Giesecke & Devrient
Creating Confidence.

PRESS RELEASE

Giesecke & Devrient and IBM Team Up on New Connected Vehicle Cryptographic Security

Munich (Germany), September 16, 2015 – Giesecke & Devrient (G&D) and IBM (NYSE: IBM) are teaming up to work on a new connected vehicle security solution with the intent to make car hacks much more difficult in the future.

IT security is becoming a crucial precondition for the automotive industry in terms of a wider adoption of connected vehicles.

“With dozens of ECUs (electronic control units) and several in-vehicle bus systems as well as various wireless connections to the external world of a connected vehicle, it is vital to protect those systems in the best possible way against remote hacks, fraudulent attacks and any attempts that could affect traffic safety,” states Erich Nickel, Director of Automotive Solutions CoC DACH at IBM. “As a multitude of connected vehicle online services are already available, involving aspects of data privacy and secure payments, secure infrastructures and communication channels are needed.”

Security infrastructures are required within the vehicle and from the vehicle to the backend infrastructures. As trusted partners and suppliers for the automotive industry, IBM and G&D team up to tackle these security challenges for the connected vehicle ecosystem.

“As a leading provider of M2M SIMs and of securing digital identities, G&D has transferred its high security standards from the smart card ecosystem into the world of networked mobility. The products and solutions fulfil the requirements and standards of the specific industries such as ISO/TS 16949, which is considered the model for quality management systems in the automotive industry,” says Axel Deininger, Head of the Enterprise Security/OEM division in the Mobile Security business unit at G&D.

IBM and G&D showcase connected vehicle security solution

Giesecke & Devrient GmbH · Corporate Communications · www.gi-de.com/press
Press inquiries: Tobias Steininger · E-Mail: Tobias.Steininger@gi-de.com
Prinzregentenstr. 159 · 81677 Munich · Phone +49 89 4119 1389 · Fax +49 89 4119 1208

IBM and G&D present a first showcase of the connected vehicle security. The technology partners will demonstrate a “Secure Gateway ECU” to enable a more secure communication within the vehicle and to the backend. The partners expect a further development of the platform based on OEM customer requirements over time, potentially combining other security elements to enhance the existing crypto key and chip core elements. The highlights:

- Management of trusted identities in a secure environment
- Trusted Service Management to ensure driver data security and privacy
- Secure Gateway ECU to ensure the communication within the car and to the backend
- Highly flexible connectivity management with G&D’s subscription management solution

Multiple IT security related solution components

The IBM/G&D end-to-end connected vehicle security solution platform will be based upon multiple IT security related solution components:

- Highly protected hardware elements with Smart Card level security, so-called “embedded Secure Elements” (eSE), within the vehicle for storing cryptographic keys in a protected high-level tamper-resistant area help to raise the level of security and to reduce the number of car hacks drastically.
- Key creation and lifecycle management in a key management back-end is essential to ensure both the availability and security of the encrypted information. The management of trusted identities protects users identity and enables authorized access to vehicle.
- The Subscription Management of the SIM modules (M2M SIM cards) provides automotive OEMs with more flexible connectivity solutions. A car can be individually configured for security settings when delivered in different markets and connected to service operators without changing the SIM module to simplify the

logistics. This allows vehicle manufactures more flexibility when producing vehicles for different counties with many mobile network operators (MNOs). The subscription to the MNO can be programmed when the vehicle is delivered to the destination country after manufacturing.

- Security intelligence within the vehicle, closely linked to security intelligence capabilities on the backend side, improves the detection of hacker attacks from abnormally operation monitoring. Security intelligence on the backend side with Security Operations Centers and Security Intelligence and Event Management helps detect tampering operations at an early stage to detect hacker attacks early and to avoid damages to the system. Secured communication channels and secured data storage in the cloud ensure highest standards for data privacy. This also helps to make payment transactions safer with a resilient backend infrastructure.

About Giesecke & Devrient

Giesecke & Devrient (G&D) is a leading international technology provider headquartered in Munich, Germany. Founded in 1852, the Group has a workforce of over 11,450 employees and generated sales of approximately EUR 1.83 billion in the 2014 fiscal year. 58 subsidiaries and joint ventures in 31 countries ensure customer proximity worldwide.

G&D develops, produces, and distributes products and solutions in the payment, secure communication, and identity management sectors. G&D is a technology leader in these markets and holds a strong competitive position. The Group's customer base mainly comprises central and commercial banks, mobile network operators, business enterprises, governments, and public authorities. For more information, please visit: www.gi-de.com.

About IBM

More Information about IBM: www.ibm.com

More Information about Automotive Solutions from IBM: www.ibm.com/automotive

Giesecke & Devrient GmbH · Corporate Communications · www.gi-de.com/press
Press inquiries: Tobias Steininger · E-Mail: Tobias.Steininger@gi-de.com
Prinzregentenstr. 159 · 81677 Munich · Phone +49 89 4119 1389 · Fax +49 89 4119 1208