Giesecke+Devrient

Solution Brief

Safer Driving with eSIM technology

Implementing vehicle connectivity for safety in the Russian Federation

Fatalities resulting from road traffic accidents cause more than one million deaths per year annually. The ongoing effects of these accidents have a significant economic impact on the victims, their families and nations at a whole.

As connected vehicles become more common, sophisticated sensors and connectivity services can help to prevent accidents. eCall, the automatic emergency response system connects vehicles involved in accidents to emergency services. The positive effect of eCall on safety and resulting economic benefits have led the EU to legislate that all vehicles produced for use in the EU after April 2018 must have eCall systems enabled.

The Russian Federation also has an emergency response system (ERS) in place, implemented over the domestic ERA-GLONASS satellite and communications network. The Russian ERS is similar to the EU's eCall service, but there are significant differences in testing, certification and approval processes, import procedures and in life operation.

The ERA-GLONASS technology

The emergency response service in Russian territories uses the GLONASS satellite positioning system and different cellular networks to manage the connection to the service.

The vehicle detects its position with the satellite positioning system and interacts with domestic cellular services through a SIM loaded with a specific profile that manages authentication and network interface. The SIM makes the call to the 112 ERS over the domestic Russian network. The data is then dealt with appropriately and emergency services are informed. GLONASS report that it takes on average 19 seconds for the information to be transmitted to the emergency services.

eCall at a glance

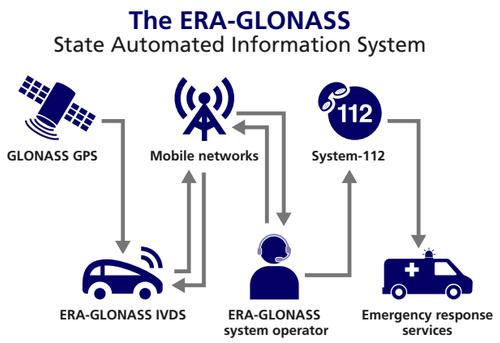
The eCall system that operates over the EU is based on a single European-wide emergency number – 112. In the event an accident is detected by the vehicle, it connects to a local Public Service Answering Point (PSAP). The PSAP receives a pre-determined set of information, transmitted by means of standardized transmission protocols. This Minimum Set of Data (MSD) is forwarded to the most appropriate emergency services and includes:

- Time of incident
- Accurate location of the vehicle
- Likely direction of travel
- Vehicle identification

Vehicles are also fitted with manual eCall buttons so that the driver can report an accident. The SIM profile that enables the service only activates when requested or when an accident is detected, so any potential privacy concerns are alleviated. eCall's quicker, more informed process has a significant impact on the costs of an accident. The European Commission calculates that a fatality averted by prompt eCall response can save over €13,000 per accident.

The Russian ERA-Glonass system is harmonized with the European eCall standards but specifies some extensions to better support the Russian infrastructure.

The accident response procedure



JSC GLONASS manages the State Automated Information System (SAIS). They are responsible for network access in Russia for vehicles using the ERS service. They act as a Mobile Virtual Network Operator (MVNO) for this connectivity.

The profile that governs the access to the ERS service is independent from any other SIM profile already in the vehicle, so multiple profiles loaded on the eSIM, also known as the embedded universal integrated circuit card (eUICC), are needed to access the entire connected experience. Digital profiles loaded on to the eUICC allow multiple connectivity configurations on same chip, seamlessly switching between them.

As the eSIM can be updated OTA, profile updates and additional applet functionality can be applied remotely at any stage of the lifecycle, so your customers will remain secure throughout their ownership of the vehicle. This also helps to reduce costs for manufacturers, as it helps to simplify product development and production.

Certification and approvals
There are two distinct stages to the testing process for approval of any new eCall system:

1. Certification of the In-vehicle emergency call system (IVDS)
The In-vehicle emergency call system (IVDS) goes through several testing processes, but one test stage relates to the testing the eSIM itself. The eSIM must conform to exacting standards set out in the Russian government's GOST specification.

Once the eSIM has been integrated into the new eCall device there is a clearly defined process of testing. The supplier must prove that the profile on the eUICC can be updated over the air. This testing can be done either in a certification lab's system simulator or in the field using a live eSIM management solution and mobile communications network.

The certification testing process examines the OTA capabilities of the eSIM in the device. To pass, the eSIM must demonstrate that it is capable of:

- Downloading additional profile data
- Initializing and activating the additional profile
- Controlling (switching) operator profiles
- Removing the additional profile

2. Certification of the vehicle
The specifications state that the eCall system must also be tested in the actual assembled vehicle. A complete vehicle must therefore be shipped to Russia to demonstrate its effectiveness in accessing the eCall functionality. This process happens after the technology itself has received approval.

This testing process must demonstrate complete ERS functionality. The IVDS must show that it can deal with a crash and automatically contact the change to ERA systems operator. In this full-vehicle test, the IVDS hardware must be identical to that used for initial lab or system tests. For instance, it could be necessary to replace the SIM profiles used in the test environment with profiles used by real MNOs.

Importing vehicles into the Russian Federation

Once successful testing and certification is complete, permission is then sought to import vehicles into Russian territories. There are specific regulations that govern the import and registration of vehicles produced outside Russia. For example, The OEM must supply documentation outlining the vehicles' Profile ID (ICCID), VIN, car model and color. These documents are supplied to customs before the vehicle enters the country.

This information is held to pass onto the ERA-GLONASS call centers in case of accident or emergency as an additional source of identification. For example, if the emergency services know the color of the vehicle, this can speed up response.

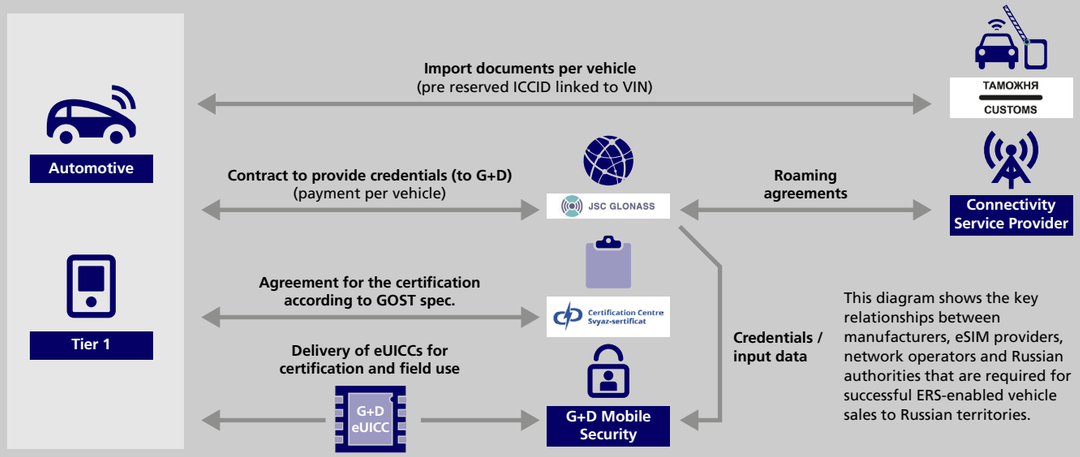
The MNO data, provided by JSC GLONASS to configure the SIM profile for the vehicle to be used in Russia has to be requested by the OEM itself. JSC GLONASS charges a one-time fee per eUICC/vehicle to provide this data.

To complete the import, there are two further phases, affecting both the Tier 1 component manufacturer and the OEM:

1. The activation process of the eUICC
In this phase the OEM and the Tier 1 supplier of the IVDS have to work closely together. The Tier 1 and the OEM must ensure that only ICCIDs for vehicles intended for the Russian market are transmitted.

2. The car activation process
This process is the responsibility of the OEM, who must supply the VIN, ICCID and vehicle color data. For cars produced locally, the information is sent directly to the government, but for cars produced outside Russian territories, this data is sent first to Russian customs, and then on to the government.

The ERA-GLONASS business model



G+D: Your perfect eSIM partner

With decades of mobile security expertise and our global presence, G+D is your perfect partner for vehicles intended for the Russian Federation. We can help you to seamlessly navigate and integrate these complex requirements, as well as helping to streamline your worldwide operations.

G+D can help you realize the potential of eSIM solutions for your business. We are global leader in eSIM management solutions, with every 3rd connected car worldwide connecting to a network through G+D technology. Building on our core competencies of experience, interoperability and standardization, we've built effective and lasting relationships throughout every stage of the device production process, from silicon vendors all the way through to the end user.

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.

Giesecke+Devrient

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstrasse 159
81677 Munich
Germany

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

Follow us on: