# LINK MOTION AND IRDETO: PROVIDING THE AUTOMOTIVE INDUSTRY WITH THE MOST SECURE CARPUTER ON THE MARKET

## LINK MOTION AND IRDETO PARTNERSHIP

The past decade has seen software become a key component in automotive development and consumers are eager for more connectivity in their vehicles. Research from Parks Associates found that 64% of car owners in U.S. broadband households who own a smartphone want embedded access to connected car features in their next vehicle. In addition, Frost & Sullivan found that growing digitalization will drive the automotive industry to invest ~ $82.01 billion by 2020 on advanced technologies. While this connectivity is essential to satisfy consumer demand, it also introduces new security threats on the road.

Link Motion and Irdeto have partnered to provide the most secure carputer on the market, providing tier-ones and OEMs with a joint solution that protects vehicles from hackers and cybercriminals. Link Motion, a secure connected carputer maker, has implemented Cloakware™ for Automotive by Irdeto into its Motion T secure connected carputer. The Cloakware for Automotive solution helps the Motion T carputer block hackers and cybercriminals from altering the carputer, preventing cyberattacks targeting connected cars. Together, Link Motion and Irdeto have analyzed connected car vulnerabilities in depth to develop secure systems to help automakers provide a safe and reliable driving experience for consumers.

## HOW THE INTEGRATION WORKS

Motion T is a secure connected carputer combining five separate units: the instrument cluster, infotainment, head-up display, telematics and communications. Cloakware for Automotive by Irdeto is a comprehensive solution that combines innovative, patented technologies and cybercrime services to address a variety of security challenges in a car. Irdeto solutions include strong anti-hacking protection with renewable security, making it virtually impossible to reverse engineer vehicle software. The Cloakware for Automotive solution is easy and simple to deploy and is available on all major Automotive OS's. It provides automakers and tier-one suppliers with a secure, tamper-proof environment for vehicle software, ensuring that vehicles operate as intended.

Link Motion has designed the Motion T software and hardware together to create layers of defense to protect vehicles from attacks and to maximize security from the beginning. The seamless integration of Cloakware for Automotive into the Motion T carputer means that tier-one suppliers and OEMs do not have to add-on security, reducing hardware complexity. The carputer also provides car makers with less hardware, a faster development cycle and OTA updates, helping to improve cost efficiency. This also enables tier-ones and OEMs to bring new features, including connectivity, to the market faster. The integration of these two solutions protect vehicles from attacks through a sophisticated series of defenses to create the most secure connected carputer on the market.

## LINK MOTION AND IRDETO SOLUTION USE CASES

Hackers and cybercriminals are employing new strategies to exploit vulnerabilities in today's connected cars. With more consumers craving additional connectivity features in their vehicles, it is becoming increasingly important for automakers to address these vulnerabilities to prevent hackers from altering their automobiles. By implementing renewable and tamper-proof security, Link Motion and Irdeto provide the following benefits for players in the automotive industry:

- **Ransomware Protection:** Ransomware is a growing and damaging threat. Our solution does not allow any unauthorized software to execute, preventing the malware from causing damage. It does this with zero false positives and a 100% detection rate.
- **Future-Proofing Against Vulnerabilities:** Software vulnerabilities will always exist, allowing hackers to gain access to connected systems. When they are discovered in the field, vehicles will be vulnerable. Our solution assumes that hackers have already broken in and we stop them from doing any damage. So, when a vulnerability is discovered in an TCU, you are still protected.
- **Data Protection:** Modern vehicles are storing more and more personal data that needs to be protected. Our solution can protect sensitive data at rest, in-use and in transit, even against an attacker that has gained privileged access to a system (by exploiting a vulnerability).
- **Safety:** By not allowing hackers to modify any part of the connected ECU (TCU), we prevent them from making changes to the software on the system that will allow them to send malicious commands across the internal networks from the TCU.

## CONTACTS

For more information on this joint solution, please contact Irdeto and Link Motion:

**Daniel Thunberg**
Global Head | Automotive
Email: vehiclesecurity@irdeto.com
https://irdeto.com/automotive/automotive-security.html

**Pasi Nieminen**
CEO, Link Motion
Email: info@link-motion.com
http://link-motion.com