G+D Mobile Security

M2MD Technologies, Inc.

Solution Brief

# M2MD Communications Gateway: **fast, secure and 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 solution.
- On average, top-of-the-line, server-supporting, certificate-based security can support only 15,000 devices, driving higher hardware costs and impacting scalability.

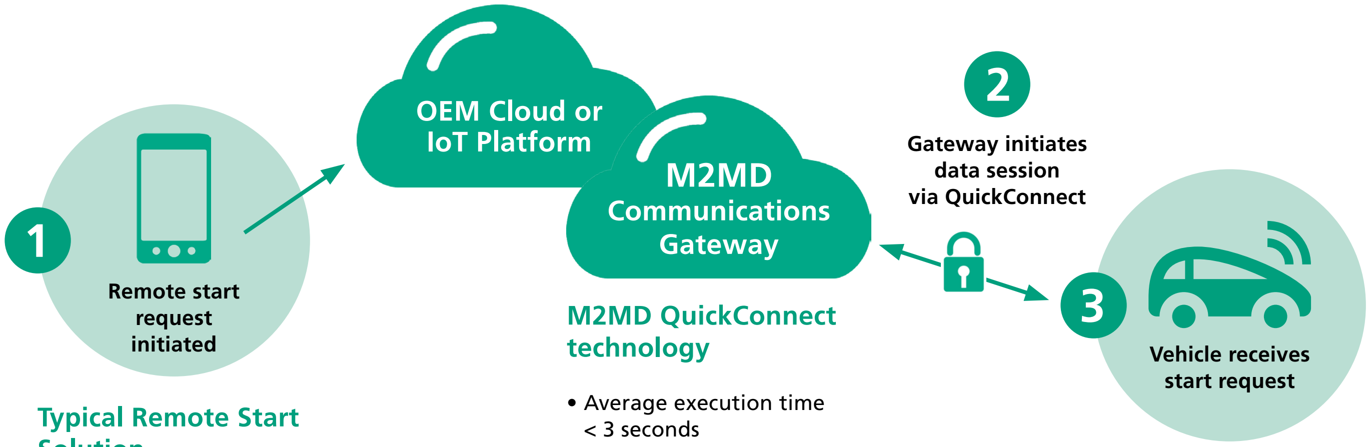
# Improved Experience – for drivers and automakers

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 up to 30 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 analyse 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 symmetric cryptography only, it avoids the challenges associated with certificates.

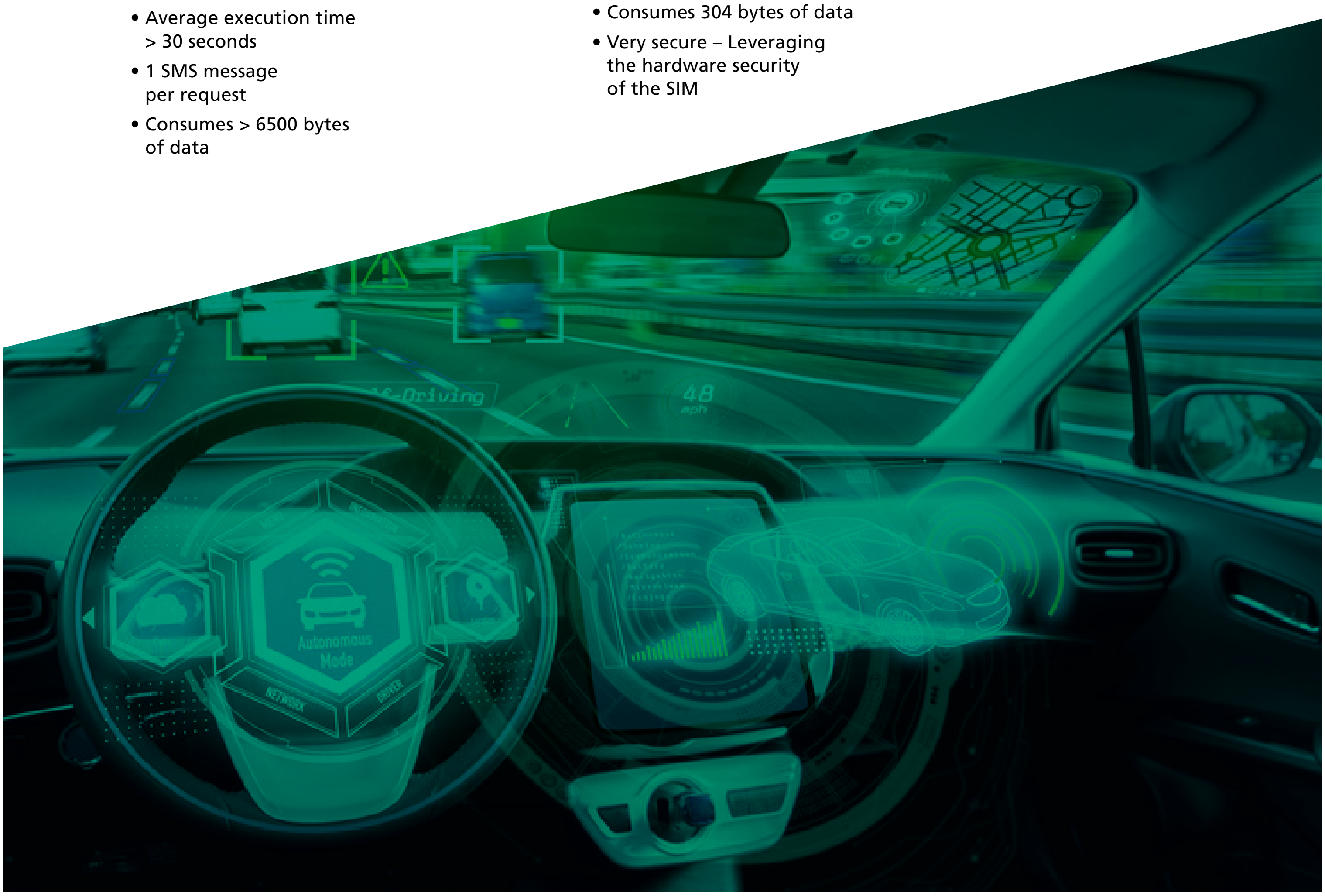

1
Remote start request initiated
OEM Cloud or IoT Platform
M2MD Communications Gateway
2
Gateway initiates data session via QuickConnect
3
Vehicle receives start request

## Typical Remote Start Solution

- Average execution time > 30 seconds
- 1 SMS message per request
- Consumes > 6500 bytes of data

## M2MD QuickConnect technology

- Average execution time < 3 seconds
- No SMS message
- Consumes 304 bytes of data
- Very secure – Leveraging the hardware security of the SIM



## Reduced costs through 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 10x 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 back end.

**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 eSIM hardware security
- Only session keys are used for operations outside of SIM hardware
- Regular key rollovers reduce the impact of potential attacks by providing forward secrecy

**Efficient**

- Cost savings: No SMS required, only 304 bytes for 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 on the market
- 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 provides trustworthy and secure solutions in an everchanging world – whether virtual or physical, online or offline. Our experience in future-proof identity management makes us the perfect partner to enable businesses to satisfy customer demands for quick, convenient and smart services, while ensuring the security of customer identities and data.

## Learn more about G+D Mobile Security automotive solutions

For more information, contact your G+D Mobile Security representative, or visit
https://www.gi-de.com/en/de/mobile-security/industries/automotive/

G+D
Mobile Security

**Giesecke+Devrient**
**G+D Mobile Security, Inc.**
45925 Horseshoe Drive
Dulles, VA 20166
USA

P +1-703-480-2000
mobilesecurity-us@gi-de.com

Visit our automotive solutions website:
https://www.gi-de.com/en/us/mobile-security/industries/automotive/

Connect with us: