© The investment is financed by the Republic of Slovenia and the European Regional Development Fund. Copyrights governed by the Consortium Agreement 5G Varnost.

5G Safety - Phase 1 Industrial Research, Sub-phase IR.3

Report on Security and Integrity

Result IR.11, Task T.3.4 End-to-end Security and Integrity

Tip dokumenta	Result (Deliverable)
Zapis v arhivu	5GVAR-IR3-R11-Public
Narejeno za	5G Safety
Avtor	Iskratel, d.o.o., Kranj, OSI d.o.o., Univerza v Ljubljani, Fakulteta za elektrotehniko, Telekom Slovenije d.d.
Stopnja zaupnosti	Public

Obr.: 78-089c

© The investment is financed by the Republic of Slovenia and the European Regional Development Fund. Copyrights governed by the Consortium Agreement 5G Varnost.

1. Abstract

The summary is prepared based on document IR.11: Integrated perspective on security and defining security aspects within the framework of the project 5G Safety, which is the result of activity T.3.4.
Presented are approaches, solutions and technologies which are based on widely accepted standards and best practices from the field of information security. The document summarizes necessary and recommended measures for ensuring information and cyber security of such an important system as 5G Safety and describes concrete measures, which are put into practice in the project itself.
In the first part of the document there is a general presentation of measures for managing information security. Legislative frameworks and standards are outlined, with particular emphasis on the area of 5G and ensuring security in the area of critical infrastructure, where PPDR obviously belongs. For achieving high level of information security of such a complex system, it is necessary to use the appropriate framework and tools which ensure that all the aspects of security are taken into account. Standard ISO/IEC 27001 is one of the most widely used basic frameworks of information security, since it is appropriate for wide specter of systems and services. For individual subsystems we can use also other standards, e.g. ISO/IEC 27032, ISA/IEC62443 or NIST standards as an extension or addition. In case of a production environment, it is advisable to establish also own measures and standards, which summarize the mentioned standards, are lighter or stricter than the controls in the mentioned standards, depending on the identified risks. For the needs of the project 5G Safety we rely on standard ISO/IEC 27001/27002 and on ENISA recommendations for cybersecurity of 5G networks.
The fifth chapter is dedicated to threat modelling. The model of threats was made through theoretical frameworks for specific example of PPDR application, then the model was used in the demonstration environment and threats were determined. The model of threats itself was produced with the help of UML diagrams, on the base of which we analyzed the particular installation in the demonstration environment. The result of the analysis are guidelines given for improving cybersecurity and resilience.
A special chapter is dedicated to ensuring security in 5G network. Examined are all aspects of security, from 5G core infrastructure, RAN network, to 5G access network. Given are also guidelines related to the safety of integration of 5G terminals in the network and mechanisms of access control.
Yet another chapter is dedicated to security aspects of the application development. We reviewed the process of safe development and the existing control mechanisms. Bearing in mind the characteristics of 5G Safety project, there was strong focus on the development of mobile applications, due to the fact that the 112 application was developed within the project framework. Risk assessment was also carried out, threats were identified and security screening of the application was done. On the basis of this, guidelines were given which need to be respected upon further development of the application.
The last part of the document is dedicated to ensuring operational safety. Given are guidelines for building the Security Operation Center. The methodology for performing penetration tests is also described. The system for operational management of incidents and vulnerability search is presented, which was installed and tested in the demonstration environment. The system for recording audit trails, based on blockchain cryptographic methods, was also implemented and validated in the demonstration environment.

© The investment is financed by the Republic of Slovenia and the European Regional Development Fund. Copyrights governed by the Consortium Agreement 5G Varnost.