infopulse

Case for **Manufacturer of electric cars**

OTA Software Update Solution Concept for Next-Gen Vehicles_

Industry: Automotive

Location: Germany

Client Background

Development of a concept of over-the-air (OTA) solution, which allows distributing software updates over a wireless network without the need of a physical access to a vehicle. A manufacturer can remotely deliver firmware updates, patches, software and data updates to a vehicle removing the need for a driver to contact a dealer or a repair shop.

Business Challenge

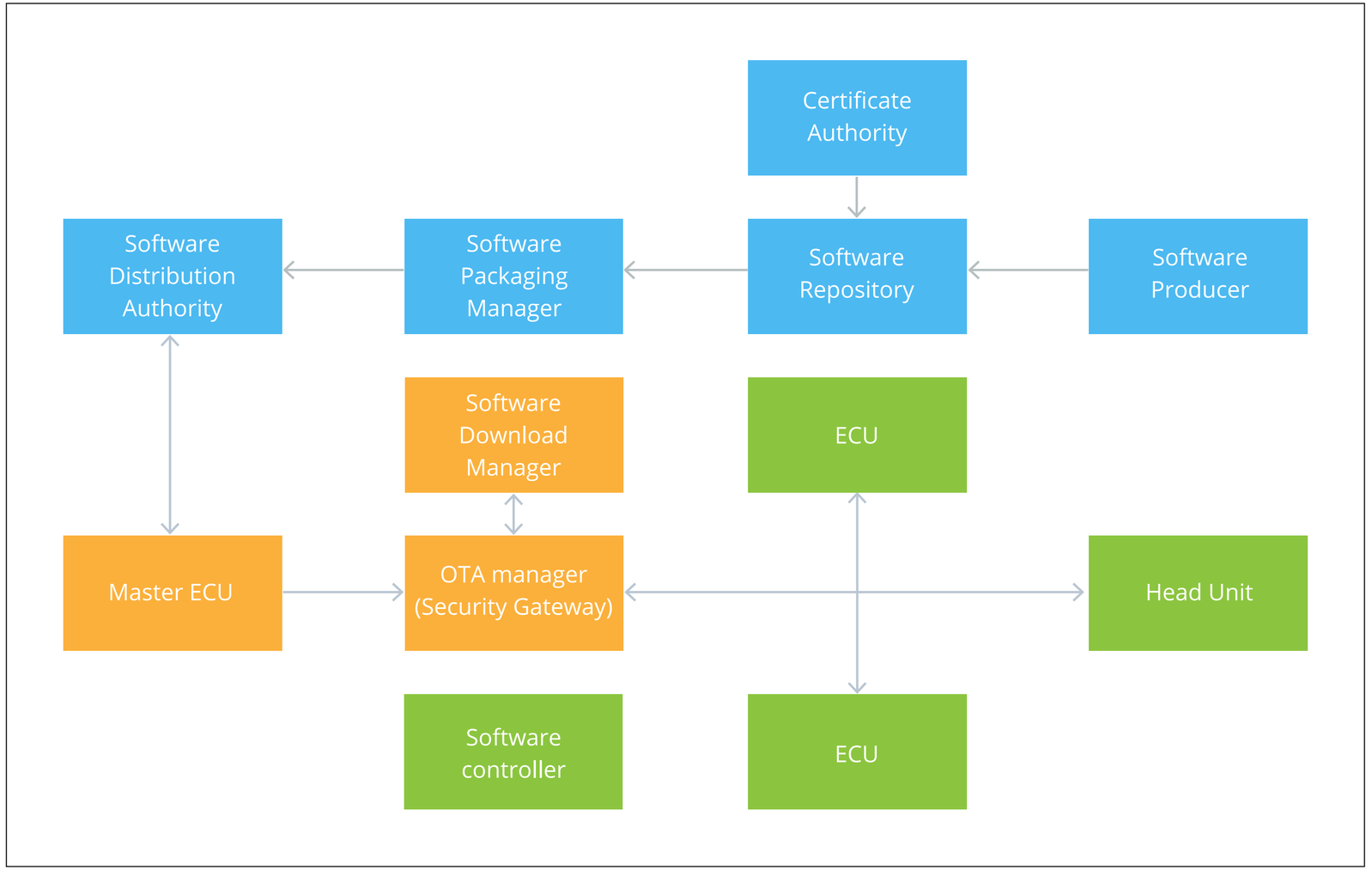
- **Software Update delivery guarantee.** Even when Wi-Fi is not available, critical updates still must be delivered via LTE or 3G network as soon as possible. Solution must enable updates staggering to avoid cellular networks overload, especially when vehicles are often clustered in urban centers.
- **Software Update installation reliability and rollback.** Installation must not fail under any conditions, as there is no personnel to fix it. Thus, engineers of OTA Update follow the highest standard of update reliability by verifying sustainability on every step. If software update is interrupted due to any external factors, a system is designed to roll back to the previous state from the backup.
- **Over-the-air update must be secure.** The goal is to eliminate any issues related to ensuring safe vehicle-to-cloud communications. The team had to figure out how to enable an intact exchange of firmware, software and their meta data between OEM, Tier 1 and the Security Gateway ECU. Moreover, there were also other concerns regarding update package authenticity and integrity (data modification or data forging), authentication, and confidentiality.
- **Fleet management.** Also, the updates must be applied timely to large fleet of vehicles. Special campaigns were designed in order to monitor and control the status of software update distribution among vehicles in respect to model, market and other criteria.

Solution

Development of a concept of over-the-air (OTA) solution, which allows distributing software updates over a wireless network without the need of a physical access to a vehicle. A manufacturer can **remotely deliver firmware updates, patches, software and data updates to a vehicle** removing the need for a driver to contact a dealer or a repair shop.

- Our team has selected the following OTA update flow based on its three key points:
- Generating and storing software versions in the cloud-based Software Repository.
- Uploading OTA required software into the local vehicle storage.
- Installing new software and/or updating ECUs.

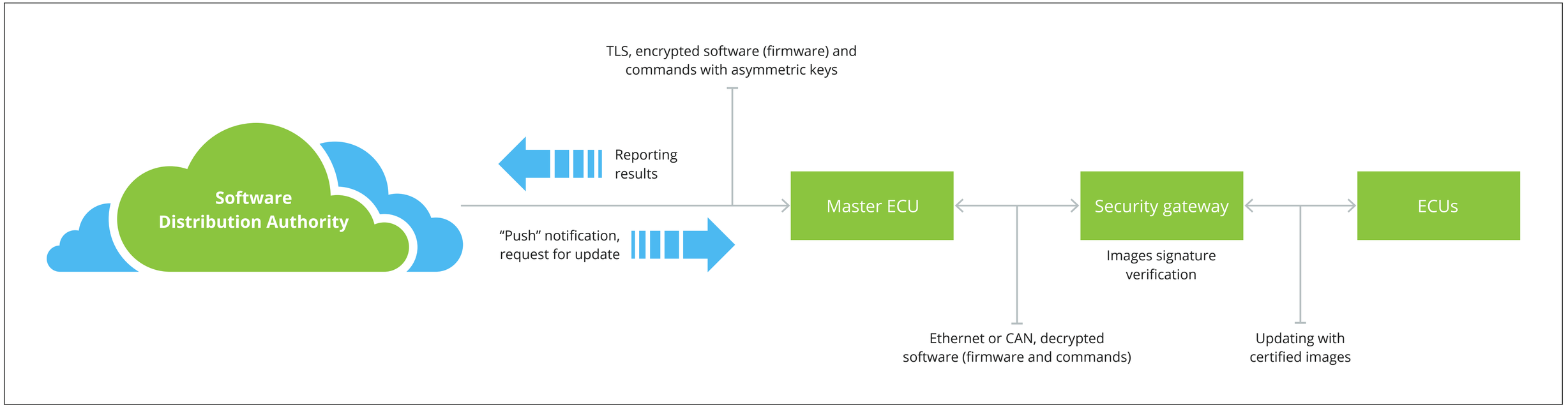
OTA Update Flow



To overcome security challenges the team used the following approach:

- All vehicle-to-cloud communications **are secured by TLS mutual authentication** based on certificates.
- **The authenticity and integrity** of the software is ensured by HMAC, CMAC or Digital Signature of the OEM and other stakeholders. For example, according to Digital Signature Standard (DSS), **any update must be digitally signed** with valid certificate and checked by distributor on all stages.
- **The confidentiality** is protected by the encryption of software update and data based on the asymmetric algorithm before their transmission to or from the cloud.

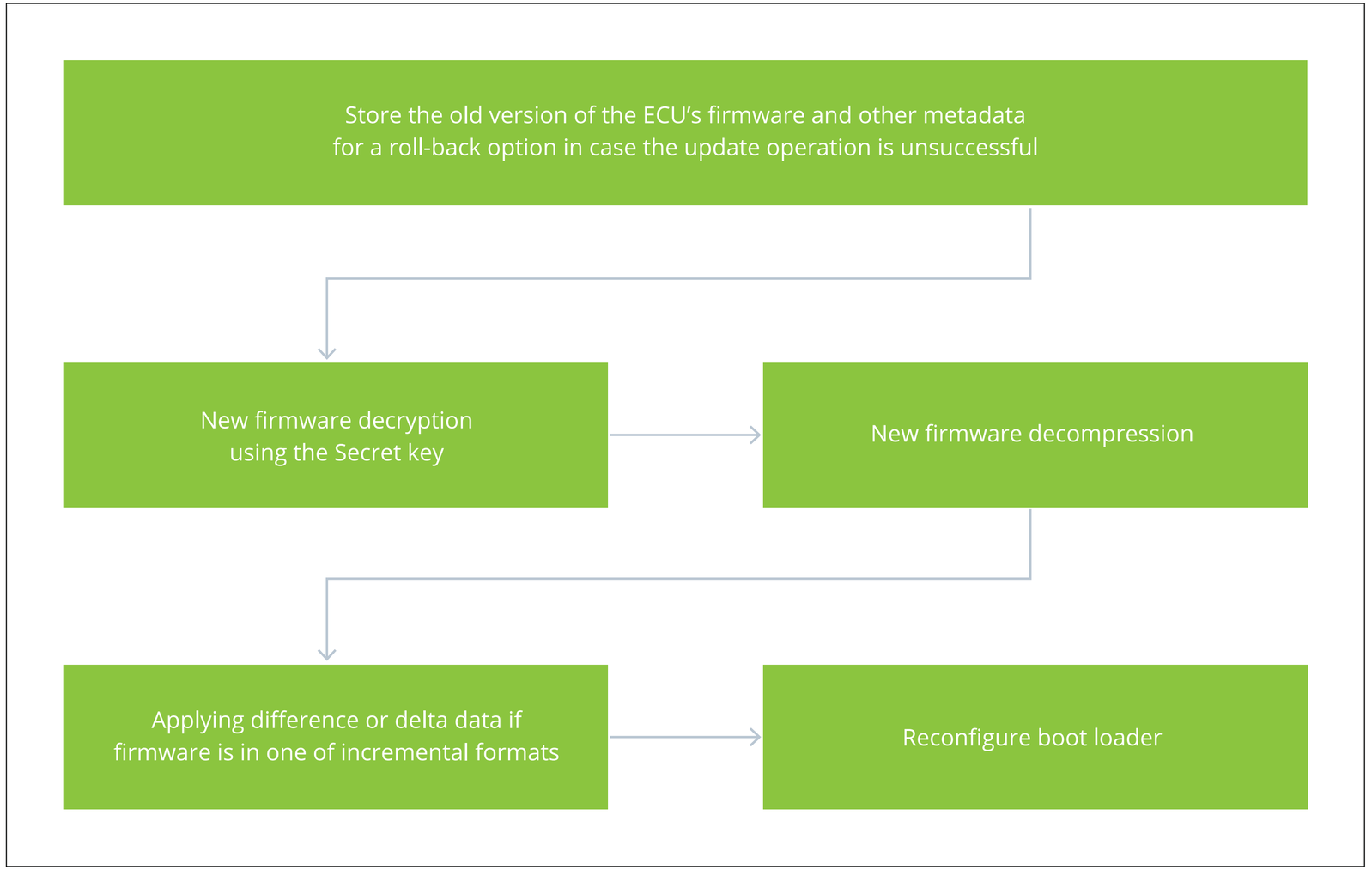
OTA Security Approach



To ensure firmware installation regardless of disruptive factors, the software must be fully downloaded, the vehicle must be parked and the engine turned off. A Special **Diagnosis manager** is introduced as an extension **to verify that the newly updated software operates as expected**. It can also initiate rollback procedure to the previous software version.

Here's how software installation process is organized by our team.

Generic Firmware Installation Process



Technologies

In-vehicle IPC: CommonAPI

Vehicle-to-Cloud IPC: GRPC

Cloud: Azure

HMI: Qt5

Over-The-Air: Wi-Fi

Over-The-Air: LTE

Over-The-Air: 3G

Diagnostic Log and Trace: DLT component (AUTOSAR compliant)

OS: Linux

Arch: ARMv8

Hardware: Renesas R-Car H3 (Raspberry Pi for test purposes)

Business Value

- Automating software-based recalls to resolve software defects
- Upselling new or existing features to increase subscription revenue
- Cost-effective updates of vehicle software and firmware
- Managing much shorter lifecycle of software and firmware
- Tracking ECU software down to the VIN, including software dependencies
- Reducing warranty costs for OEMs
- In-time updates stand for greater flexibility in the supply chain
- Improved vehicle security due to timely keys updating, security libraries updating,
- zero-day vulnerabilities patching
- Enhancing a driver’s satisfaction and brand loyalty

About Infopulse

Infopulse, part of the leading Nordic digital services company Tietoevry, is an international vendor of services in the areas of Software R&D, Application Management, Cloud & IT Operations, and Cybersecurity to SMEs and Fortune 100 companies across the globe. Founded in 1991, the company has a team of over 2,300 professionals and is represented in 7 countries across Europe and the Americas.

Infopulse is trusted by many established brands, such as BICS, Bosch, British American Tobacco, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, Offshore Norge, OLX Group, OTP Bank, SAP, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin Group, and others.

For more information, please visit **www.infopulse.com**

Contact us

PL +48 (606) 291-154

DE +49 (69) 505-060-4719

US +1 (888) 339-75-56

UK +44 (8455) 280-080

UA +38 (044) 585-25-00

BG +359 (876) 92-30-90

BR +55 (21) 99298-3389

info@infopulse.com