strength of the isolation mechanism in this security model is according the needs for a Common Criteria security evaluation or certification.
  
- **Secure Memory Access:**
  - Cases will occur where storage must be used that is not mapped to exclusive access by secure processes. This is true for the possible use of conventional RAM that is administered by the Normal World software (e. g. for shared memory) and this is especially true for all Secure World data to be stored in conventional persistent storage. The answer to this is integrity protection by automated calculation and verification of hash values at any conventional memory access or – to provide confidentiality – automatic encryption/decryption with a secret only known to MOBICORE4.
  
- **Secure Trustlets and Trustlet Access:**
  - The code and data of Trustlets are protected against read and write access from the Normal World software. This is mainly achieved by the TrustZone security feature itself, when the memory used for MOBICORE4 and its Trustlets is exclusively mapped to the secure mode.
  - Trustlets want to use sensitive data such as cryptographic keys. This sensitive data must be protected against unauthorised access from the Normal World and other Trustlets. Therefore, a memory separation between Trustlets is part of MOBICORE4.

- Protection against bus-based Attacks:
  - The underlying MOBICORE4 hardware security of the TrustZone relies on the MMU (Memory Management Unit) to a large extent. Bus Master Devices can completely circumvent the MMU. To guarantee security in this case, it is important that no malicious or faulty bus master driver is present in the hardware design on the given system. Bus masters that do not need to be trusted are prevented from accessing the Secure World. Therefore G&D and ARM can support a hardware validation and review process from the security standpoint.
  - Advanced attackers could intercept secrets or completely circumvent the MMU protection via bus probing methods. Use cases for MOBICORE4 exist that involve the processing of secrets where such an attack could be considered worthwhile. Therefore, the target hardware platforms on which the MOBICORE4 is implemented could provide an exclusive portion of RAM that is located on the System-on-Chip (SoC) and therefore not reachable for bus probing. The MOBICORE4 provides an option to map this memory for exclusive usage and thus protect it against bus probing. The design of MOBICORE4 has put particular focus on placing such sensitive code and data and everything that handles MMU settings into the On-SoC-RAM. Hence, MOBICORE4 assures a higher level of security, especially in comparison with solutions which are merely based on para-virtualisation.
  
- Secure Communication with trustworthy Backends:
  - Providing certificate based IPSec tunnel functionality, the secure automotive platform supports the secure communication of a car with a trusted backend system. Such functionality enables secure remote maintenance i. e. a secure life cycle management of the secure automotive platform.
  
- Detection of Attacks from external Interfaces and filtering-out malicious communication towards the cars' core systems:
  - The driver and network monitors detect any attacks that might occur via the external interface on network layer, e. g. flooding attacks. It monitors the numbers of IP-packets, which are transmitted via the external interfaces, and checks IP-Stack- and firewall-rules. Thus flooding attacks and attacks, that are based on TCP/IP-headers and -protocols .
  - The Bus Monitor filters the whole communication that comes from the Normal World and is bound for the vehicle network. It detects unwanted data and events that might compromise the safety of the vehicle networks e. g. CAN.
  
- Detection of abnormal Application Behaviour:
  - The application monitor detects abnormal behaviour of applications which are executed in the Normal World and monitors application level protocols.

- Runtime Integrity Checks:
  - The monitors run in the Normal World, where the communication of third party application with external systems like the Internet terminates. Therefore their execution is monitored by the watchdog module during runtime to ensure that the integrity of the monitors is never compromised and that it is always alive and reports incidents to the watchdog module. (cf. below).
  
- Active Neutralisation of Remote Attacks against the Car:
  - The secunet watchdog module assures the continuous and trusted execution of crucial core processes of the secure automotive platform. It blocks communication towards the car's bus systems in case of an attack being detected by the bus monitor, shuts-down or restarts external interfaces if necessary and re-establishes the runtime integrity of the Normal World.
  
- Diagnostics of in-car Systems:
  - The interaction between the Normal and the Secure World can be enhanced even further by the secunet diagnostics module which checks and sets the configuration and status of applications upon request. This can be done over-the-air (OTA) or in combination with proprietary diagnostics systems of the OEM. This could enable the OEM to provide OTA car diagnostic services to its customers via a secure communication channel to each single car.
  
- Secure Boot, Cryptography and Updates:
  - In combination with the secunet technology, the G&D MOBICORE4 serves as Secure OS with a secure boot process and also provides security libraries, including cryptographic applications. It serves as secure execution environment for the driver-, network- and application-monitor, and enables the provision secunet technology updates across platform's lifecycle.

## 6 Glossary

API	Application Programming Interface
ARM	ARM Ltd – Architects of the Digital World
CC	Common Criteria
Container	Space for MOBICORE Applications i. e. Trustlets
CPU	Central processing Unit
DoS	Denial of Service
DRM	Digital Rights Management
ECU	Electronic Control Unit
HSDPA	High Speed Downlink Packet Access (HSDPA), part of UMTS standard
IPv6	Internet Protocol version 6
IPSec	Internet Protocol Security, Protocol for a confidential, authenticated and integrity checked communication
M2M	Machine-to-Machine
MAC-Address	Media Access Control Address, unique identifier for network devices.
MMU	Memory Management Unit
NIF	Network interface
NFC	Near Field Communication
NVM	Non Volatile Memory
OEM	Original Equipment Manufacturer
OTA	Over-the-air
RAM	Random Access Memory
RISC	Reduced Instruction Set Computing
SE	Secure Element
SCU	Secure Communication Unit
SMC	Secure Monitor Call
SYN-flooding	Internet attack, that initializes too many Internet connections and forces the OS to keep them open. Thus all of the CPU computing power is consumed by these useless connections.
Trustlet	Application running in the TrustZone
Trustlet API	API for the Development of Applications on top of MOBICORE
TZ	TrustZone
TZ API	TrustZone Application Programming Interface
WLAN	Wireless LAN, wireless communication standard standardized in IEEE 802.11

## About secunet

secunet is one of Germany's leading providers of superior IT security. In a close dialogue with its customers – enterprises, public authorities and international organisations – secunet develops high-capacity products and excellent IT security solutions. Thus, secunet not only keeps IT infrastructures secure for its customers, but also achieves intelligent process optimisation and creates sustainable added value.

secunet has an impeccable track record as a partner and consultant for manufacturers and suppliers in the automotive industry. We provide support in designing, implementing and testing innovative security solutions in the areas of flash ware protection, function enabling, car immobilisers and integration of mobile devices. In addition, we support customers in the development of innovative vehicle technologies in view of IT security aspects. This includes for instance communication between vehicles and the Internet or driver and vehicle authentication for downloads of data that are subject to fees, the corresponding backend infrastructure as well as required processes in all development phases of the vehicle.

### Contact

**Dr. Marc Lindlbauer**

**E-mail: [automotive@secunet.com](mailto:automotive@secunet.com)**

**secunet**

**secunet Security Networks AG**

**Kronprinzenstraße 30**

**45128 Essen**

**Germany**

**Tel: +49-201-5454-0**

**E-Mail: [info@secunet.com](mailto:info@secunet.com)**

**[www.secunet.com](http://www.secunet.com)**