ERICSSON

Baseline Product Security Requirements for Suppliers

BPSRS

Instruction

Preface

The Ericsson Baseline Product Security Requirements for Suppliers represent the minimum product security and privacy requirements that the Supplier, its affiliates, sub-suppliers and their Personnel must adhere to when delivering products to Ericsson.

The Supplier shall ensure that any additional requirements regarding security and privacy required as part of contractual agreements and applicable laws and regulations are also complied with. More detailed requirements will be specified in the Technical Specification in connection with the supplier agreement.

This document undergoes reviews on a regular basis and will be updated from time to time.

Contents

1 Baseline Product Security and Privacy Requirements for Suppliers

Supplier shall provide secure products when delivering to Ericsson, by implementing applicable controls as set forth in this Document.

The product security and privacy requirements presented in this document are the minimum product security and privacy requirements that the suppliers must adhere to when delivering hardware products, software products or any combinations thereof (herein "products") to Ericsson. These baseline security and privacy requirements will be complemented with additional product security and privacy requirements for a specific product or service, specified in the Technical Specification.

Communications to Ericsson regarding security incidents and new vulnerabilities shall be made to the Ericsson Product Security Incident Response Team ("PSIRT") at: psirt@ericsson.com.

2 General security requirements

2.1 Vulnerability disclosure

Supplier shall inform Ericsson PSIRT if they discover new security vulnerabilities or security incidents in their products delivered or to be delivered to Ericsson, including security incidents impacting the design, development, manufacturing, delivery, installation or use of such products.

2.2 Security Assurance

Supplier shall according to what Ericsson reasonably request:

a. adhere to a documented secure development process. This process may be supplier specific;

b. continuously educate its staff on security related topics;

c. provide the technical security expert contact information to the contact person at Ericsson;

d. have a risk management process as part of the secure development process including threat analysis, risk assessments and risk treatment plan on products and services;

e. follow secure coding practices, in particular code configuration management, static code analysis and code peer review;

f. perform vulnerability analysis including penetration testing;

g. perform hardening.

3 Security requirements for products

3.1 Ways of working

These requirements specify how the product shall be developed and maintained, and how the product shall be documented.

3.1.1 Supply chain integrity

Supplier shall provide Ericsson with a bill of materials of products and country of their origins at the latest when they are delivered to Ericsson or its customer.

3.1.2 Security Assurance

Supplier shall according to what Ericsson reasonably request:

a. specify and document security features and architecture for products;

b. specify and document third party software components used and their respective version numbers (both open source and proprietary components), and upon request provide Ericsson with a software bill of materials, in a form advised by Ericsson, for all software that is to be delivered to or be made available for use by Ericsson or its customer;

c. have a user manual for security configuration and hardening;

d. have a process for handling security patches and updates.

3.1.3 Documentation

Supplier shall deliver to Ericsson product documentation containing a user manual/guide for security and possibly other product documents that cover

a. all features, commands and services in the product;

b. hardening and troubleshooting functionality;

c. any other functionality/information that is necessary for the secure management of the product.

Supplier shall deliver the documentation according to what Ericsson reasonably require and at agreed times, or on request by Ericsson.

3.2 Features

Detailed functional security requirements on the products will be specified and agreed in the Technical Specification. The detailed functional security requirements encompass basically the following six functional areas. Examples of requirement topics for each functional area are also outlined below to illustrate the potential detailed requirements.

3.2.1 Network protection

This functional area covers requirements on e.g. confidentiality and integrity protection of O&M traffic and traffic separation.

3.2.2 Identity and access management

This functional area covers requirements on e.g. O&M user ID administration, password management and user authentication and authorization.

3.2.3 Logging

This functional area covers requirements on e.g. security event logging, support for both local and remote logging and full personal accountability.

3.2.4 Data protection

This functional area covers requirements on e.g. protection of passwords, and confidentiality and integrity of personal data.

3.2.5 Application security

This functional area covers requirements on e.g. web application security and secure default values of parameters.

3.2.6 Platform security

This functional area covers requirements on e.g. software signing.

4 Product privacy requirements

4.1.1 Assurance

Supplier shall according to what Ericsson reasonably request:

a. perform privacy impact assessment on the product;

b. report to Ericsson whether the products or services delivered to Ericsson are capable of processing personal data. If that is the case, the supplier must specify what personal data can be processed. Personal data means data that can be used to identify an individual person, e.g. demographics, MSISDN, IMEI, location, and IP addresses;

c. specify and document the privacy features in the products;

d. provide the technical security and privacy expert contact information to the contact person at Ericsson.

4.1.2 Documentation

Supplier shall deliver to Ericsson product documentation that covers all privacy features and commands. Supplier shall deliver the documentation at agreed times, or on request by Ericsson.

4.2 Features

Detailed functional privacy requirements on the products will be specified and agreed in the Technical Specification. The detailed functional privacy requirements encompass, but may not be limited to, the following three functional areas. Examples of requirement topics for each functional area are also outlined below to illustrate the potential detailed requirements.

4.2.1 Personal data classification

This functional area covers requirements on e.g. classification of personal data.

4.2.2 Fair data processing

This functional area covers requirements on e.g. personal data tagging.

4.2.3 Personal data management

This functional area covers requirements on e.g. personal data retention.

5 Compliance

Without limiting other rights of Ericsson or obligations of supplier according to the supplier agreement entered into:

a. Supplier internal audits and/or assessments concerning security and privacy shall be performed by supplier regularly by trained personnel and findings shall be evaluated for possible corrective actions and reported without delay to Ericsson if they are likely to have any negative impact on Ericsson or its customers.

b. Upon 10 days' request from Ericsson, supplier shall be able to demonstrate compliance with this document and any other security and privacy requirements or measures that have been agreed with Ericsson. Identified non-compliances shall be corrected promptly without additional cost to Ericsson

6 Definitions

For the purposes of this document, the following words and expressions shall have the meaning assigned to them below unless the context would obviously require otherwise.

Technical Specification	A set of detailed requirements for a specific product or service, which complement the frame agreement requirements in this document. The Technical Specification is part of the supplier agreement between the supplier and Ericsson.