The Ericsson Security Reliability Model
Introduction

Security and privacy continue to be the cornerstones of digital agendas and ICT policies for information technology and telecom companies around the world. Citizens and governments have high and legitimate expectations that companies – especially those developing or operating critical infrastructure – will address security and privacy concerns appropriately.

To succeed in this difficult and quickly evolving landscape, the whole ecosystem of industries, operators and vendors must mature, understand the challenge of this new environment and embrace solutions to mitigate the threats. For this reason, Ericsson has developed a framework, which sets the product security and privacy ambition level, promotes the security and privacy by design attitude, and follows up actual product security in all our deliverables.

The Security Reliability Model

For many years, Ericsson has systematically developed a state-of-the-art model to incorporate security and privacy considerations into all phases of product development. The result of this effort is a well-established internal governance framework for security and privacy by design called SRM.

SRM is the framework that Ericsson uses to deliver on security and privacy ambitions across the product portfolio. Its key characteristics are:

— Defining the product security and privacy ambition level;
— Ensuring the implementation of appropriate security and privacy features and functions;
— Following up and measuring actual product security and privacy status; and

Ericsson’s internal directive defines how responsibilities and authorities are distributed between different roles and functions to ensure, manage and control product security and privacy across Ericsson product portfolio.

Functions

The Security Reliability Model, or SRM, defines a set of security and privacy baseline requirements for Ericsson products. Those requirements are the result of decades of experience and they also come from inside the telecom and IT industry, including from company standards, customer policies and regulations.

The product organization responsible for each Ericsson product will analyze, decide and document the applicability and compliance to the given security and privacy requirements, with a risk-based approach. A Risk Assessment and Privacy Impact Assessment process is then used to identify and prioritize a list of the security and privacy functions required to mitigate risks to an acceptable level.
Assurance

Assurance activities are divided into three levels: basic, advanced, and tailored. All basic level assurance activities relevant to the product shall be performed by product development. Advanced level assurance activities can be performed for parts of products that require high security and privacy. Tailored level activities are used for products, or parts thereof, where product specific assurance requirements exist.

The most prominent assurance activities leveraged by Ericsson are: Risk Assessments, Privacy Impact Assessments, Secure Coding practices, Vulnerability Analysis and Hardening.

- A Risk Assessment and Privacy Impact Assessment will identify risks related to the product when used in the customer’s network. The assessment will also identify the privacy risks related to the individuals, such as subscribers, when their personal data is processed. As a result, a risk treatment plan is created to define the security and privacy mechanisms needed to protect the identified information assets. The plan is implemented in accordance with Ericsson security and privacy design rules.

- By following secure coding best practices, Ericsson reduces design weaknesses and implementation bugs during software development. Secure coding activities aim to reduce flaws and weaknesses in the software code through code reviews and selected static and dynamic code analysis tools.

- The Ericsson way of performing Vulnerability Analysis, also called Vulnerability Assessment, comprises the testing and verification (including penetration testing) activities designed to identify weaknesses and vulnerabilities present in the product or solution. The vulnerability analysis verifies security characteristics and security configuration of the system under test and identifies vulnerabilities through both black box and white box testing. A Vulnerability Analysis verifies that Risks discovered in the Risk Assessment activity are sufficiently mitigated in the final product. Vulnerabilities that are found are handled according to the trouble report process before the product’s release.

- Hardening means increasing product security by reducing its attack surface. Hardening is relevant both for design and configuration, and for deployment. Hardening ensures that the product is configured in a manner that minimizes the risk of unauthorized access, including system compromise. Hardening includes, for example, removal of unnecessary software, installation of the latest patches, disablement of insecure services and replacement of default passwords.

We have also included training as part of the security assurance activities. The relevant modules of instruction have been selected and time has been allocated for people to take the training because we believe that continuous learning is an important part of secure product development.

Documentation


SRM documentation allows the customers to know what security functions are available on the product and how to configure them to achieve and maintain security and privacy compliance. The documentation informs customers about which assurance activities were performed on the product and it communicates other sensitive aspects related to operating the product, like the impact on privacy and the processed personal data.
Product Near Security Services

Ericsson’s product-near security services are handled separately by the service organizations and are independently defined by the products.

Typical deliverables are security and privacy training recommendations, solution level integration guidance, international data flow handling and potential deployment-time hardening activities that need to be included in customer delivery projects.

Security activities do not end when the product or service has been deployed and taken into use. Ericsson monitors constantly new vulnerabilities disclosed and verifies if there is an impact on any Ericsson product or service. Ericsson PSIRT (Product Security Incident Response Team) is responsible for Ericsson product vulnerability management process, coordination of customer product security incidents and reported security issues affecting Ericsson products, solutions, and services. We strongly believe in the principles of responsible vulnerability disclosure to all parties involved.

SRM in the supply chain

Over the last few years, dramatic shifts in cyber security and privacy landscape have taken place. The demand for vendors to show evidence of a trustworthy supply chains to customers, regulators and national security organizations has increased significantly. Ericsson has taken up the effort of addressing the challenge of the security of various supply chains. The entire supply chain must be secured, starting from the selection of third-party vendors all the way through to the deployment and patching of our products on the customer’s premises. This requires the identification of the gaps to have a holistic and end-to-end management of the security of supply chain for both software and hardware. Ericsson sees this as one of the fundamental enablers of building trust into our customers’ networks.

SRM as a key enabler of the Trust Stack

Security and privacy are at the top of the digital industries’ list for needs and requirements. 5G, IoT and Cloud are introducing new actors; new models for business and continued trust need to be considered. Trust is needed for collaboration and partnering. Trust is also needed during the selection of providers, products, vendors, and manufacturers. Trusted business is based on ambitions and strategies, customers’ needs and expectations, partner capabilities, and standards and regulations.

From a trust stack perspective, the Ericsson Security Reliability Model addresses the core challenges of software product development. It provides a best-in-class framework for security and privacy by design. Trusted hardware and software products are the fundamental building blocks of trusted networks. When products are designed with security and privacy in mind, it will also be possible to successfully deploy them to build secure networks. This will enable secure network operations and it will also enable a trusted business relationship between operators, subscribers, and consumers.

Example of the SRM in the development process

Completion of the various phases of the Security Reliability Model is an essential part of the development of all Ericsson hardware and software products. The process is typically initiated well in advance the release of a major product and the SRM framework clearly defines the activities to be performed, including inputs, outputs and supporting guidelines.

Figure 2 - The Trust Stack
If we could see a product going through the risk assessment and privacy impact assessment process under SRM, it would look like this in the graphic below:

Security Assessment and Privacy Impact Assessment Process

Start

Activity
- Asset identification, Data Classification
- RA/PIA workshop#1
- RA/PIA workshops
- Communication to Ericsson PSIRT

Output
- Product sensitivity calculation
- Preliminary RA/PIA report
- Final RA/PIA report

Templates
- Product sensitivity calculation
- RA/PIA report templates

Support
- Product Security knowledge base
- Product Privacy knowledge base
- SRM guidelines

Baseline Security and Privacy Requirements

High sensitivity
- Privacy User Guide is mandatory
- Sensitive business process

Select applicable SRM Functions
Select applicable SRM Assurance
Select applicable SRM Documentation

Security and Privacy by design execution

Figure 3 – The Risk Assessment and the Privacy Impact Assessment process in SRM
The starting point of the process is always the identification of the product or asset to be protected and the sensitivity of the data to be processed through that same product or asset. The product release or the new feature is analyzed through the Risk Assessment and the Privacy Impact Assessment process. Its sensitivity is assessed, and a calculation is made to determine its potential impact on privacy. Utilizing the baseline security and privacy requirements as input, one or more security and privacy workshops are run, led by security and privacy experts in the area, and a preliminary Risk Assessment/Privacy Impact Assessment is produced and used to highlight potential risks and to propose measures to mitigate those risks.

The Security Reliability Model also mandates that a privacy user guide is included in customer documentation for sensitive products or for products with new sensitive features.

After several workshops, the process is concluded, and the result is communicated to product management, who then take ownership of the proposed risk mitigations, as well as to Ericsson PSIRT for risk management purposes. At this point, product management can add the proposed security and privacy functions to the product backlog.

Assurance levels in SRM

Different levels of assurance are needed depending on the risk level and the sensitivity of the product. SRM defines a set of security assurance activities, dividing them in three levels: Basic, Advanced, and Tailored.

While Basic-level activities are performed by all product development, Advanced and Tailored-level activities are performed for parts of products with need for higher security or privacy assurance level or where specific assurance requirements exist.

How SRM supports customer compliance

Supporting Ericsson customers to achieve compliance with relevant laws and regulations is one of the key drivers and major reasons of existence of SRM. Products and technology can enable achieving and maintaining compliance when the relevant features and functions have been built into the software, and the corresponding assurance activities have been executed.

Impact of applying SRM

The continuous development and application of SRM is crucial for Ericsson to deliver on the legitimate expectation of customers, regulators and society around issues of security and privacy.

SRM ensures that:
- Product security and privacy gaps are identified early, ideally during the conception phase of a new product or feature. This allows us to control the direction of product development towards secure implementation
- Relevant security and privacy requirements are considered during the product design phase, which allows a secure implementation on a risk-based approach
- The products deployed in the field are free from unacceptable risks, so security and privacy incidents are avoided. The security and privacy assurance of work done is documented and the outcome is known and used for improvements in subsequent releases, as part of the product roadmap
- The customer is informed about the security and privacy aspects of the product via appropriate CPI documentation. This allows Ericsson customers to operate Ericsson products in a secure way and ensure better compliance to relevant privacy laws and regulations, such as the European Union’s General Data Protection Regulation.
Ericsson is one of the leading providers of Information and Communication Technology (ICT) to service providers, with about 40% of the world's mobile traffic carried through our networks. We enable the full value of connectivity by creating game-changing technology and services that are easy to use, adopt and scale, making our customers successful in a fully connected world. For more than 140 years, our ideas, technology and people have changed the world: real turning points that have transformed lives, industries and society as a whole.

Read more on www.ericsson.com