G+D Mobile Security

M2MD Technologies, Inc.

Solution Brief

M2MD Communications Gateway:

fast, secure, efficient

G+D Mobile Security and M2MD enable automakers to improve user experience through fast, secure and efficient cellular automotive connectivity.

Technology has transformed almost every aspect of modern life, but the car has seen changes that significantly affect our day-to-day lives. Computerization has changed the way cars work, how they are produced, and how we view and interact with them. Getting from point A to point B is no longer enough. Today's cars have smart features and are connected – transitioning to tomorrow's cars, which will be fully autonomous and require always-on connectivity.

With an increasing number of connected vehicles on the road, the need for strong security and efficient communication has become paramount. However, the increasing computerization of the car brings with it the threat of digital security breaches. Now that our cars are connected and use our personal information, car makers must protect our data while still providing convenient and flexible access.

KEY BENEFITS

The M2MD Communications Gateway transforms vehicle connectivity

- Instant connection
- Keys stored in hardware for optimal security
- Manages power consumption and costs effectively

Security challenges for the connected car

Certificate-based security is the authentication process used on the "public" internet between two devices that are unknown to each other (e.g. a personal computer and a bank's server).

This authentication process typically requires a computationally intensive handshake that takes time and requires the devices to pass data back and forth to establish a secure session. When using a computer on a home or office network, this transaction happens quickly over a data circuit with nearly unlimited data budgets and sufficient bandwidth to make certificate-based security efficient.

To minimize cost and battery consumption, car telematics control units (TCUs) typically have far less powerful processors than a normal personal computer, which increases the time needed to complete a certificate-based handshake.

In addition, wireless operators charge automakers according to the amount of data transmitted over the network, which makes the data consumed in the handshake process a relatively expensive overhead cost.

Automakers require a proven, tested security solution but need it to be fast, cost effective, and designed for the unique automotive environment.

The M2MD Communications Gateway provides end-to-end security and efficient connectivity for mobile applications. With the ability to instantly connect to a vehicle, it delivers a better user experience whilst securing the connection. No additional hardware is required – the solution works with most of the currently installed vehicle hardware.

Certificate operations in connected cars

- In automotive telematics, cellular communications happen on a private network and between two known devices that have been preconfigured to work together.
- Certificate-based handshakes require time and power to compute on embedded devices, using significant overhead data and increasing costs with each cellular session established.
- Certificate operations were designed for human intervention. They have expiration dates and require regular updates.
  If a certificate is compromised in a vehicle, the vehicle may have to be recalled, and a trip to the dealer may be the only resolution.
- On average, top-of-the-line, server-supporting, certificate-based security can support only 15,000 devices, which drives higher hardware costs and impacts scalability.

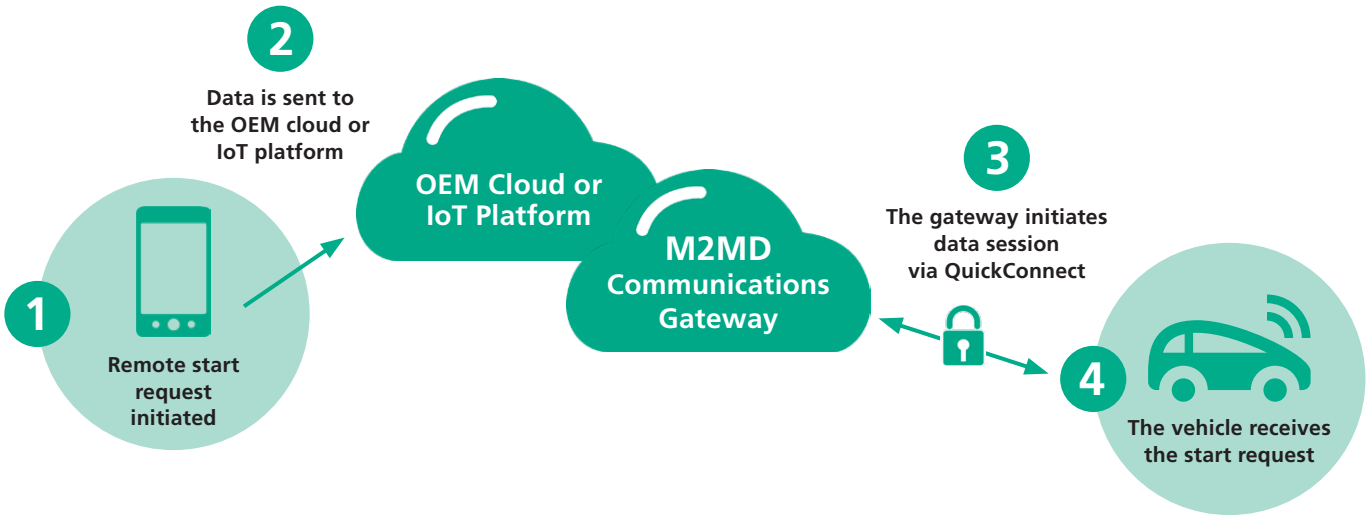
Improved Experience – for drivers and automakers

Designed for interactive use cases, the gateway provides a whole new user experience in terms of responsiveness without sacrificing security. The secure gateway provides the ability to instantly connect to a vehicle. Today's connected cars typically require thirty seconds to receive a mobile command. The M2MD Communications Gateway has reduced this communication time to just a few seconds. For improved connectivity, the M2MD Communications Gateway instantly triggers a network initiated data session to the vehicle, resulting in an immediate response to complete requests for remote control functions (e.g. remote vehicle battery charging status check).
The automakers also benefit from improved connectivity with the vehicle using the M2MD Communications Gateway. This results in an immediate response regarding diagnostic trouble codes. The automaker can analyze the data and make adjustments immediately.

Improved Security

The M2MD Communications Gateway merges M2MD's proprietary security solutions with G+D's expertise in encryption, key management and highly secure hosting capabilities. The gateway provides a secure communications channel between the TCU in the vehicle and a backend platform. The essential cryptographic key material is stored on hardware, utilizing the certified security of the SIM.

The M2MD Communications Gateway strengthens data transmission security and the speed of initiating communications between the vehicle and the automaker's preferred telematics platform. The solution leverages well-tested and standardized security technologies like TLS and 3GPP methods. By using only symmetric cryptography, it avoids the challenges associated with certificates.



To provide always-ready connectivity the M2MD Communications Gateway instantly triggers a data session using the QuickConnect technology. QuickConnect establishes a secure connection within seconds.

Reduce costs with QuickConnect technology

The M2MD Communications Gateway is optimized for embedded devices with low power budgets. The gateway has built-in QuickConnect "wake-up" technology, which requires negligible power consumption by both the vehicle and the device. The car is in an "always ready" state of connection as opposed to being "always-on", which taxes the battery.

The gateway's unique QuickConnect feature establishes a secure connection within seconds – about ten times faster than today's methods. QuickConnect uses minimal mobile data to establish the connection as symmetric cryptography does not require data-heavy keys and certificates. While a single vehicle manages only a single connection, the automotive manufacturers handle thousands of connections through their backend systems. Symmetric encryption requires far less computing time, which greatly reduces the load on the backend platform and thus reduces the cost of managing the connectivity services.

Why the SIM is the best security anchor for automotive connectivity

The SIM has a long history as the trusted element for securing subscriber identity and connectivity credentials for mobile networks. The highly secure, multifunctional SIM or UICC (Universal Integrated Circuit Card) can also act as a security anchor for the horizontal security required for IoT and, in this case, car connectivity.

The UICC is a compact computational device with data storage capability. It is tamper-resistant, and provides a secure repository for critical information. As an independent computing entity inside the connected car, the UICC can store the factory reset configuration in its secure storage and perform supervisory tasks, thus ensuring that cars can be remotely managed as needed.

G+D Mobile Security manages 3+ billion cards across 80 countries. Furthermore, G+D Mobile Security leads the industry in eSIM management, which directly enables secure, over-the-air credential management using remote devices. Globally, G+D has deployed and supports more than 200 over-the-air platforms. Nine of the top ten automotive manufacturers trust G+D Mobile Security to provide UICC hardware, eSIM management software, and secure communications for current and next generation connected cars.

M2MD Communications Gateway Key Features

The M2MD Communications Gateway allows drivers to quickly connect to the vehicle over mobile networks, execute remote commands more rapidly, and enjoy extended battery life. In addition to a more satisfied customer, the automaker benefits from reduced vehicle data costs on the backend.

The solution combines these benefits with G+D Mobile Security's expertise in hardware security, key management, and highly secure hosting capabilities. G+D Mobile Security's market leading M2M SIM expertise and secure data centers that are certified by banking and telecommunications institutions ensure the highest level of security and data privacy for car manufacturers and their customers.

Fast

- < 3 second reaction time, 10 times faster than current solutions on the market

Secure

- Proven and well-known security mechanisms are used (e.g. TLS 1.2)
- Static cryptographic elements are protected by SIM hardware security
- Only session keys are used for operations outside of SIM hardware
- Regular key rollovers reduce the impact of potential attacks

Efficient

- Cost savings: No SMS required, only 304 bytes per connection establishment, 6,000 bytes less than certificate-based methods
- Power savings: Highly optimized embedded solution allows the TCU to be always ready, whereas current solutions have to go offline for periods of time to stay within the vehicle's power budget
- Run-time savings: Fewer CPU operations needed
- Client side: Faster execution, lower CPU requirements
- Server side: Up to 350,000 vehicles per server vs.15,000 clients per server for current solutions
- No additional hardware required, works with all TCUs/modems
- Dual/multi-source SIM strategy possible for automotive manufacturers

Managing identities in a connected world

G+D Mobile Security is a global mobile security technology company headquartered in Munich, Germany. The company is part of the Giesecke+Devrient group. G+D Mobile Security has a workforce of 5,300 employees and generated sales of approximately EUR 868 m in the 2018 fiscal year. More than 40 sales and partner offices as well as 20+ certified production and personalization sites and data centers ensure customer proximity worldwide.

G+D Mobile Security manages and secures billions of digital identities throughout their entire life cycle. Our products and solutions are used by commercial banks, mobile network operators, car and mobile device manufacturers, business enterprises, transit authorities and health insurances and their customers every day to secure payment, communication and device-to-device interaction. G+D Mobile Security is a technology leader in its markets and holds a strong competitive position.

G+D
Mobile Security

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstrasse 159
81677 Munich
Germany

www.gi-de.com/mobile-security
mobilesecurity@gi-de.com

Follow us on:

smart!