

## System Description and Risk Analysis

[illegible]

Page limit: 30 pages.

# Contents

<b>1</b>	<b>System Characterization</b>	<b>2</b>
1.1	System Overview . . . . .	2
1.2	System Functionality . . . . .	2
1.3	Security Design . . . . .	2
1.4	Components . . . . .	2
1.5	Backdoors . . . . .	3
1.6	Additional Material . . . . .	3
<b>2</b>	<b>Risk Analysis and Security Measures</b>	<b>3</b>
2.1	Assets . . . . .	3
2.2	Threat Sources . . . . .	3
2.3	Risks Definitions . . . . .	3
2.4	Risk Evaluation . . . . .	3
2.4.1	<i>Evaluation Asset X</i> . . . . .	4
2.4.2	<i>Evaluation Asset y</i> . . . . .	4
2.4.3	Detailed Description of Selected Countermeasures . . . . .	4
2.4.4	Risk Acceptance . . . . .	4

*Recall the following guidelines when writing your reports:*

- *Adhere to the given templates.*
- *Refer to the security principles in the book for justification.*
- *Use clear terminology:*
  - *secure = confidential + authentic. Be clear about which properties you are writing.*
  - *Are pairwise distinct: certificate, private key, public key, archive to of certificate with private key. Please avoid mixing these up.*
- *Refer to the source document of your risk definitions if appropriate.*
- *For the risk evaluation, formulate the threats in active, not passive, voice: who (threat source) does what (threat action)?*
- *Use a spell checker before hand-in!*

## 1 System Characterization

### 1.1 System Overview

Describe the system's mission, the system boundaries, and the overall system architecture, including the main subsystems and their relationships. This description should provide a high-level overview of the system, e.g., suitable for managers, that complements the more technical description that follows.

### 1.2 System Functionality

Describe the system's functions.

### 1.3 Security Design

Describe the system's security design, including access control, key and session management, and security of data at rest and in transit.

### 1.4 Components

List all system components and their interfaces, subdivided, for example, into categories such as platforms, applications, data records, etc. For each component, state its relevant properties.

## 1.5 Backdoors

Describe the implemented backdoors.

**Hide this subsection in the version handed over to the reviewing team by setting the flag `showbackdoors` at the top of this document to `false`.**

## 1.6 Additional Material

You may have additional sections according to your needs.

# 2 Risk Analysis and Security Measures

## 2.1 Assets

Describe the relevant assets and their required security properties. For example, data objects, access restrictions, configurations, etc.

## 2.2 Threat Sources

Name and describe potential threat sources (*not* threats!) including their motivation.

## 2.3 Risks Definitions

Define likelihood, impact and risk level using the following three tables.

Likelihood		Impact	
Likelihood	Description	Impact	Description
High	...	High	...
Medium	...	Medium	...
Low	...	Low	...

Risk Level			
Likelihood	Impact		
	Low	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

## 2.4 Risk Evaluation

List all potential threats and the corresponding countermeasures. Estimate the risk based on the information about the threat, the threat sources and the corresponding countermeasure. Adhere to the risk definitions you have given above. As a sanity check, there should be at least one high-risk entry.

#### 2.4.1 Evaluation Asset X

Evaluate the likelihood, impact and the resulting risk, *after implementation of the corresponding countermeasures*. Formulate the threats in active, not passive, voice: who (threat source) does what (threat action)?

No.	Threat	Countermeasure(s)	L	I	Risk
1	...	...	<i>Low</i>	<i>Low</i>	<i>Low</i>
2	...	...	<i>Medium</i>	<i>High</i>	<i>Medium</i>

#### 2.4.2 Evaluation Asset y

No.	Threat	Countermeasure(s)	L	I	Risk
1	...	...	<i>Low</i>	<i>Low</i>	<i>Low</i>
2	...	...	<i>Medium</i>	<i>High</i>	<i>Medium</i>

#### 2.4.3 Detailed Description of Selected Countermeasures

Optionally explain the details of the countermeasures mentioned above.

#### 2.4.4 Risk Acceptance

List all medium and high risks, according to the evaluation above. For each risk, propose additional countermeasures that could be implemented to further reduce the risks.

No. of threat	Proposed additional countermeasure including expected impact
...	...
...	...