Contents

Chapter 1

Metadata: Common Criteria Security Target

Document-ID: 0000
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

1.1 Handbook Information

Handbook Title: Common Criteria Security Target (ISO/IEC 15408)
Organization: {{ meta.organization }}
Author: Andreas Huemmer [andreas.huemmer@adminsend.de]
Creation Date: {{ meta.date }}
Version: {{ meta.version }}
Scope: {{ meta.scope }}

1.2 Purpose

This Security Target (ST) documents the security properties of the Target of Evaluation (TOE) according to ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation). It describes the security functions, security objectives, and security requirements of the TOE as well as the Evaluation Assurance Level (EAL).

1.3 Target Audience

- Evaluators and certification bodies
- Product developers and security architects

- Customers and procurers of security-critical IT products
- Auditors and compliance officers

1.4 Document Structure

The Security Target follows the structure of ISO/IEC 15408-1:2022 and includes:

1. **ST Introduction** - Introduction, TOE overview, conformance claims
2. **TOE Description** - Detailed description of the evaluation object
3. **Security Problem Definition** - Threats, organizational security policies, assumptions
4. **Security Objectives** - Security objectives for TOE and environment
5. **Security Requirements** - Functional and assurance requirements (SFR, SAR)
6. **TOE Summary Specification** - Summary of security functions
7. **Appendices** - PP conformance, rationale, glossary

1.5 Usage Notes

- All `[TODO]` placeholders must be replaced with specific information
- Placeholders in `{{ source.field }}` format are automatically populated from data sources
- Diagrams can be stored in the `diagrams/` subdirectory
- The ST must be consistent with the chosen Protection Profile (PP)
- All security requirements must be derived from ISO/IEC 15408-2 and 15408-3

Document History:

Version	Date	Author	Changes
{{ meta.version }}	{{ meta.date }}	Andreas Huemmer [andreas.huemmer@adminsend.de]	Initial version

ewpage

Chapter 2

ST Introduction

Document-ID: 0010
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

2.1 1. ST Identification

2.1.1 1.1 ST Title

ST Title: [TODO: Full title of the Security Target]
ST Version: {{ meta.version }}
ST Date: {{ meta.date }}

2.1.2 1.2 ST Author

Author: Andreas Huemmer [andreas.huemmer@adminsend.de]
Organization: {{ meta.organization }}
Contact: [TODO: Contact information]

2.1.3 1.3 TOE Identification

TOE Name: [TODO: Name of the Target of Evaluation]
TOE Version: [TODO: Version of the TOE]
TOE Developer: [TODO: Manufacturer/Developer]
TOE Type: [TODO: Product type, e.g., Firewall, Smartcard, Operating System]

2.2 2. ST Overview

2.2.1 2.1 Purpose

This Security Target (ST) describes the security properties of [TODO: TOE Name] according to ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation). The ST serves as the basis for the evaluation and certification of the TOE.

2.2.2 2.2 Scope

The ST includes: - Physical and logical description of the TOE - Definition of security problems (threats, OSPs, assumptions) - Security objectives for TOE and environment - Security requirements (SFRs and SARs) - Summary of security functions - Rationales for all relationships

2.2.3 2.3 Intended Readership

This ST is intended for: - Evaluators and certification bodies - Product developers and security architects - Customers and procurers - Auditors and compliance officers

2.3 3. ST Reference

2.3.1 3.1 ST Identification

ST Reference: [TODO: Unique reference, e.g., ST-PRODUCT-v1.0]
ST Registration: [TODO: Registration number with certification body]

2.3.2 3.2 TOE Reference

TOE Reference: [TODO: Unique TOE reference]
TOE Platform: [TODO: Hardware/Software platform]
TOE Delivery: [TODO: Delivery form, e.g., Software download, Hardware device]

2.4 4. Document Organization

2.4.1 4.1 ST Structure

The ST is structured as follows:

1. **ST Introduction** (this document) - Introduction and identification
2. **TOE Description** - Detailed description of the TOE
3. **Security Problem Definition** - Threats, OSPs, assumptions
4. **Security Objectives** - Security objectives
5. **Security Requirements** - SFRs and SARs
6. **TOE Summary Specification** - Security functions
7. **Appendices** - PP conformance, rationales, glossary

2.4.2 4.2 Document Conventions

- **SFR**: Security Functional Requirement
- **SAR**: Security Assurance Requirement

- **TOE**: Target of Evaluation
- **TSF**: TOE Security Functionality
- **PP**: Protection Profile
- **EAL**: Evaluation Assurance Level

2.5 5. Related Documentation

2.5.1 5.1 Common Criteria Documentation

- ISO/IEC 15408-1:2022 - Introduction and general model
- ISO/IEC 15408-2:2022 - Security functional components
- ISO/IEC 15408-3:2022 - Security assurance components
- Common Methodology for Information Technology Security Evaluation (CEM)

2.5.2 5.2 Protection Profiles

[TODO: List of relevant Protection Profiles, if applicable] - PP Name: [TODO] - PP Version: [TODO] - PP Registration: [TODO]

2.5.3 5.3 TOE Documentation

[TODO: List of TOE documentation] - User Guide: [TODO] - Administrator Guide: [TODO] - Security Guide: [TODO] - Installation Guide: [TODO]

2.6 6. Revision History

Version	Date	Author	Changes
{{ meta.version }}	{{ meta.date }}	Andreas Huemmer [andreas.huemmer@adminsend.de]	Initial version
[TODO]	[TODO]	[TODO]	[TODO: Description of changes]

Next Steps: 1. Complete all [TODO] placeholders 2. Verify consistency with other ST sections 3. Ensure all references are correct 4. Have the document reviewed by relevant stakeholders

ewpage

Chapter 3

TOE Overview

Document-ID: 0020
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

3.1 1. TOE Overview

3.1.1 1.1 TOE Type

Product Type: [TODO: e.g., Firewall, Operating System, Smartcard, Database, etc.]
Product Category: [TODO: e.g., Network Security, Access Control, Cryptography]
Technology: [TODO: e.g., Software, Hardware, Firmware, Hybrid]

3.1.2 1.2 TOE Purpose

[TODO: Describe the primary purpose and functionality of the TOE]

The TOE provides: - [TODO: Main function 1] - [TODO: Main function 2] - [TODO: Main function 3]

3.1.3 1.3 TOE Usage

Intended Use: [TODO: Describe the intended use case]
Target Environment: [TODO: e.g., Enterprise network, Government facility, Consumer device]
User Types: [TODO: e.g., Administrators, End users, Security officers]

3.2 2. TOE Scope

3.2.1 2.1 Physical Scope

The TOE consists of the following physical components:

Component	Type	Description
[TODO: Component 1]	Hardware/Software/Firmware	[TODO: Description]
[TODO: Component 2]	Hardware/Software/Firmware	[TODO: Description]
[TODO: Component 3]	Hardware/Software/Firmware	[TODO: Description]

3.2.2 2.2 Logical Scope

The TOE provides the following security functions:

Security Function	Description
[TODO: Function 1]	[TODO: Description]
[TODO: Function 2]	[TODO: Description]
[TODO: Function 3]	[TODO: Description]

3.2.3 2.3 TOE Boundaries

Included in TOE: - [TODO: Component/function included] - [TODO: Component/function included]

Excluded from TOE: - [TODO: Component/function excluded] - [TODO: Component/function excluded]

3.3 3. TOE Features

3.3.1 3.1 Major Security Features

[TODO: Describe the major security features]

1. **[TODO: Feature 1]**
   - Description: [TODO]
   - Security benefit: [TODO]
2. **[TODO: Feature 2]**
   - Description: [TODO]
   - Security benefit: [TODO]
3. **[TODO: Feature 3]**
   - Description: [TODO]
   - Security benefit: [TODO]

3.3.2 3.2 Non-Security Features

[TODO: List non-security features that are part of the TOE but not evaluated] - [TODO: Feature 1] - [TODO: Feature 2]

3.4 4. TOE Architecture

3.4.1 4.1 High-Level Architecture

[TODO: Provide a high-level architectural diagram]

`[TODO: Insert architecture diagram or description]`

3.4.2 4.2 Components

Major Components: 1. [TODO: Component name] - Purpose: [TODO] - Technology: [TODO] - Interfaces: [TODO]

2. [TODO: Component name]
   - Purpose: [TODO]
   - Technology: [TODO]
   - Interfaces: [TODO]

3.4.3 4.3 Data Flow

[TODO: Describe the main data flows within the TOE]

`[TODO: Insert data flow diagram or description]`

3.5 5. TOE Environment

3.5.1 5.1 Operational Environment

Hardware Platform: [TODO: Required hardware]
Operating System: [TODO: Required OS]
Network: [TODO: Network requirements]
Dependencies: [TODO: External dependencies]

3.5.2 5.2 Environmental Assumptions

The TOE assumes the following about its environment: - [TODO: Assumption 1] - [TODO: Assumption 2] - [TODO: Assumption 3]

3.5.3 5.3 Environmental Security

The environment must provide: - [TODO: Security measure 1] - [TODO: Security measure 2] - [TODO: Security measure 3]

3.6 6. TOE Interfaces

3.6.1 6.1 User Interfaces

Interface	Type	Users	Description
[TODO: Interface 1]	GUI/CLI/API	[TODO: User type]	[TODO: Description]
[TODO: Interface 2]	GUI/CLI/API	[TODO: User type]	[TODO: Description]

3.6.2 6.2 External Interfaces

Interface	Protocol	Purpose	Security
[TODO: Interface 1]	[TODO: Protocol]	[TODO: Purpose]	[TODO: Security measures]
[TODO: Interface 2]	[TODO: Protocol]	[TODO: Purpose]	[TODO: Security measures]

3.6.3 6.3 Administrative Interfaces

[TODO: Describe administrative interfaces] - Configuration interface: [TODO] - Monitoring interface: [TODO] - Logging interface: [TODO]

3.7 7. TOE Lifecycle

3.7.1 7.1 Development

Development Process: [TODO: Describe development methodology]
Security in Development: [TODO: Security measures during development]

3.7.2 7.2 Delivery

Delivery Method: [TODO: e.g., Download, Physical media, Pre-installed]
Integrity Protection: [TODO: e.g., Digital signature, Checksum]

3.7.3 7.3 Installation

Installation Process: [TODO: Brief description]
Secure Installation: [TODO: Security measures during installation]

3.7.4 7.4 Operation

Operational Modes: [TODO: e.g., Normal mode, Maintenance mode]
Secure Operation: [TODO: Security measures during operation]

3.7.5 7.5 Maintenance

Maintenance Activities: [TODO: e.g., Updates, Patches, Configuration changes]
Secure Maintenance: [TODO: Security measures during maintenance]

3.7.6 7.6 Decommissioning

Decommissioning Process: [TODO: Brief description]
Secure Decommissioning: [TODO: e.g., Data sanitization, Key destruction]

3.8 8. TOE Documentation

3.8.1 8.1 User Documentation

- [TODO: User Guide]
- [TODO: Quick Start Guide]

- [TODO: Online Help]

3.8.2 8.2 Administrator Documentation

- [TODO: Administrator Guide]
- [TODO: Installation Guide]
- [TODO: Configuration Guide]
- [TODO: Security Guide]

3.8.3 8.3 Developer Documentation

- [TODO: Architecture Document]
- [TODO: Design Specification]
- [TODO: Security Architecture]

Next Steps: 1. Complete all [TODO] placeholders with TOE-specific information 2. Create architectural and data flow diagrams 3. Verify consistency with detailed TOE description 4. Ensure all interfaces are documented

ewpage

Chapter 4

TOE Description Summary

Document-ID: 0030
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

4.1 1. TOE Summary

4.1.1 1.1 Product Summary

Product Name: [TODO: Product name]
Version: [TODO: Version]
Type: [TODO: Product type]

Brief Description:
[TODO: 2-3 sentences summarizing the TOE]

4.1.2 1.2 Security Summary

The TOE provides security through: - [TODO: Main security feature 1] - [TODO: Main security feature 2] - [TODO: Main security feature 3]

4.2 2. Physical Description

4.2.1 2.1 Hardware Components

[TODO: If applicable] - [TODO: Hardware component 1] - [TODO: Hardware component 2]

4.2.2 2.2 Software Components

[TODO: If applicable] - [TODO: Software component 1] - [TODO: Software component 2]

4.2.3 2.3 Firmware Components

[TODO: If applicable] - [TODO: Firmware component 1] - [TODO: Firmware component 2]

4.3 3. Logical Description

4.3.1 3.1 Security Functions

The TOE implements the following security functions:

1. **[TODO: Function 1]**
   - Purpose: [TODO]
   - Mechanism: [TODO]
2. **[TODO: Function 2]**
   - Purpose: [TODO]
   - Mechanism: [TODO]
3. **[TODO: Function 3]**
   - Purpose: [TODO]
   - Mechanism: [TODO]

4.3.2 3.2 Security Domains

[TODO: Describe security domains if applicable] - Domain 1: [TODO] - Domain 2: [TODO]

4.4 4. TOE Configuration

4.4.1 4.1 Evaluated Configuration

Configuration: [TODO: Describe the evaluated configuration]
Options: [TODO: Configuration options]
Modes: [TODO: Operating modes]

4.4.2 4.2 Non-Evaluated Configurations

[TODO: List configurations that are not part of the evaluation] - [TODO: Configuration 1] - [TODO: Configuration 2]

4.5 5. TOE Capabilities

4.5.1 5.1 Security Capabilities

Capability	Description	Implementation
[TODO: Capability 1]	[TODO: Description]	[TODO: Implementation]
[TODO: Capability 2]	[TODO: Description]	[TODO: Implementation]

4.5.2 5.2 Performance Characteristics

[TODO: Describe relevant performance characteristics] - Throughput: [TODO] - Latency: [TODO] - Capacity: [TODO]

4.6 6. TOE Dependencies

4.6.1 6.1 Hardware Dependencies

[TODO: List hardware dependencies] - [TODO: Dependency 1] - [TODO: Dependency 2]

4.6.2 6.2 Software Dependencies

[TODO: List software dependencies] - [TODO: Dependency 1] - [TODO: Dependency 2]

4.6.3 6.3 Environmental Dependencies

[TODO: List environmental dependencies] - [TODO: Dependency 1] - [TODO: Dependency 2]

4.7 7. TOE Limitations

4.7.1 7.1 Functional Limitations

[TODO: Describe functional limitations] - [TODO: Limitation 1] - [TODO: Limitation 2]

4.7.2 7.2 Security Limitations

[TODO: Describe security limitations] - [TODO: Limitation 1] - [TODO: Limitation 2]

4.7.3 7.3 Out of Scope

[TODO: What is explicitly out of scope] - [TODO: Item 1] - [TODO: Item 2]

Next Steps: 1. Complete all [TODO] placeholders 2. Ensure consistency with detailed TOE description 3. Verify that all components are listed

ewpage

Chapter 5

Conformance Claims

Document-ID: 0040
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

5.1 1. CC Conformance Claim

5.1.1 1.1 CC Version

Common Criteria Version: ISO/IEC 15408:2022
CC Part 1: ISO/IEC 15408-1:2022
CC Part 2: ISO/IEC 15408-2:2022
CC Part 3: ISO/IEC 15408-3:2022

5.1.2 1.2 CC Conformance

Conformance: [TODO: Select one option] - [ ] CC Part 2 conformant - [ ] CC Part 2 extended - [ ] CC Part 3 conformant - [ ] CC Part 3 extended

Rationale: [TODO: Justify the conformance claims]

5.2 2. PP Conformance Claim

5.2.1 2.1 PP Identification

[TODO: If applicable, identify the Protection Profile]

PP Name: [TODO: Protection Profile name]
PP Version: [TODO: Version]
PP Registration: [TODO: Registration number]
PP Date: [TODO: Date]

5.2.2 2.2 PP Conformance Type

[TODO: Select conformance type] - [ ] Strict conformance - [ ] Demonstrable conformance - [ ] No PP conformance

Rationale: [TODO: Justify the conformance type]

5.2.3 2.3 PP Deviations

[TODO: If applicable, document deviations from PP]

Deviation	Type	Justification
[TODO: Deviation 1]	Addition/Omission/Refinement	[TODO: Justification]
[TODO: Deviation 2]	Addition/Omission/Refinement	[TODO: Justification]

5.3 3. Package Conformance Claim

5.3.1 3.1 Assurance Package

Package: [TODO: Select the assurance package] - [ ] EAL1 (Functionally tested) - [ ] EAL2 (Structurally tested) - [ ] EAL3 (Methodically tested and checked) - [ ] EAL4 (Methodically designed, tested, and reviewed) - [ ] EAL5 (Semiformally designed and tested) - [ ] EAL6 (Semiformally verified design and tested) - [ ] EAL7 (Formally verified design and tested)

5.3.2 3.2 Augmented Package

[TODO: If applicable, list additional SARs]

Augmentation: [TODO: Yes/No]

SAR Component	Rationale
[TODO: SAR 1]	[TODO: Rationale for addition]
[TODO: SAR 2]	[TODO: Rationale for addition]

5.4 4. Conformance Rationale

5.4.1 4.1 CC Part 2 Conformance Rationale

[TODO: Justify conformance with CC Part 2]

SFR Selection: - All SFRs are derived from ISO/IEC 15408-2:2022 - [TODO: Additional details]

SFR Extensions: [TODO: If applicable, justify SFR extensions] - [TODO: Extension 1] - [TODO: Extension 2]

5.4.2 4.2 CC Part 3 Conformance Rationale

[TODO: Justify conformance with CC Part 3]

SAR Selection: - All SARs are derived from ISO/IEC 15408-3:2022 - [TODO: Additional details]

SAR Augmentation: [TODO: If applicable, justify SAR augmentations] - [TODO: Augmentation 1] - [TODO: Augmentation 2]

5.4.3 4.3 PP Conformance Rationale

[TODO: If PP conformance is claimed]

Conformance Demonstration: - [TODO: Show how the ST conforms to the PP] - [TODO: Document all deviations] - [TODO: Justify all additions]

5.5 5. Conformance Statement Summary

5.5.1 5.1 Summary Table

Conformance Type	Claim	Details
CC Version	ISO/IEC 15408:2022	[TODO: Details]
CC Part 2	[TODO: conformant/extended]	[TODO: Details]
CC Part 3	[TODO: conformant/extended]	[TODO: Details]
PP	[TODO: PP Name or "None"]	[TODO: Details]
Assurance Package	[TODO: EAL Level]	[TODO: Details]
Augmentation	[TODO: Yes/No]	[TODO: Details]

5.5.2 5.2 Conformance Verification

[TODO: Describe how conformance can be verified] - Verification method: [TODO] - Verification evidence: [TODO]

5.6 6. Conformance Maintenance

5.6.1 6.1 Version Control

ST Version: {{ meta.version }}
Last Conformance Review: {{ meta.date }}
Next Review: [TODO: Date]

5.6.2 6.2 Change Management

[TODO: Describe how changes to conformance claims are managed] - Change process: [TODO] - Impact assessment: [TODO] - Re-evaluation triggers: [TODO]

Next Steps: 1. Complete all [TODO] placeholders 2. Verify conformance with selected standards 3. Document all deviations completely 4. Ensure consistency with other ST sections

ewpage

Chapter 6

Document Conventions

Document-ID: 0050
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

6.1 1. Terminology and Notation

6.1.1 1.1 Common Criteria Terminology

This Security Target uses terminology from ISO/IEC 15408:2022:

Term	Definition
TOE	Target of Evaluation - the IT product or system being evaluated
TSF	TOE Security Functionality - combined functionality of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs
TSP	TOE Security Policy - set of rules that regulate how assets are managed, protected, and distributed within the TOE
SFR	Security Functional Requirement - requirement for security enforcement by the TOE
SAR	Security Assurance Requirement - requirement to assure the security of the TOE
PP	Protection Profile - implementation-independent statement of security needs for a TOE type
ST	Security Target - implementation-dependent statement of security needs for a specific identified TOE
EAL	Evaluation Assurance Level - package of assurance requirements

6.1.2 1.2 TOE-Specific Terminology

[TODO: Define TOE-specific terms]

Term	Definition
[TODO: Term 1]	[TODO: Definition]
[TODO: Term 2]	[TODO: Definition]
[TODO: Term 3]	[TODO: Definition]

6.2 2. Notation Conventions

6.2.1 2.1 SFR Notation

Security Functional Requirements are identified using the notation from ISO/IEC 15408-2:2022:

Format: `CLASS.FAMILY.COMPONENT.ELEMENT`

Example: `FIA_UAU.1.1` - **FIA** = Class (Identification and Authentication) - **UAU** = Family (User Authentication) - **1** = Component number - **1** = Element number

6.2.2 2.2 SAR Notation

Security Assurance Requirements are identified using the notation from ISO/IEC 15408-3:2022:

Format: `CLASS.FAMILY.COMPONENT`

Example: `ADV_FSP.1` - **ADV** = Class (Development) - **FSP** = Family (Functional Specification) - **1** = Component number

6.2.3 2.3 Operations on Requirements

The following operations can be performed on SFRs and SARs:

Operation	Symbol	Description
Assignment	[assignment:]	Specify a parameter
Selection	[selection:]	Choose from a list of options
Refinement	**bold**	Add detail or restrict
Iteration	/iteration	Apply requirement multiple times

Example: - Original: “The TSF shall authenticate [assignment: list of users]” - Completed: “The TSF shall authenticate [assignment: administrators, operators]”

6.3 3. Document Structure

6.3.1 3.1 Section Organization

This ST is organized according to ISO/IEC 15408-1:2022:

1. **ST Introduction** - Identification and overview

2. **TOE Description** - Physical and logical description
3. **Security Problem Definition** - Threats, OSPs, assumptions
4. **Security Objectives** - Objectives for TOE and environment
5. **Security Requirements** - SFRs and SARs
6. **TOE Summary Specification** - Security functions
7. **Appendices** - Supporting information

6.3.2 3.2 Cross-References

Cross-references within this ST use the following format: - Section references: "See Section X.Y" - Table references: "See Table X" - Figure references: "See Figure X"

6.4 4. Formatting Conventions

6.4.1 4.1 Text Formatting

Format	Usage
Bold	Emphasis, refinements
Italic	Definitions, first use of terms
`Monospace`	Code, commands, identifiers
[TODO]	Placeholder requiring completion

6.4.2 4.2 Lists and Tables

- **Bulleted lists**: Used for unordered items
- **Numbered lists**: Used for sequential steps or ordered items
- **Tables**: Used for structured data and mappings

6.4.3 4.3 Diagrams

[TODO: Describe diagram conventions if applicable] - Architecture diagrams: [TODO] - Data flow diagrams: [TODO] - Sequence diagrams: [TODO]

6.5 5. Abbreviations and Acronyms

6.5.1 5.1 Common Criteria Abbreviations

Abbreviation	Full Term
CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement

Abbreviation	Full Term
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy

6.5.2 5.2 TOE-Specific Abbreviations

[TODO: List TOE-specific abbreviations]

Abbreviation	Full Term
[TODO: Abbr 1]	[TODO: Full term]
[TODO: Abbr 2]	[TODO: Full term]
[TODO: Abbr 3]	[TODO: Full term]

6.6 6. References

6.6.1 6.1 Normative References

The following documents are referenced normatively in this ST:

1. ISO/IEC 15408-1:2022, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model
2. ISO/IEC 15408-2:2022, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components
3. ISO/IEC 15408-3:2022, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components
4. Common Methodology for Information Technology Security Evaluation (CEM)

6.6.2 6.2 Informative References

[TODO: List informative references]

1. [TODO: Reference 1]
2. [TODO: Reference 2]
3. [TODO: Reference 3]

6.7 7. Document Conventions Summary

6.7.1 7.1 Key Conventions

- All SFRs are from ISO/IEC 15408-2:2022 unless marked as extended
- All SARs are from ISO/IEC 15408-3:2022 unless marked as augmented
- Operations on requirements are clearly marked
- All [TODO] placeholders must be completed before finalization

6.7.2 7.2 Consistency Rules

- Terminology must be consistent throughout the ST
- All cross-references must be valid
- All tables and figures must be numbered sequentially
- All requirements must be uniquely identified

Next Steps: 1. Complete all [TODO] placeholders 2. Verify consistency of terminology usage 3. Ensure all abbreviations are defined 4. Check that all references are complete

ewpage

Chapter 7

TOE Physical Scope

Document-ID: 0100
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

7.1 1. Physical Components Overview

7.1.1 1.1 TOE Physical Composition

The TOE consists of the following physical components:

Component ID	Component Name	Type	Version	Description
[TODO: PC-001]	[TODO: Component name]	Hardware/Software/Firmware	[TODO: Version]	[TODO: Description]
[TODO: PC-002]	[TODO: Component name]	Hardware/Software/Firmware	[TODO: Version]	[TODO: Description]
[TODO: PC-003]	[TODO: Component name]	Hardware/Software/Firmware	[TODO: Version]	[TODO: Description]

7.1.2 1.2 Component Dependencies

[TODO: Describe dependencies between physical components]

`[TODO: Insert component dependency diagram]`

7.2 2. Hardware Components

7.2.1 2.1 Hardware Inventory

Hardware components in the TOE:

Hardware ID	Name	Manufacturer	Model	Specifications
[TODO: HW-001]	[TODO: Name]	[TODO: Manufacturer]	[TODO: Model]	[TODO: Specifications]
[TODO: HW-002]	[TODO: Name]	[TODO: Manufacturer]	[TODO: Model]	[TODO: Specifications]

7.2.2 2.2 Hardware Specifications

[TODO: Hardware Component 1] - Processor: [TODO: CPU specifications] - Memory: [TODO: RAM specifications] - Storage: [TODO: Storage specifications] - Network: [TODO: Network interfaces] - Security modules: [TODO: e.g., TPM, HSM, Secure Element]

[TODO: Hardware Component 2] - [TODO: Specifications]

7.2.3 2.3 Hardware Security Features

[TODO: Describe hardware-based security features] - Secure Boot: [TODO: Description] - Hardware encryption: [TODO: Description] - Tamper protection: [TODO: Description] - Physical security features: [TODO: Description]

7.3 3. Software Components

7.3.1 3.1 Software Inventory

Software components in the TOE:

Software ID	Name	Type	Version	Build	License
[TODO: SW-001]	[TODO: Name]	[TODO: Application/Service/Library]	[TODO: Version]	[TODO: Build]	[TODO: License]
[TODO: SW-002]	[TODO: Name]	[TODO: Application/Service/Library]	[TODO: Version]	[TODO: Build]	[TODO: License]

7.3.2 3.2 Software Modules

[TODO: Software Module 1] - Purpose: [TODO: Description] - Programming language: [TODO: e.g., C, C++, Java, Python] - Size: [TODO: LOC or file size] - Dependencies: [TODO: External libraries]

[TODO: Software Module 2] - [TODO: Details]

7.3.3 3.3 Software Configuration

Configuration files: - [TODO: Configuration file 1]: [TODO: Purpose] - [TODO: Configuration file 2]: [TODO: Purpose]

Databases: - [TODO: Database 1]: [TODO: Purpose and schema]

7.4 4. Firmware Components

7.4.1 4.1 Firmware Inventory

Firmware components in the TOE:

Firmware ID	Name	Target Hardware	Version	Purpose
[TODO: FW-001]	[TODO: Name]	[TODO: Hardware]	[TODO: Version]	[TODO: Purpose]
[TODO: FW-002]	[TODO: Name]	[TODO: Hardware]	[TODO: Version]	[TODO: Purpose]

7.4.2 4.2 Firmware Details

[TODO: Firmware Component 1] - Type: [TODO: e.g., BIOS, UEFI, Embedded Controller] - Size: [TODO: Size in KB/MB] - Update mechanism: [TODO: Description] - Signature: [TODO: Signing method]

7.4.3 4.3 Firmware Security

[TODO: Describe firmware security measures] - Secure firmware update: [TODO] - Firmware integrity verification: [TODO] - Rollback protection: [TODO]

7.5 5. Documentation Components

7.5.1 5.1 User Documentation

User documentation included in the TOE: - [TODO: User Guide]: [TODO: Format, version] - [TODO: Quick Start Guide]: [TODO: Format, version] - [TODO: Online Help]: [TODO: Format, version]

7.5.2 5.2 Administrator Documentation

Administrator documentation included in the TOE: - [TODO: Administrator Guide]: [TODO: Format, version] - [TODO: Installation Guide]: [TODO: Format, version] - [TODO: Configuration Guide]: [TODO: Format, version] - [TODO: Security Guide]: [TODO: Format, version]

7.5.3 5.3 Security Documentation

Security-related documentation: - Security Target (ST): [TODO: Version] - [TODO: Additional security documentation]

7.6 6. Physical Boundaries

7.6.1 6.1 Included Components

The following components are included in the TOE: - [TODO: Component 1]: [TODO: Rationale for inclusion] - [TODO: Component 2]: [TODO: Rationale for inclusion] - [TODO: Component 3]: [TODO: Rationale for inclusion]

7.6.2 6.2 Excluded Components

The following components are NOT included in the TOE: - [TODO: Component 1]: [TODO: Rationale for exclusion] - [TODO: Component 2]: [TODO: Rationale for exclusion] - [TODO: Component 3]: [TODO: Rationale for exclusion]

7.6.3 6.3 Boundary Rationale

[TODO: Explain the rationale for the physical boundaries of the TOE]

The physical boundaries were defined as follows: - [TODO: Rationale 1] - [TODO: Rationale 2] - [TODO: Rationale 3]

7.7 7. Delivery and Packaging

7.7.1 7.1 Delivery Format

The TOE is delivered as: - [TODO: e.g., Physical device, Software download, Container image, etc.]

Delivery media: - [TODO: e.g., USB drive, DVD, Download link, etc.]

7.7.2 7.2 Package Contents

The TOE package contains: 1. [TODO: Component 1] 2. [TODO: Component 2] 3. [TODO: Component 3] 4. [TODO: Documentation] 5. [TODO: License information]

7.7.3 7.3 Integrity Protection

Integrity protection for delivery: - Digital signature: [TODO: Signature algorithm and key] - Checksums: [TODO: Hash algorithm] - Sealing: [TODO: Physical sealing if applicable]

7.8 8. Version Control

7.8.1 8.1 Component Versions

Version control for TOE components:

Component	Version	Release Date	Changes
[TODO: Component 1]	[TODO: Version]	[TODO: Date]	[TODO: Changes]
[TODO: Component 2]	[TODO: Version]	[TODO: Date]	[TODO: Changes]

7.8.2 8.2 Version Identification

Version identification: - Method: [TODO: e.g., About dialog, Version file, CLI command] - Command: [TODO: e.g., `--version`, `/version`, etc.] - Output format: [TODO: Example output]

7.8.3 8.3 Configuration Management

Configuration management: - CM system: [TODO: e.g., Git, SVN, etc.] - Repository: [TODO: Repository information] - Build system: [TODO: Build system information]

7.9 9. Physical Scope Diagram

7.9.1 9.1 Component Diagram

[TODO: Create a diagram showing all physical components and their relationships]

`[TODO: Insert component diagram]`

7.9.2 9.2 Deployment Diagram

[TODO: Create a deployment diagram showing how components are deployed]

`[TODO: Insert deployment diagram]`

Next Steps: 1. Complete all [TODO] placeholders with TOE-specific information 2. Create detailed component diagrams 3. Document all versions and build information 4. Verify consistency with logical scope (Template 0110) 5. Ensure all delivery components are documented

ewpage

Chapter 8

TOE Logical Scope

Document-ID: 0110
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

8.1 1. Logical Components Overview

8.1.1 1.1 TOE Logical Composition

The TOE consists of the following logical components:

Component ID	Component Name	Type	Purpose	Security Relevance
[TODO: LC-001]	[TODO: Component name]	Module/Service/Function	[TODO: Purpose]	High/Medium/Low
[TODO: LC-002]	[TODO: Component name]	Module/Service/Function	[TODO: Purpose]	High/Medium/Low
[TODO: LC-003]	[TODO: Component name]	Module/Service/Function	[TODO: Purpose]	High/Medium/Low

8.1.2 1.2 Logical Architecture

[TODO: Describe the logical architecture of the TOE]

`[TODO: Insert logical architecture diagram]`

8.2 2. Security Functions

8.2.1 2.1 Security Function Overview

The TOE provides the following security functions:

Function ID	Function Name	Category	Description
[TODO: SF-001]	[TODO: Function name]	Identification/Authentication/Access Control/Audit/etc.	[TODO: Description]
[TODO: SF-002]	[TODO: Function name]	Identification/Authentication/Access Control/Audit/etc.	[TODO: Description]
[TODO: SF-003]	[TODO: Function name]	Identification/Authentication/Access Control/Audit/etc.	[TODO: Description]

8.2.2 2.2 Identification and Authentication

Identification and authentication functions:

[TODO: Function 1] - Purpose: [TODO: e.g., User identification] - Mechanism: [TODO: e.g., Username/Password, Biometrics, Token] - Strength: [TODO: e.g., Multi-factor, Single-factor] - Supported methods: [TODO: List of methods]

[TODO: Function 2] - [TODO: Details]

8.2.3 2.3 Access Control

Access control functions:

[TODO: Function 1] - Model: [TODO: e.g., DAC, MAC, RBAC, ABAC] - Granularity: [TODO: e.g., File, Object, Field] - Enforcement: [TODO: Description] - Management: [TODO: Description]

[TODO: Function 2] - [TODO: Details]

8.2.4 2.4 Audit and Logging

Audit and logging functions:

[TODO: Function 1] - Event types: [TODO: List of audited events] - Audit data: [TODO: Stored information] - Storage: [TODO: Storage mechanism] - Protection: [TODO: Integrity protection] - Review: [TODO: Review mechanisms]

[TODO: Function 2] - [TODO: Details]

8.2.5 2.5 Cryptographic Functions

Cryptographic functions:

[TODO: Function 1] - Purpose: [TODO: e.g., Encryption, Signature, Hashing] - Algorithms: [TODO: e.g., AES-256, RSA-2048, SHA-256] - Key lengths: [TODO: Key lengths] - Modes: [TODO: e.g., CBC, GCM, CTR] - Key management: [TODO: Description]

[TODO: Function 2] - [TODO: Details]

8.2.6 2.6 Data Protection

Data protection functions:

[TODO: Function 1] - Data type: [TODO: e.g., User data, Configuration, Credentials] - Protection mechanism: [TODO: e.g., Encryption, Hashing, Obfuscation] - Storage location: [TODO: e.g., Database, File system, Memory] - Lifecycle: [TODO: Creation, Use, Deletion]

[TODO: Function 2] - [TODO: Details]

8.2.7 2.7 Communication Security

Communication security functions:

[TODO: Function 1] - Protocol: [TODO: e.g., TLS 1.3, IPsec, SSH] - Encryption: [TODO: Algorithms and modes] - Authentication: [TODO: Mechanism] - Integrity protection: [TODO: Mechanism]

[TODO: Function 2] - [TODO: Details]

8.2.8 2.8 Security Management

Security management functions:

[TODO: Function 1] - Management area: [TODO: e.g., Users, Policies, Configuration] - Management interface: [TODO: GUI/CLI/API] - Permissions: [TODO: Required privileges] - Audit: [TODO: Auditing of management actions]

[TODO: Function 2] - [TODO: Details]

8.3 3. Functional Modules

8.3.1 3.1 Core Modules

Core modules of the TOE:

[TODO: Module 1] - Purpose: [TODO: Description] - Functions: [TODO: Provided functions] - Interfaces: [TODO: Internal and external interfaces] - Dependencies: [TODO: Dependencies on other modules] - Security relevance: [TODO: Security functions]

[TODO: Module 2] - [TODO: Details]

8.3.2 3.2 Security Modules

Security modules:

[TODO: Security Module 1] - Purpose: [TODO: Description] - Security functions: [TODO: Implemented security functions] - Cryptography: [TODO: Used cryptographic mechanisms] - Interfaces: [TODO: Interfaces]

[TODO: Security Module 2] - [TODO: Details]

8.3.3 3.3 Support Modules

Support modules:

[TODO: Module 1] - Purpose: [TODO: Description] - Functions: [TODO: Provided functions] - Security relevance: [TODO: Indirect security relevance]

[TODO: Module 2] - [TODO: Details]

8.4 4. Functional Capabilities

8.4.1 4.1 User Functions

User functions:

Function	Description	Security Impact
[TODO: Function 1]	[TODO: Description]	[TODO: Security impact]
[TODO: Function 2]	[TODO: Description]	[TODO: Security impact]
[TODO: Function 3]	[TODO: Description]	[TODO: Security impact]

8.4.2 4.2 Administrative Functions

Administrative functions:

Function	Description	Required Privilege
[TODO: Function 1]	[TODO: Description]	[TODO: Required privilege]
[TODO: Function 2]	[TODO: Description]	[TODO: Required privilege]
[TODO: Function 3]	[TODO: Description]	[TODO: Required privilege]

8.4.3 4.3 System Functions

System functions:

Function	Description	Trigger
[TODO: Function 1]	[TODO: Description]	[TODO: Trigger]
[TODO: Function 2]	[TODO: Description]	[TODO: Trigger]
[TODO: Function 3]	[TODO: Description]	[TODO: Trigger]

8.5 5. Logical Boundaries

8.5.1 5.1 Included Functions

The following functions are included in the TOE:

Security functions: - [TODO: Function 1]: [TODO: Rationale for inclusion] - [TODO: Function 2]: [TODO: Rationale for inclusion]

Non-security functions: - [TODO: Function 1]: [TODO: Rationale for inclusion] - [TODO: Function 2]: [TODO: Rationale for inclusion]

8.5.2 5.2 Excluded Functions

The following functions are NOT included in the TOE: - [TODO: Function 1]: [TODO: Rationale for exclusion] - [TODO: Function 2]: [TODO: Rationale for exclusion] - [TODO: Function 3]: [TODO: Rationale for exclusion]

8.5.3 5.3 Boundary Rationale

[TODO: Explain the rationale for the logical boundaries of the TOE]

The logical boundaries were defined as follows: - [TODO: Rationale 1] - [TODO: Rationale 2] - [TODO: Rationale 3]

8.6 6. Security Mechanisms

8.6.1 6.1 Authentication Mechanisms

Authentication mechanisms:

Mechanism	Type	Strength	Use Case
[TODO: Mechanism 1]	Password/Biometric/Token/Certificate	[TODO: Strength]	[TODO: Use case]
[TODO: Mechanism 2]	Password/Biometric/Token/Certificate	[TODO: Strength]	[TODO: Use case]

8.6.2 6.2 Authorization Mechanisms

Authorization mechanisms:

Mechanism	Model	Enforcement Point	Policy
[TODO: Mechanism 1]	DAC/MAC/RBAC/ABAC	[TODO: Enforcement point]	[TODO: Policy]
[TODO: Mechanism 2]	DAC/MAC/RBAC/ABAC	[TODO: Enforcement point]	[TODO: Policy]

8.6.3 6.3 Cryptographic Mechanisms

Cryptographic mechanisms:

Mechanism	Algorithm	Key Length	Purpose
[TODO: Mechanism 1]	[TODO: Algorithm]	[TODO: Key length]	[TODO: Purpose]
[TODO: Mechanism 2]	[TODO: Algorithm]	[TODO: Key length]	[TODO: Purpose]

8.6.4 6.4 Integrity Mechanisms

Integrity mechanisms:

Mechanism	Type	Protected Asset	Verification
[TODO: Mechanism 1]	Hash/MAC/Signature	[TODO: Protected asset]	[TODO: Verification]
[TODO: Mechanism 2]	Hash/MAC/Signature	[TODO: Protected asset]	[TODO: Verification]

8.7 7. Data Flow

8.7.1 7.1 Internal Data Flow

[TODO: Describe the internal data flow between logical components]

`[TODO: Insert internal data flow diagram]`

8.7.2 7.2 Security-Critical Data Flow

[TODO: Describe security-critical data flows]

[TODO: Data Flow 1] - Source: [TODO: Source component] - Destination: [TODO: Destination component] - Data type: [TODO: e.g., Credentials, Keys, Audit Data] - Protection: [TODO: Protection mechanisms]

[TODO: Data Flow 2] - [TODO: Details]

8.7.3 7.3 Trust Boundaries

[TODO: Define trust boundaries within the TOE]

`[TODO: Insert trust boundary diagram]`

8.8 8. Functional Architecture

8.8.1 8.1 Layered Architecture

[TODO: Describe the layered architecture of the TOE]

Layer 1: [TODO: Layer name] - Purpose: [TODO: Description] - Components: [TODO: Components in this layer] - Interfaces: [TODO: Interfaces]

Layer 2: [TODO: Layer name] - [TODO: Details]

8.8.2 8.2 Component Interactions

[TODO: Describe interactions between components]

`[TODO: Insert component interaction diagram]`

8.8.3 8.3 Security Enforcement Points

Security enforcement points:

Enforcement Point	Location	Enforced Policy	Mechanism
[TODO: Point 1]	[TODO: Location]	[TODO: Policy]	[TODO: Mechanism]
[TODO: Point 2]	[TODO: Location]	[TODO: Policy]	[TODO: Mechanism]

8.9 9. Operational Modes

8.9.1 9.1 Normal Operation Mode

Normal operation mode: - Description: [TODO: Description] - Available functions: [TODO: Functions] - Security behavior: [TODO: Security behavior]

8.9.2 9.2 Maintenance Mode

Maintenance mode: - Description: [TODO: Description] - Available functions: [TODO: Functions] - Security behavior: [TODO: Security behavior] - Access control: [TODO: Access control]

8.9.3 9.3 Secure State

Secure state: - Definition: [TODO: Definition of secure state] - Maintenance: [TODO: How secure state is maintained] - Recovery: [TODO: Recovery after failure]

Next Steps: 1. Complete all [TODO] placeholders with TOE-specific information 2. Create detailed functional architecture diagrams 3. Document all security mechanisms completely 4. Verify consistency with physical scope (Template 0100) 5. Ensure all security functions are documented

ewpage

Chapter 9

TOE Interfaces

Document-ID: 0120
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

9.1 1. Interface Overview

9.1.1 1.1 Interface Categories

The TOE provides the following interface categories:

Category	Count	Description
User Interfaces	[TODO: Count]	Interfaces for end users
Administrative Interfaces	[TODO: Count]	Interfaces for administrators
External Interfaces	[TODO: Count]	Interfaces to external systems
Internal Interfaces	[TODO: Count]	Interfaces between TOE components

9.1.2 1.2 Interface Architecture

[TODO: Describe the interface architecture]

`[TODO: Insert interface architecture diagram]`

9.2 2. User Interfaces

9.2.1 2.1 Graphical User Interface (GUI)

[TODO: GUI Name]

General Information: - Type: Web-based / Desktop Application / Mobile App - Technology: [TODO: e.g., HTML5, React, Qt, etc.] - Access: [TODO: e.g., Browser, Native App] - Authentication: [TODO: Authentication method]

Functions: - [TODO: Function 1]: [TODO: Description] - [TODO: Function 2]: [TODO: Description] - [TODO: Function 3]: [TODO: Description]

Security Features: - Session management: [TODO: Description] - Input validation: [TODO: Description] - Output encoding: [TODO: Description] - CSRF protection: [TODO: Description]

User Roles: | Role | Access Level | Available Functions | |——|————|————————| | [TODO: Role 1] | [TODO: Level] | [TODO: Functions] | | [TODO: Role 2] | [TODO: Level] | [TODO: Functions] |

9.2.2 2.2 Command Line Interface (CLI)

[TODO: CLI Name]

General Information: - Access: [TODO: e.g., SSH, Local Console] - Shell: [TODO: e.g., Bash, PowerShell, Custom Shell] - Authentication: [TODO: Authentication method]

Available Commands: | Command | Syntax | Description | Required Privilege | |———|——|———————-|—————-| | [TODO: Command 1] | [TODO: Syntax] | [TODO: Description] | [TODO: Privilege] | | [TODO: Command 2] | [TODO: Syntax] | [TODO: Description] | [TODO: Privilege] | | [TODO: Command 3] | [TODO: Syntax] | [TODO: Description] | [TODO: Privilege] |

Security Features: - Command validation: [TODO: Description] - Audit logging: [TODO: Description] - Privilege separation: [TODO: Description]

9.2.3 2.3 Application Programming Interface (API)

[TODO: API Name]

General Information: - Type: REST / SOAP / GraphQL / gRPC - Protocol: HTTPS / HTTP / Custom - Authentication: [TODO: e.g., OAuth 2.0, API Keys, JWT] - Authorization: [TODO: Authorization mechanism]

API Endpoints: | Endpoint | Method | Description | Authentication | Authorization | |———-|——|————-|—————-|—————| | [TODO: /api/endpoint1] | GET/POST/PUT/DELETE | [TODO: Description] | [TODO: Auth] | [TODO: Authz] | | [TODO: /api/endpoint2] | GET/POST/PUT/DELETE | [TODO: Description] | [TODO: Auth] | [TODO: Authz] | | [TODO: /api/endpoint3] | GET/POST/PUT/DELETE | [TODO: Description] | [TODO: Auth] | [TODO: Authz] |

Security Features: - TLS encryption: [TODO: Version and cipher suites] - Rate limiting: [TODO: Description] - Input validation: [TODO: Description] - API versioning: [TODO: Description]

API Documentation: - Format: [TODO: e.g., OpenAPI/Swagger, WSDL] - Access: [TODO: URL or location]

9.3 3. Administrative Interfaces

9.3.1 3.1 Configuration Interface

[TODO: Configuration Interface]

General Information: - Type: GUI / CLI / API / Configuration File - Access: [TODO: Access method] - Authentication: [TODO: Authentication method] - Authorization: [TODO: Required privilege]

Configurable Parameters: | Parameter | Type | Default | Description | Security Impact | |———–|——|———|————-|—————| | [TODO: Parameter 1] | [TODO: Type] | [TODO: Default] | [TODO: Description] | High/Medium/Low | | [TODO: Parameter 2] | [TODO: Type] | [TODO: Default] | [TODO: Description] | High/Medium/Low | | [TODO: Parameter 3] | [TODO: Type] | [TODO: Default] | [TODO: Description] | High/Medium/Low |

Security Features: - Configuration validation: [TODO: Description] - Change audit: [TODO: Description] - Rollback mechanism: [TODO: Description]

9.3.2 3.2 Monitoring Interface

[TODO: Monitoring Interface]

General Information: - Type: GUI / CLI / API - Protocol: [TODO: e.g., SNMP, REST, Proprietary] - Authentication: [TODO: Authentication method]

Monitored Metrics: | Metric | Type | Unit | Threshold | Alert | |———|——|——|———–|——-| | [TODO: Metric 1] | Performance/Security/Availability | [TODO: Unit] | [TODO: Threshold] | [TODO: Alert] | | [TODO: Metric 2] | Performance/Security/Availability | [TODO: Unit] | [TODO: Threshold] | [TODO: Alert] |

Security Features: - Access control: [TODO: Description] - Data integrity: [TODO: Description]

9.3.3 3.3 Logging Interface

[TODO: Logging Interface]

General Information: - Type: Syslog / File-based / Database / SIEM Integration - Protocol: [TODO: e.g., Syslog, REST] - Format: [TODO: e.g., JSON, CEF, Plain Text]

Log Categories: | Category | Events | Severity Levels | Retention | |———-|——|—————|———–| | [TODO: Category 1] | [TODO: Events] | [TODO: Levels] | [TODO: Retention] | | [TODO: Category 2] | [TODO: Events] | [TODO: Levels] | [TODO: Retention] |

Security Features: - Log integrity: [TODO: Description] - Encryption: [TODO: Description] - Access control: [TODO: Description]

9.3.4 3.4 Backup and Restore Interface

[TODO: Backup/Restore Interface]

General Information: - Type: CLI / API / GUI - Authentication: [TODO: Authentication method] - Authorization: [TODO: Required privilege]

Functions: - Backup creation: [TODO: Description] - Backup restoration: [TODO: Description] - Backup verification: [TODO: Description]

Security Features: - Backup encryption: [TODO: Algorithm] - Integrity protection: [TODO: Mechanism] - Access control: [TODO: Description]

9.4 4. External Interfaces

9.4.1 4.1 Network Interfaces

[TODO: Network Interface 1]

General Information: - Type: Ethernet / Wi-Fi / Serial / etc. - Protocol: [TODO: e.g., TCP/IP, UDP] - Port: [TODO: Port number] - Direction: Inbound / Outbound / Bidirectional

Communication Partners: | Partner | Purpose | Protocol | Security | |———|———|———-|———-| | [TODO: System 1] | [TODO: Purpose] | [TODO: Protocol] | [TODO: Security] | | [TODO: System 2] | [TODO: Purpose] | [TODO: Protocol] | [TODO: Security] |

Security Features: - Encryption: [TODO: e.g., TLS 1.3] - Authentication: [TODO: Mechanism] - Firewall rules: [TODO: Description]

9.4.2 4.2 Database Interfaces

[TODO: Database Interface]

General Information: - Database type: [TODO: e.g., PostgreSQL, MySQL, Oracle] - Connection protocol: [TODO: e.g., JDBC, ODBC, Native] - Authentication: [TODO: Authentication method]

Database Operations: | Operation | Tables | Purpose | Frequency | |———|——|———|———-| | [TODO: Operation 1] | [TODO: Tables] | [TODO: Purpose] | [TODO: Frequency] | | [TODO: Operation 2] | [TODO: Tables] | [TODO: Purpose] | [TODO: Frequency] |

Security Features: - Connection encryption: [TODO: Description] - SQL injection protection: [TODO: Description] - Access control: [TODO: Description]

9.4.3 4.3 Directory Service Interfaces

[TODO: Directory Service Interface]

General Information: - Type: LDAP / Active Directory / Azure AD / etc. - Protocol: [TODO: e.g., LDAPS, Kerberos] - Purpose: [TODO: e.g., Authentication, Authorization]

Operations: - Authentication: [TODO: Description] - Attribute query: [TODO: Description] - Group membership: [TODO: Description]

Security Features: - Encryption: [TODO: Description] - Certificate validation: [TODO: Description]

9.4.4 4.4 External System Interfaces

[TODO: External System 1]

General Information: - System: [TODO: System name] - Purpose: [TODO: Integration purpose] - Protocol: [TODO: Communication protocol] - Data format: [TODO: e.g., JSON, XML, Binary]

Data Exchange: | Data Type | Direction | Format | Frequency | Security | |————|————|————|————|————| | [TODO: Data type 1] | In/Out/Both | [TODO: Format] | [TODO: Frequency] | [TODO: Security] | | [TODO: Data type 2] | In/Out/Both | [TODO: Format] | [TODO: Frequency] | [TODO: Security] |

Security Features: - Authentication: [TODO: Mechanism] - Encryption: [TODO: Mechanism] - Data validation: [TODO: Description]

9.5 5. Internal Interfaces

9.5.1 5.1 Inter-Component Interfaces

[TODO: Internal Interface 1]

General Information: - Source: [TODO: Source component] - Destination: [TODO: Destination component] - Type: Function Call / IPC / Message Queue / etc. - Protocol: [TODO: Internal protocol]

Data Exchange: | Data Type | Purpose | Format | Security | |————|————|————|————| | [TODO: Data type 1] | [TODO: Purpose] | [TODO: Format] | [TODO: Security] | | [TODO: Data type 2] | [TODO: Purpose] | [TODO: Format] | [TODO: Security] |

Security Features: - Access control: [TODO: Description] - Data validation: [TODO: Description]

9.5.2 5.2 Module Interfaces

[TODO: Module Interface 1]

General Information: - Module: [TODO: Module name] - Type: API / Library / Service - Programming language: [TODO: Language]

Provided Functions: | Function | Parameters | Return Type | Description | |————|————|————|————| | [TODO: Function 1] | [TODO: Parameters] | [TODO: Return type] | [TODO: Description] | | [TODO: Function 2] | [TODO: Parameters] | [TODO: Return type] | [TODO: Description] |

Security Features: - Input validation: [TODO: Description] - Error handling: [TODO: Description]

9.6 6. Interface Security

9.6.1 6.1 Authentication Mechanisms

Interface authentication:

Interface	Authentication Method	Credential Type	Multi-Factor
[TODO: Interface 1]	[TODO: Method]	[TODO: Credential type]	Yes/No

Interface	Authentication Method	Credential Type	Multi-Factor
[TODO: Interface 2]	[TODO: Method]	[TODO: Credential type]	Yes/No

9.6.2 6.2 Authorization Mechanisms

Interface authorization:

Interface	Authorization Model	Enforcement Point	Policy
[TODO: Interface 1]	[TODO: Model]	[TODO: Point]	[TODO: Policy]
[TODO: Interface 2]	[TODO: Model]	[TODO: Point]	[TODO: Policy]

9.6.3 6.3 Encryption and Integrity

Encryption and integrity:

Interface	Encryption	Algorithm	Integrity Protection
[TODO: Interface 1]	Yes/No	[TODO: Algorithm]	[TODO: Mechanism]
[TODO: Interface 2]	Yes/No	[TODO: Algorithm]	[TODO: Mechanism]

9.6.4 6.4 Input Validation

Input validation:

Interface	Validation Type	Sanitization	Error Handling
[TODO: Interface 1]	[TODO: Type]	[TODO: Sanitization]	[TODO: Error handling]
[TODO: Interface 2]	[TODO: Type]	[TODO: Sanitization]	[TODO: Error handling]

9.7 7. Interface Protocols

9.7.1 7.1 Communication Protocols

Used communication protocols:

Protocol	Version	Purpose	Security Features
[TODO: Protocol 1]	[TODO: Version]	[TODO: Purpose]	[TODO: Security features]
[TODO: Protocol 2]	[TODO: Version]	[TODO: Purpose]	[TODO: Security features]

9.7.2 7.2 Data Formats

Used data formats:

Format	Purpose	Schema	Validation
[TODO: Format 1]	[TODO: Purpose]	[TODO: Schema]	[TODO: Validation]
[TODO: Format 2]	[TODO: Purpose]	[TODO: Schema]	[TODO: Validation]

9.7.3 7.3 Error Handling

Error handling at interfaces:

Interface	Error Types	Error Codes	Error Messages	Logging
[TODO: Interface 1]	[TODO: Types]	[TODO: Codes]	[TODO: Messages]	Yes/No
[TODO: Interface 2]	[TODO: Types]	[TODO: Codes]	[TODO: Messages]	Yes/No

9.8 8. Interface Documentation

9.8.1 8.1 User Interface Documentation

- [TODO: GUI User Guide]: [TODO: Location]
- [TODO: CLI Reference]: [TODO: Location]
- [TODO: API Documentation]: [TODO: Location]

9.8.2 8.2 Administrator Interface Documentation

- [TODO: Configuration Guide]: [TODO: Location]
- [TODO: Monitoring Guide]: [TODO: Location]
- [TODO: Logging Guide]: [TODO: Location]

9.8.3 8.3 Developer Interface Documentation

- [TODO: API Specification]: [TODO: Location]
- [TODO: Integration Guide]: [TODO: Location]
- [TODO: Protocol Documentation]: [TODO: Location]

Next Steps: 1. Complete all [TODO] placeholders with TOE-specific information 2. Create detailed interface diagrams 3. Document all security mechanisms for each interface 4. Verify consistency with TOE architecture (Template 0130) 5. Ensure all interfaces are fully documented

ewpage

Chapter 10

TOE Architecture

Document-ID: 0130
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

10.1 1. Architecture Overview

10.1.1 1.1 High-Level Architecture

[TODO: Describe the high-level architecture of the TOE]

The TOE follows a [TODO: e.g., layered, modular, service-oriented] architecture with the following main components:

`[TODO: Insert high-level architecture diagram]`

10.1.2 1.2 Architecture Style

Architecture style: [TODO: e.g., Layered, Microservices, Client-Server, Event-Driven]

Rationale: [TODO: Explain why this architecture style was chosen]

10.1.3 1.3 Architecture Principles

Guiding architecture principles: 1. [TODO: Principle 1, e.g., Separation of Concerns] 2. [TODO: Principle 2, e.g., Least Privilege] 3. [TODO: Principle 3, e.g., Defense in Depth] 4. [TODO: Principle 4, e.g., Fail Secure] 5. [TODO: Principle 5, e.g., Simplicity]

10.2 2. Layered Architecture

10.2.1 2.1 Architecture Layers

The TOE is organized into the following layers:

Layer	Name	Responsibility	Components
[TODO: Layer 1]	[TODO: Name]	[TODO: Responsibility]	[TODO: Components]
[TODO: Layer 2]	[TODO: Name]	[TODO: Responsibility]	[TODO: Components]
[TODO: Layer 3]	[TODO: Name]	[TODO: Responsibility]	[TODO: Components]
[TODO: Layer 4]	[TODO: Name]	[TODO: Responsibility]	[TODO: Components]

10.2.2 2.2 Layer Interactions

[TODO: Describe how layers interact with each other]

Interaction rules: - [TODO: Rule 1, e.g., Layers may only communicate with adjacent layers] - [TODO: Rule 2, e.g., No bypassing of layers] - [TODO: Rule 3]

`[TODO: Insert layer interaction diagram]`

10.2.3 2.3 Layer Details

10.2.3.1 Layer: [TODO: Layer name 1]

Purpose: [TODO: Description]

Components: - [TODO: Component 1]: [TODO: Description] - [TODO: Component 2]: [TODO: Description]

Interfaces: - Upward: [TODO: Provided interfaces] - Downward: [TODO: Used interfaces]

Security responsibilities: - [TODO: Security responsibility 1] - [TODO: Security responsibility 2]

10.2.3.2 Layer: [TODO: Layer name 2]

[TODO: Details as above]

10.3 3. Component Architecture

10.3.1 3.1 Component Overview

Main components of the TOE:

Component ID	Name	Type	Layer	Purpose
[TODO: COMP-001]	[TODO: Name]	Core/Security/Support: [TODO:	TODO: Layer]	[TODO: Purpose]
[TODO: COMP-002]	[TODO: Name]	Core/Security/Support: [TODO:	TODO: Layer]	[TODO: Purpose]
[TODO: COMP-003]	[TODO: Name]	Core/Security/Support: [TODO:	TODO: Layer]	[TODO: Purpose]

10.3.2 3.2 Component Relationships

[TODO: Describe relationships between components]

`[TODO: Insert component relationship diagram]`

10.3.3 3.3 Component Details

10.3.3.1 Component: [TODO: Component name 1]

General information: - ID: [TODO: COMP-001] - Type: [TODO: Core/Security/Support] - Layer: [TODO: Layer] - Technology: [TODO: e.g., Java, C++, Python]

Purpose: [TODO: Describe the purpose of this component]

Responsibilities: - [TODO: Responsibility 1] - [TODO: Responsibility 2] - [TODO: Responsibility 3]

Provided interfaces: | Interface | Type | Consumers | |————|——|————| | [TODO: Interface 1] | [TODO: Type] | [TODO: Consumers] | | [TODO: Interface 2] | [TODO: Type] | [TODO: Consumers] |

Used interfaces: | Interface | Provider | Purpose | |————|———-|———| | [TODO: Interface 1] | [TODO: Provider] | [TODO: Purpose] | | [TODO: Interface 2] | [TODO: Provider] | [TODO: Purpose] |

Dependencies: - [TODO: Dependency 1] - [TODO: Dependency 2]

Security relevance: [TODO: Describe the security relevance of this component]

10.3.3.2 Component: [TODO: Component name 2]

[TODO: Details as above]

10.4 4. Security Architecture

10.4.1 4.1 Security Architecture Overview

[TODO: Describe the security architecture of the TOE]

`[TODO: Insert security architecture diagram]`

10.4.2 4.2 Trust Boundaries

Trust boundaries in the TOE:

Boundary	Description	Protection Mechanism
[TODO: Boundary 1]	[TODO: Description]	[TODO: Protection mechanism]
[TODO: Boundary 2]	[TODO: Description]	[TODO: Protection mechanism]
[TODO: Boundary 3]	[TODO: Description]	[TODO: Protection mechanism]

`[TODO: Insert trust boundary diagram]`

10.4.3 4.3 Security Zones

Security zones:

Zone	Trust Level	Components	Access Control
[TODO: Zone 1]	High/Medium/Low	[TODO: Components]	[TODO: Access control]
[TODO: Zone 2]	High/Medium/Low	[TODO: Components]	[TODO: Access control]

10.4.4 4.4 Security Enforcement Points

Security enforcement points:

Enforcement Point	Location	Enforced Policies	Mechanism
[TODO: Point 1]	[TODO: Location]	[TODO: Policies]	[TODO: Mechanism]
[TODO: Point 2]	[TODO: Location]	[TODO: Policies]	[TODO: Mechanism]

10.4.5 4.5 Security Functions Mapping

Mapping of security functions to components:

Security Function	Implementing Component	Layer	Mechanism
[TODO: Function 1]	[TODO: Component]	[TODO: Layer]	[TODO: Mechanism]
[TODO: Function 2]	[TODO: Component]	[TODO: Layer]	[TODO: Mechanism]

10.5 5. Data Architecture

10.5.1 5.1 Data Flow Architecture

[TODO: Describe the data flow architecture]

`[TODO: Insert data flow architecture diagram]`

10.5.2 5.2 Data Storage Architecture

Data storage architecture:

Data Store	Type	Purpose	Security
[TODO: Store 1]	Database/File/Memory	[TODO: Purpose]	[TODO: Security]
[TODO: Store 2]	Database/File/Memory	[TODO: Purpose]	[TODO: Security]

10.5.3 5.3 Data Protection Architecture

Data protection architecture:

Data Type	Classification	Protection Mechanism	Location
[TODO: Data type 1]	Public/Internal/Confidential/Secret	[TODO: Protection mechanism]	[TODO: Location]
[TODO: Data type 2]	Public/Internal/Confidential/Secret	[TODO: Protection mechanism]	[TODO: Location]

10.5.4 5.4 Data Flow Paths

Critical data flow paths:

[TODO: Data flow path 1] - Source: [TODO: Source] - Destination: [TODO: Destination] - Traversed components: [TODO: Components] - Security measures: [TODO: Measures]

[TODO: Data flow path 2] - [TODO: Details]

10.6 6. Deployment Architecture

10.6.1 6.1 Deployment Overview

[TODO: Describe the deployment architecture]

```
[TODO: Insert deployment diagram]
```

10.6.2 6.2 Deployment Scenarios

Supported deployment scenarios:

Scenario 1: [TODO: Scenario name] - Description: [TODO: Description] - Components: [TODO: Deployed components] - Infrastructure: [TODO: Required infrastructure] - Security aspects: [TODO: Security aspects]

Scenario 2: [TODO: Scenario name] - [TODO: Details]

10.6.3 6.3 Physical Deployment

Physical deployment topology:

Node	Type	Hosted Components	Network
[TODO: Node 1]	Server/Client/Appliance	[TODO: Components]	[TODO: Network]
[TODO: Node 2]	Server/Client/Appliance	[TODO: Components]	[TODO: Network]

10.6.4 6.4 Network Architecture

Network architecture:

```
[TODO: Insert network architecture diagram]
```

Network segments: | Segment | Purpose | Components | Security | |———|———|————|———-| | [TODO: Segment 1] | [TODO: Purpose] | [TODO: Components] | [TODO: Security] | | [TODO: Segment 2] | [TODO: Purpose] | [TODO: Components] | [TODO: Security] |

10.7 7. Runtime Architecture

10.7.1 7.1 Process Architecture

Process architecture:

Process	Type	Components	Privileges
[TODO: Process 1]	Service/Daemon/Application	[TODO: Components]	[TODO: Privileges]
[TODO: Process 2]	Service/Daemon/Application	[TODO: Components]	[TODO: Privileges]

10.7.2 7.2 Thread Architecture

Threading model: [TODO: Describe the threading model of the TOE]

10.7.3 7.3 Memory Architecture

Memory architecture: - Heap management: [TODO: Description] - Stack management: [TODO: Description] - Memory protection: [TODO: Mechanisms]

10.7.4 7.4 Execution Flow

Execution flow:

```
[TODO: Insert execution flow diagram]
```

10.8 8. Integration Architecture

10.8.1 8.1 External System Integration

Integration with external systems:

External System	Integration Type	Protocol	Security
[TODO: System 1]	API/Message Queue/Database	[TODO: Protocol]	[TODO: Security]
[TODO: System 2]	API/Message Queue/Database	[TODO: Protocol]	[TODO: Security]

10.8.2 8.2 Integration Patterns

Used integration patterns: - [TODO: Pattern 1, e.g., Request-Response] - [TODO: Pattern 2, e.g., Publish-Subscribe] - [TODO: Pattern 3, e.g., Message Queue]

10.8.3 8.3 Integration Security

Integration security: - Authentication: [TODO: Mechanism] - Authorization: [TODO: Mechanism] - Encryption: [TODO: Mechanism] - Data validation: [TODO: Mechanism]

10.9 9. Scalability and Performance Architecture

10.9.1 9.1 Scalability Design

Scalability design: - Horizontal scaling: [TODO: Description] - Vertical scaling: [TODO: Description] - Load balancing: [TODO: Mechanism]

10.9.2 9.2 Performance Considerations

Performance considerations: - Caching strategy: [TODO: Description] - Database optimization: [TODO: Description] - Network optimization: [TODO: Description]

10.9.3 9.3 Resource Management

Resource management: - CPU management: [TODO: Description] - Memory management: [TODO: Description] - I/O management: [TODO: Description]

10.10 10. Resilience Architecture

10.10.1 10.1 Fault Tolerance

Fault tolerance: - Redundancy: [TODO: Description] - Failover: [TODO: Mechanism] - Recovery: [TODO: Mechanism]

10.10.2 10.2 Error Handling

Error handling: - Error detection strategy: [TODO: Description] - Error handling strategy: [TODO: Description] - Error logging: [TODO: Description]

10.10.3 10.3 Availability Design

Availability design: - Target availability: [TODO: e.g., 99.9%] - High availability mechanisms: [TODO: Description] - Maintenance windows: [TODO: Description]

10.11 11. Architecture Decisions

10.11.1 11.1 Key Architecture Decisions

Key architecture decisions:

Decision 1: [TODO: Decision title] - Context: [TODO: Context] - Decision: [TODO: Decision made] - Alternatives: [TODO: Considered alternatives] - Rationale: [TODO: Rationale] - Consequences: [TODO: Consequences]

Decision 2: [TODO: Decision title] - [TODO: Details]

10.11.2 11.2 Trade-offs

Architecture trade-offs: - [TODO: Trade-off 1, e.g., Performance vs. Security] - [TODO: Trade-off 2, e.g., Complexity vs. Maintainability] - [TODO: Trade-off 3]

10.11.3 11.3 Constraints

Architecture constraints: - Technical constraints: [TODO: List] - Organizational constraints: [TODO: List] - Regulatory constraints: [TODO: List]

10.12 12. Architecture Documentation

10.12.1 12.1 Architecture Views

Available architecture views: - Logical view: [TODO: Location] - Process view: [TODO: Location] - Development view: [TODO: Location] - Physical view: [TODO: Location] - Scenario view: [TODO: Location]

10.12.2 12.2 Architecture Models

Architecture models: - UML models: [TODO: Location] - C4 models: [TODO: Location] - Data models: [TODO: Location]

10.12.3 12.3 Architecture Standards

Used architecture standards: - [TODO: Standard 1] - [TODO: Standard 2] - [TODO: Standard 3]

Next Steps: 1. Complete all [TODO] placeholders with TOE-specific information 2. Create all required architecture diagrams 3. Document all architecture decisions completely 4. Verify consistency with other TOE description documents 5. Ensure the security architecture is fully documented

ewpage

Chapter 11

TOE Lifecycle

Document-ID: 0140
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

11.1 1. Lifecycle Overview

11.1.1 1.1 Lifecycle Phases

The TOE lifecycle includes the following phases:

Phase	Duration	Responsible	Security Focus
[TODO: Phase 1]	[TODO: Duration]	[TODO: Responsible]	[TODO: Security focus]
[TODO: Phase 2]	[TODO: Duration]	[TODO: Responsible]	[TODO: Security focus]
[TODO: Phase 3]	[TODO: Duration]	[TODO: Responsible]	[TODO: Security focus]
[TODO: Phase 4]	[TODO: Duration]	[TODO: Responsible]	[TODO: Security focus]

11.1.2 1.2 Lifecycle Diagram

[TODO: Create a diagram showing all lifecycle phases and transitions]

`[TODO: Insert lifecycle diagram]`

11.1.3 1.3 Lifecycle Roles

Roles in the TOE lifecycle:

Role	Responsibilities	Phases
[TODO: Role 1]	[TODO: Responsibilities]	[TODO: Phases]
[TODO: Role 2]	[TODO: Responsibilities]	[TODO: Phases]
[TODO: Role 3]	[TODO: Responsibilities]	[TODO: Phases]

11.2 2. Development Phase

11.2.1 2.1 Development Process

Development process: - Methodology: [TODO: e.g., Agile, Waterfall, DevSecOps] - Development environment: [TODO: Description] - Version control: [TODO: e.g., Git, SVN] - Build system: [TODO: e.g., Maven, Gradle, Make]

11.2.2 2.2 Security in Development

Security measures during development:

Secure Coding Practices: - Coding standards: [TODO: e.g., CERT, MISRA] - Code reviews: [TODO: Process] - Static analysis: [TODO: Tools and process] - Security training: [TODO: Training program]

Security Testing: - Unit testing: [TODO: Description] - Integration testing: [TODO: Description] - Security testing: [TODO: e.g., SAST, DAST, Penetration Testing] - Vulnerability scanning: [TODO: Tools and process]

11.2.3 2.3 Configuration Management

Configuration management: - CM system: [TODO: System] - Baseline management: [TODO: Process] - Change control: [TODO: Process] - Release management: [TODO: Process]

11.2.4 2.4 Development Documentation

Development documentation: - Requirements specification: [TODO: Location] - Design documentation: [TODO: Location] - Implementation documentation: [TODO: Location] - Test documentation: [TODO: Location]

11.2.5 2.5 Development Environment Security

Development environment security: - Access control: [TODO: Access control mechanisms] - Network segmentation: [TODO: Network segmentation] - Audit logging: [TODO: Audit logging] - Backup: [TODO: Backup strategy]

11.3 3. Build and Integration Phase

11.3.1 3.1 Build Process

Build process: - Build system: [TODO: System] - Build automation: [TODO: CI/CD pipeline] - Build environment: [TODO: Description] - Build verification: [TODO: Verification mechanisms]

11.3.2 3.2 Build Security

Build security: - Build integrity: [TODO: Integrity protection] - Dependency management: [TODO: Dependency management] - Supply chain security: [TODO: Security measures] - Build reproducibility: [TODO: Reproducibility]

11.3.3 3.3 Integration Testing

Integration testing: - Test strategy: [TODO: Strategy] - Test environment: [TODO: Environment] - Test automation: [TODO: Automation] - Test documentation: [TODO: Documentation]

11.3.4 3.4 Quality Assurance

Quality assurance: - QA process: [TODO: Process] - Code coverage: [TODO: Target coverage] - Performance testing: [TODO: Performance tests] - Security validation: [TODO: Security validation]

11.4 4. Delivery Phase

11.4.1 4.1 Delivery Process

Delivery process: - Delivery method: [TODO: e.g., Download, Physical Media, Pre-installed] - Packaging: [TODO: Packaging] - Distribution channels: [TODO: Distribution channels] - Delivery timeline: [TODO: Timeline]

11.4.2 4.2 Delivery Security

Delivery security:

Integrity Protection: - Digital signature: [TODO: Signature algorithm and key] - Checksums: [TODO: Hash algorithm] - Tamper-evident packaging: [TODO: Tamper-evident packaging]

Authenticity Verification: - Certificate chain: [TODO: Certificate chain] - Verification process: [TODO: Verification process] - Public key distribution: [TODO: Public key distribution]

11.4.3 4.3 Delivery Documentation

Delivery documentation: - Release notes: [TODO: Location] - Installation guide: [TODO: Location] - User documentation: [TODO: Location] - Security guide: [TODO: Location]

11.4.4 4.4 Delivery Verification

Delivery verification: - Verification steps: [TODO: Verification steps] - Verification tools: [TODO: Tools] - Verification documentation: [TODO: Documentation]

11.5 5. Installation Phase

11.5.1 5.1 Installation Process

Installation process: - Installation method: [TODO: e.g., Automated, Manual, Hybrid] - Installation steps: [TODO: Steps] - Installation time: [TODO: Estimated time] - Prerequisites: [TODO: Prerequisites]

11.5.2 5.2 Secure Installation

Secure installation:

Pre-Installation: - System requirements verification: [TODO: Verification] - Security prerequisites: [TODO: Security prerequisites] - Backup existing system: [TODO: Backup process]

During Installation: - Integrity verification: [TODO: Integrity verification] - Secure configuration: [TODO: Secure configuration] - Credential setup: [TODO: Credential setup] - Security hardening: [TODO: Hardening measures]

Post-Installation: - Installation verification: [TODO: Verification] - Security testing: [TODO: Security testing] - Documentation: [TODO: Documentation]

11.5.3 5.3 Initial Configuration

Initial configuration: - Configuration parameters: [TODO: Parameters] - Security settings: [TODO: Security settings] - Network configuration: [TODO: Network configuration] - User setup: [TODO: User setup]

11.5.4 5.4 Installation Validation

Installation validation: - Functional testing: [TODO: Functional tests] - Security validation: [TODO: Security validation] - Performance baseline: [TODO: Performance baseline] - Documentation: [TODO: Documentation]

11.6 6. Operation Phase

11.6.1 6.1 Operational Procedures

Operational procedures: - Startup procedures: [TODO: Startup procedures] - Shutdown procedures: [TODO: Shutdown procedures] - Backup procedures: [TODO: Backup procedures] - Monitoring procedures: [TODO: Monitoring procedures]

11.6.2 6.2 Secure Operation

Secure operation:

Access Control: - User management: [TODO: User management] - Privilege management: [TODO: Privilege management] - Authentication: [TODO: Authentication] - Authorization: [TODO: Authorization]

Monitoring and Logging: - Security monitoring: [TODO: Security monitoring] - Audit logging: [TODO: Audit logging] - Log review: [TODO: Log review] - Incident detection: [TODO: Incident detection]

Configuration Management: - Configuration baseline: [TODO: Configuration baseline] - Change management: [TODO: Change management] - Configuration audits: [TODO: Configuration audits]

11.6.3 6.3 Operational Modes

Operational modes:

Normal Operation Mode: - Description: [TODO: Description] - Available functions: [TODO: Available functions] - Security behavior: [TODO: Security behavior]

Maintenance Mode: - Description: [TODO: Description] - Access control: [TODO: Access control] - Security restrictions: [TODO: Security restrictions]

Emergency Mode: - Description: [TODO: Description] - Activation criteria: [TODO: Activation criteria] - Security measures: [TODO: Security measures]

11.6.4 6.4 Operational Documentation

Operational documentation: - Operations manual: [TODO: Location] - Security operations guide: [TODO: Location] - Troubleshooting guide: [TODO: Location] - Incident response plan: [TODO: Location]

11.7 7. Maintenance Phase

11.7.1 7.1 Maintenance Types

Maintenance types:

Corrective Maintenance: - Bug fixes: [TODO: Process] - Security patches: [TODO: Process] - Emergency updates: [TODO: Process]

Preventive Maintenance: - Regular updates: [TODO: Schedule] - Security hardening: [TODO: Measures] - Performance optimization: [TODO: Measures]

Adaptive Maintenance: - Feature updates: [TODO: Process] - Configuration changes: [TODO: Process] - Integration updates: [TODO: Process]

11.7.2 7.2 Secure Maintenance

Secure maintenance:

Update Process: - Update verification: [TODO: Verification] - Backup before update: [TODO: Backup process] - Update testing: [TODO: Test process] - Rollback capability: [TODO: Rollback mechanism]

Maintenance Access: - Access control: [TODO: Access control] - Authentication: [TODO: Authentication] - Audit logging: [TODO: Audit logging] - Session management: [TODO: Session management]

11.7.3 7.3 Patch Management

Patch management: - Patch assessment: [TODO: Assessment process] - Patch testing: [TODO: Test process] - Patch deployment: [TODO: Deployment process] - Patch verification: [TODO: Verification]

11.7.4 7.4 Maintenance Documentation

Maintenance documentation: - Maintenance log: [TODO: Location] - Change records: [TODO: Location] - Test results: [TODO: Location] - Incident reports: [TODO: Location]

11.8 8. Monitoring and Incident Response

11.8.1 8.1 Continuous Monitoring

Continuous monitoring: - Monitoring scope: [TODO: Monitoring scope] - Monitoring tools: [TODO: Tools] - Monitoring frequency: [TODO: Frequency] - Alert thresholds: [TODO: Alert thresholds]

11.8.2 8.2 Incident Response

Incident response: - Incident detection: [TODO: Detection mechanisms] - Incident classification: [TODO: Classification] - Incident response process: [TODO: Response process] - Incident documentation: [TODO: Documentation]

11.8.3 8.3 Security Events

Security events:

Event Type	Severity	Response	Escalation
[TODO: Event type 1]	Critical/High/Medium/Low	[TODO: Response]	[TODO: Escalation]
[TODO: Event type 2]	Critical/High/Medium/Low	[TODO: Response]	[TODO: Escalation]

11.8.4 8.4 Forensics and Investigation

Forensics and investigation: - Evidence collection: [TODO: Evidence collection] - Evidence preservation: [TODO: Evidence preservation] - Investigation process: [TODO: Investigation process] - Reporting: [TODO: Reporting]

11.9 9. Decommissioning Phase

11.9.1 9.1 Decommissioning Process

Decommissioning process: - Decommissioning planning: [TODO: Planning] - Decommissioning steps: [TODO: Steps] - Decommissioning timeline: [TODO: Timeline] - Decommissioning verification: [TODO: Verification]

11.9.2 9.2 Secure Decommissioning

Secure decommissioning:

Data Sanitization: - Data identification: [TODO: Data identification] - Sanitization method: [TODO: e.g., Overwriting, Degaussing, Physical Destruction] - Sanitization verification: [TODO: Verification] - Sanitization documentation: [TODO: Documentation]

Key Destruction: - Key identification: [TODO: Key identification] - Destruction method: [TODO: Destruction method] - Destruction verification: [TODO: Verification] - Destruction documentation: [TODO: Documentation]

Configuration Removal: - Configuration backup: [TODO: Configuration backup] - Configuration removal: [TODO: Removal] - Verification: [TODO: Verification]

11.9.3 9.3 Asset Disposal

Asset disposal: - Hardware disposal: [TODO: Hardware disposal] - Software removal: [TODO: Software removal] - Documentation disposal: [TODO: Documentation disposal] - Certificate revocation: [TODO: Certificate revocation]

11.9.4 9.4 Decommissioning Documentation

Decommissioning documentation: - Decommissioning plan: [TODO: Location] - Sanitization records: [TODO: Location] - Disposal records: [TODO: Location] - Completion certificate: [TODO: Location]

11.10 10. Lifecycle Security Controls

11.10.1 10.1 Security Controls by Phase

Security controls by phase:

Phase	Security Controls	Verification	Documentation
[TODO: Phase 1]	[TODO: Controls]	[TODO: Verification]	[TODO: Documentation]
[TODO: Phase 2]	[TODO: Controls]	[TODO: Verification]	[TODO: Documentation]
[TODO: Phase 3]	[TODO: Controls]	[TODO: Verification]	[TODO: Documentation]

11.10.2 10.2 Continuous Security

Continuous security: - Security assessments: [TODO: Assessments] - Vulnerability management: [TODO: Vulnerability management] - Compliance monitoring: [TODO: Compliance monitoring] - Security updates: [TODO: Security updates]

11.10.3 10.3 Lifecycle Audits

Lifecycle audits: - Audit frequency: [TODO: Frequency] - Audit scope: [TODO: Scope] - Audit process: [TODO: Process] - Audit documentation: [TODO: Documentation]

Next Steps: 1. Complete all [TODO] placeholders with TOE-specific information 2. Create detailed process diagrams for each lifecycle phase 3. Document all security measures completely 4. Verify consistency with other TOE description documents 5. Ensure all phases and transitions are documented

ewpage

Chapter 12

Security Problem Definition

Document-ID: 0200
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

12.1 1. Security Problem Overview

12.1.1 1.1 Purpose

This document defines the security problem that the TOE shall solve. It describes: - **Threats**: Potential attacks and security violations - **Organizational Security Policies (OSPs)**: Security policies that must be enforced - **Assumptions**: Expectations about the operational environment

12.1.2 1.2 Security Problem Context

Application Context: [TODO: Describe the context in which the TOE is deployed]

Security-Relevant Factors: - [TODO: Factor 1] - [TODO: Factor 2] - [TODO: Factor 3]

12.1.3 1.3 Security Problem Scope

In Scope: - [TODO: What is covered by the security problem definition]

Out of Scope: - [TODO: What is not covered]

12.2 2. Assets

12.2.1 2.1 Asset Identification

Assets to be Protected:

Asset ID	Asset Name	Type	Value	Description
[TODO: A.001]	[TODO: Asset Name]	Data/Service/Function	High/Medium/Low	[TODO: Description]
[TODO: A.002]	[TODO: Asset Name]	Data/Service/Function	High/Medium/Low	[TODO: Description]
[TODO: A.003]	[TODO: Asset Name]	Data/Service/Function	High/Medium/Low	[TODO: Description]

12.2.2 2.2 Asset Classification

Data Assets: - [TODO: Data Asset 1]: [TODO: Classification and protection needs] - [TODO: Data Asset 2]: [TODO: Classification and protection needs]

Service Assets: - [TODO: Service Asset 1]: [TODO: Availability requirements] - [TODO: Service Asset 2]: [TODO: Availability requirements]

Function Assets: - [TODO: Function Asset 1]: [TODO: Integrity requirements] - [TODO: Function Asset 2]: [TODO: Integrity requirements]

12.2.3 2.3 Asset Dependencies

[TODO: Describe dependencies between assets]

```
[TODO: Insert asset dependency diagram]
```

12.3 3. Threat Agents

12.3.1 3.1 Threat Agent Profiles

Identified Threat Agents:

Agent ID	Agent Type	Motivation	Capability	Resources	Description
[TODO: TA.001]	[TODO: e.g., Insider, External Attacker]	[TODO: Motivation]	High/Medium/Low	High/Medium/Low	[TODO: Description]
[TODO: TA.002]	[TODO: Type]	[TODO: Motivation]	High/Medium/Low	High/Medium/Low	[TODO: Description]

12.3.2 3.2 Threat Agent Capabilities

[TODO: Threat Agent 1] - **Capabilities**: [TODO: e.g., Network access, physical access, insider knowledge] - **Resources**: [TODO: e.g., Time, budget, tools] - **Motivation**: [TODO: e.g., Financial gain, sabotage, espionage] - **Attack Vectors**: [TODO: Possible attack paths]

[TODO: Threat Agent 2] - [TODO: Details]

12.3.3 3.3 Attack Potential

Attack Potential Assessment:

Agent	Elapsed Time	Expertise	Knowledge	Window of Opportunity	Equipment	Attack Potential
[TODO: TA.001]	[TODO: < 1 day / < 1 month / > 1 month]	[TODO: Layman / Proficient / Expert]	[TODO: Public / Restricted / Sensitive]	[TODO: Unnecessary / Easy / Moderate / Difficult]	[TODO: Standard / Specialized / Bespoke]	[TODO: Basic / Enhanced-Basic / Moderate / High]

12.4 4. Threats

12.4.1 4.1 Threat Catalog

Identified Threats:

Threat ID	Threat Name	Asset	Agent	Likelihood	Impact	Risk	Description
[TODO: T.001]	[TODO: Threat Name]	[TODO: A.001]	[TODO: TA.001]	High/Medium/Low	High/Medium/Low	High/Medium/Low	[TODO: Description]
[TODO: T.002]	[TODO: Threat Name]	[TODO: A.002]	[TODO: TA.002]	High/Medium/Low	High/Medium/Low	High/Medium/Low	[TODO: Description]

12.4.2 4.2 Threat Details

12.4.2.1 T.001: [TODO: Threat Name]

Description: [TODO: Detailed description of the threat]

Affected Assets: - [TODO: Asset 1] - [TODO: Asset 2]

Threat Agent: - [TODO: TA.001]

Attack Scenario: 1. [TODO: Step 1] 2. [TODO: Step 2] 3. [TODO: Step 3]

Impact: - Confidentiality: [TODO: High/Medium/Low/None] - Integrity: [TODO: High/Medium/Low/None] - Availability: [TODO: High/Medium/Low/None]

Likelihood: [TODO: High/Medium/Low]

Risk Assessment: [TODO: High/Medium/Low]

12.4.2.2 T.002: [TODO: Threat Name]

[TODO: Repeat structure for each threat]

12.4.3 4.3 Threat Scenarios

Attack Scenario 1: [TODO: Scenario Name] [TODO: Describe a complete attack scenario]

Attack Scenario 2: [TODO: Scenario Name] [TODO: Describe another attack scenario]

12.5 5. Organizational Security Policies

12.5.1 5.1 OSP Catalog

Organizational Security Policies:

OSP ID	OSP Name	Category	Mandatory	Description
[TODO: P.001]	[TODO: Policy Name]	[TODO: e.g., Access Control, Audit, Crypto]	Yes/No	[TODO: Description]
[TODO: P.002]	[TODO: Policy Name]	[TODO: Category]	Yes/No	[TODO: Description]

12.5.2 5.2 OSP Details

12.5.2.1 P.001: [TODO: Policy Name]

Description: [TODO: Detailed description of the policy]

Purpose: [TODO: Why is this policy required?]

Requirements: - [TODO: Requirement 1] - [TODO: Requirement 2] - [TODO: Requirement 3]

Scope: [TODO: Where does this policy apply?]

Compliance Requirements: [TODO: External standards or regulations this policy fulfills]

12.5.2.2 P.002: [TODO: Policy Name]

[TODO: Repeat structure for each OSP]

12.5.3 5.3 Policy Compliance Matrix

Mapping of Policies to External Standards:

OSP ID	ISO 27001	NIST 800-53	PCI-DSS	GDPR	Other
[TODO: P.001]	[TODO: Control]	[TODO: Control]	[TODO: Req]	[TODO: Article]	[TODO: Standard]
[TODO: P.002]	[TODO: Control]	[TODO: Control]	[TODO: Req]	[TODO: Article]	[TODO: Standard]

12.6 6. Assumptions

12.6.1 6.1 Assumption Catalog

Assumptions about the Operational Environment:

Assumption ID	Assumption Name	Category	Criticality	Description
[TODO: A.001]	[TODO: Assumption Name]	[TODO: e.g., Physical, Personnel, Connectivity]	High/Medium/Low	[TODO: Description]
[TODO: A.002]	[TODO: Assumption Name]	[TODO: Category]	High/Medium/Low	[TODO: Description]

12.6.2 6.2 Assumption Details

12.6.2.1 A.001: [TODO: Assumption Name]

Description: [TODO: Detailed description of the assumption]

Rationale: [TODO: Why is this assumption justified?]

Impact: [TODO: What happens if this assumption is not met?]

Responsibility: [TODO: Who is responsible for fulfilling this assumption?]

Verification: [TODO: How can it be verified that this assumption is met?]

12.6.2.2 A.002: [TODO: Assumption Name]

[TODO: Repeat structure for each assumption]

12.6.3 6.3 Environmental Assumptions

Physical Environment: - [TODO: Assumption about physical security] - [TODO: Assumption about environmental conditions]

Personnel: - [TODO: Assumption about user behavior] - [TODO: Assumption about administrator competence]

Connectivity: - [TODO: Assumption about network security] - [TODO: Assumption about communication channels]

12.7 7. Security Problem Summary

12.7.1 7.1 Threat Summary

Threat Summary: - Number of identified threats: [TODO: Number] - High-risk threats: [TODO: Number] - Medium-risk threats: [TODO: Number] - Low-risk threats: [TODO: Number]

12.7.2 7.2 OSP Summary

Policy Summary: - Number of organizational security policies: [TODO: Number] - Mandatory policies: [TODO: Number] - Optional policies: [TODO: Number]

12.7.3 7.3 Assumption Summary

Assumption Summary: - Number of assumptions: [TODO: Number] - Critical assumptions: [TODO: Number] - Medium criticality assumptions: [TODO: Number] - Low criticality assumptions: [TODO: Number]

12.7.4 7.4 Coverage Analysis

Coverage Analysis: [TODO: Analyze whether all assets are covered by threats, OSPs, or assumptions]

12.8 8. Traceability

12.8.1 8.1 Asset-to-Threat Mapping

Mapping of Assets to Threats:

Asset ID	Threats
[TODO: A.001]	[TODO: T.001, T.003, T.005]
[TODO: A.002]	[TODO: T.002, T.004]

12.8.2 8.2 Threat-to-Agent Mapping

Mapping of Threats to Agents:

Threat ID	Threat Agents
[TODO: T.001]	[TODO: TA.001, TA.002]
[TODO: T.002]	[TODO: TA.003]

12.8.3 8.3 Security Problem Traceability Matrix

Complete Traceability:

Asset	Threat	OSP	Assumption	Agent
[TODO: A.001]	[TODO: T.001]	[TODO: P.001]	[TODO: A.001]	[TODO: TA.001]
[TODO: A.002]	[TODO: T.002]	[TODO: P.002]	[TODO: A.002]	[TODO: TA.002]

Next Steps: 1. Complete all [TODO] placeholders with TOE-specific information 2. Conduct complete threat analysis 3. Document all relevant OSPs 4. Identify and validate all assumptions 5. Create threat model and attack scenarios 6. Verify consistency with Security Objectives (Template 0300)

ewpage

Chapter 13

Threats

Document-ID: 0210
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

13.1 1. Threat Overview

13.1.1 1.1 Threat Identification Methodology

Threat Identification Methodology: [TODO: Describe the methodology used, e.g., STRIDE, PASTA, Attack Trees]

Frameworks Used: - [TODO: e.g., MITRE ATT&CK] - [TODO: e.g., OWASP Top 10] - [TODO: e.g., CWE Top 25]

13.1.2 1.2 Threat Categories

Threat Categories: - **Confidentiality Threats**: Threats to confidentiality - **Integrity Threats**: Threats to integrity - **Availability Threats**: Threats to availability - **Authentication Threats**: Threats to authentication - **Authorization Threats**: Threats to authorization - **Non-Repudiation Threats**: Threats to non-repudiation

13.1.3 1.3 Threat Scope

In Scope: [TODO: Which threats are considered?]

Out of Scope: [TODO: Which threats are not considered and why?]

13.2 2. Confidentiality Threats

13.2.1 T.UNAUTHORIZED_ACCESS

Threat ID: T.UNAUTHORIZED_ACCESS
Category: Confidentiality
Priority: [TODO: High/Medium/Low]

Description: [TODO: An attacker could gain unauthorized access to confidential data]

Affected Assets: - [TODO: A.001 - User Data] - [TODO: A.002 - Configuration Data]

Threat Agent: - [TODO: TA.001 - External Attacker] - [TODO: TA.002 - Malicious Insider]

Attack Scenario: 1. [TODO: Attacker identifies vulnerability in access control] 2. [TODO: Attacker bypasses authentication] 3. [TODO: Attacker accesses confidential data] 4. [TODO: Attacker exfiltrates data]

Prerequisites: - [TODO: Network access to TOE] - [TODO: Knowledge of system architecture]

Impact: - **Confidentiality:** High - Complete loss of data control - **Integrity:** None - **Availability:** None

Likelihood: [TODO: High/Medium/Low]
Risk Assessment: [TODO: High/Medium/Low]

MITRE ATT&CK Mapping: - [TODO: T1078 - Valid Accounts] - [TODO: T1552 - Unsecured Credentials]

13.2.2 T.EAVESDROPPING

Threat ID: T.EAVESDROPPING
Category: Confidentiality
Priority: [TODO: High/Medium/Low]

Description: [TODO: An attacker could eavesdrop on communication and obtain confidential information]

Affected Assets: - [TODO: A.003 - Communication Data]

Threat Agent: - [TODO: TA.003 - Network Attacker]

Attack Scenario: 1. [TODO: Attacker positions themselves in network path] 2. [TODO: Attacker intercepts unencrypted communication] 3. [TODO: Attacker analyzes intercepted data]

Prerequisites: - [TODO: Access to network infrastructure] - [TODO: Unencrypted communication]

Impact: - **Confidentiality:** High - **Integrity:** None - **Availability:** None

Likelihood: [TODO: High/Medium/Low]
Risk Assessment: [TODO: High/Medium/Low]

13.2.3 T.DATA_LEAKAGE

Threat ID: T.DATA_LEAKAGE
Category: Confidentiality
Priority: [TODO: High/Medium/Low]

Description: [TODO: Confidential data could be unintentionally disclosed through errors or vulnerabilities]

[TODO: Add more Confidentiality Threats]

13.3 3. Integrity Threats

13.3.1 T.DATA_MANIPULATION

Threat ID: T.DATA_MANIPULATION
Category: Integrity
Priority: [TODO: High/Medium/Low]

Description: [TODO: An attacker could unauthorized modify or manipulate data]

Affected Assets: - [TODO: A.004 - Transaction Data] - [TODO: A.005 - Configuration Data]

Threat Agent: - [TODO: TA.001 - External Attacker] - [TODO: TA.002 - Malicious Insider]

Attack Scenario: 1. [TODO: Attacker gains write access] 2. [TODO: Attacker modifies critical data] 3. [TODO: Modification remains undetected] 4. [TODO: System processes manipulated data]

Prerequisites: - [TODO: Write access to data] - [TODO: Missing integrity checks]

Impact: - **Confidentiality:** None - **Integrity:** High - Data integrity compromised - **Availability:** None

Likelihood: [TODO: High/Medium/Low]
Risk Assessment: [TODO: High/Medium/Low]

13.3.2 T.CODE_INJECTION

Threat ID: T.CODE_INJECTION
Category: Integrity
Priority: [TODO: High/Medium/Low]

Description: [TODO: An attacker could inject malicious code into the system]

[TODO: Add more Integrity Threats]

13.4 4. Availability Threats

13.4.1 T.DENIAL_OF_SERVICE

Threat ID: T.DENIAL_OF_SERVICE
Category: Availability
Priority: [TODO: High/Medium/Low]

Description: [TODO: An attacker could impair TOE availability through overload]

Affected Assets: - [TODO: A.006 - Service Availability]

Threat Agent: - [TODO: TA.003 - Network Attacker]

Attack Scenario: 1. [TODO: Attacker sends large number of requests] 2. [TODO: System resources are exhausted] 3. [TODO: Legitimate requests can no longer be processed]

Prerequisites: - [TODO: Network access] - [TODO: Missing rate limiting]

Impact: - **Confidentiality:** None - **Integrity:** None - **Availability:** High - Service unavailable

Likelihood: [TODO: High/Medium/Low]
Risk Assessment: [TODO: High/Medium/Low]

13.4.2 T.RESOURCE_EXHAUSTION

Threat ID: T.RESOURCE_EXHAUSTION
Category: Availability
Priority: [TODO: High/Medium/Low]

Description: [TODO: An attacker could exhaust system resources]

[TODO: Add more Availability Threats]

13.5 5. Authentication Threats

13.5.1 T.AUTHENTICATION_BYPASS

Threat ID: T.AUTHENTICATION_BYPASS
Category: Authentication
Priority: [TODO: High/Medium/Low]

Description: [TODO: An attacker could bypass authentication mechanisms]

Affected Assets: - [TODO: A.007 - Authentication System]

Threat Agent: - [TODO: TA.001 - External Attacker]

Attack Scenario: 1. [TODO: Attacker identifies vulnerability in authentication] 2. [TODO: Attacker bypasses authentication check] 3. [TODO: Attacker gains unauthorized access]

Prerequisites: - [TODO: Access to authentication interface] - [TODO: Vulnerability in authentication logic]

Impact: - **Confidentiality:** High - **Integrity:** High - **Availability:** Medium

Likelihood: [TODO: High/Medium/Low]
Risk Assessment: [TODO: High/Medium/Low]

13.5.2 T.CREDENTIAL_THEFT

Threat ID: T.CREDENTIAL_THEFT
Category: Authentication
Priority: [TODO: High/Medium/Low]

Description: [TODO: An attacker could steal authentication credentials]

[TODO: Add more Authentication Threats]

13.6 6. Authorization Threats

13.6.1 T.PRIVILEGE_ESCALATION

Threat ID: T.PRIVILEGE_ESCALATION
Category: Authorization
Priority: [TODO: High/Medium/Low]

Description: [TODO: An attacker could unauthorized escalate their privileges]

Affected Assets: - [TODO: A.008 - Authorization System]

Threat Agent: - [TODO: TA.002 - Malicious Insider]

Attack Scenario: 1. [TODO: Attacker with low privileges identifies vulnerability] 2. [TODO: Attacker exploits vulnerability for privilege escalation] 3. [TODO: Attacker gains administrative rights]

Prerequisites: - [TODO: Valid user account] - [TODO: Vulnerability in authorization check]

Impact: - **Confidentiality:** High - **Integrity:** High - **Availability:** High

Likelihood: [TODO: High/Medium/Low]
Risk Assessment: [TODO: High/Medium/Low]

13.6.2 T.UNAUTHORIZED_FUNCTION_ACCESS

Threat ID: T.UNAUTHORIZED_FUNCTION_ACCESS
Category: Authorization
Priority: [TODO: High/Medium/Low]

Description: [TODO: An attacker could access functions they are not authorized for]

[TODO: Add more Authorization Threats]

13.7 7. Non-Repudiation Threats

13.7.1 T.REPUDIATION

Threat ID: T.REPUDIATION
Category: Non-Repudiation
Priority: [TODO: High/Medium/Low]

Description: [TODO: A user could deny performed actions]

Affected Assets: - [TODO: A.009 - Audit Logs]

Threat Agent: - [TODO: TA.002 - Malicious Insider]

Attack Scenario: 1. [TODO: User performs critical action] 2. [TODO: User manipulates or deletes audit logs] 3. [TODO: User denies action]

Prerequisites: - [TODO: Access to audit system] - [TODO: Missing log integrity]

Impact: - **Confidentiality:** None - **Integrity:** High - **Availability:** None

Likelihood: [TODO: High/Medium/Low]
Risk Assessment: [TODO: High/Medium/Low]

13.7.2 T.LOG_TAMPERING

Threat ID: T.LOG_TAMPERING
Category: Non-Repudiation
Priority: [TODO: High/Medium/Low]

Description: [TODO: An attacker could manipulate or delete audit logs]

[TODO: Add more Non-Repudiation Threats]

13.8 8. Threat Summary

13.8.1 8.1 Threat Statistics

Threat Statistics: - Total number of threats: [TODO: Number] - Confidentiality Threats: [TODO: Number] - Integrity Threats: [TODO: Number] - Availability Threats: [TODO: Number] - Authentication Threats: [TODO: Number] - Authorization Threats: [TODO: Number] - Non-Repudiation Threats: [TODO: Number]

13.8.2 8.2 Risk Distribution

Risk Distribution: - High Risk: [TODO: Number] ([TODO: %]) - Medium Risk: [TODO: Number] ([TODO: %]) - Low Risk: [TODO: Number] ([TODO: %])

13.8.3 8.3 Threat Priority Matrix

Priority Matrix:

Priority	Likelihood High	Likelihood Medium	Likelihood Low
Impact High	[TODO: Threat IDs]	[TODO: Threat IDs]	[TODO: Threat IDs]
Impact Medium	[TODO: Threat IDs]	[TODO: Threat IDs]	[TODO: Threat IDs]
Impact Low	[TODO: Threat IDs]	[TODO: Threat IDs]	[TODO: Threat IDs]

13.9 9. Threat Model

13.9.1 9.1 Attack Trees

Attack Trees for Critical Threats:

[TODO: Create attack trees for the most important threats]

`[TODO: Insert attack tree diagram]`

13.9.2 9.2 Threat Relationships

Relationships Between Threats:

[TODO: Describe how threats relate or enable each other]

`[TODO: Insert threat relationship diagram]`

13.9.3 9.3 Attack Chains

Attack Chains:

Chain 1: [TODO: Name] 1. [TODO: T.001] → [TODO: T.003] → [TODO: T.005] 2. [TODO: Description of attack chain]

Chain 2: [TODO: Name] 1. [TODO: T.002] → [TODO: T.004] 2. [TODO: Description of attack chain]

13.10 10. Traceability

13.10.1 10.1 Threat-to-Asset Mapping

Mapping Threats to Assets:

Threat ID	Affected Assets	Impact
[TODO: T.001]	[TODO: A.001, A.002]	[TODO: High]
[TODO: T.002]	[TODO: A.003]	[TODO: Medium]

13.10.2 10.2 Threat-to-Agent Mapping

Mapping Threats to Agents:

Threat ID	Threat Agents	Capability Required
[TODO: T.001]	[TODO: TA.001, TA.002]	[TODO: High]
[TODO: T.002]	[TODO: TA.003]	[TODO: Medium]

Next Steps: 1. Complete all [TODO] placeholders with TOE-specific threats 2. Conduct complete threat analysis 3. Create attack trees for critical threats 4. Assess risks for all threats 5. Document

attack chains 6. Verify consistency with Assets (Template 0200) and Security Objectives (Template 0300)

ewpage

Chapter 14

Organizational Security Policies (OSPs)

Document-ID: 0220
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

14.1 1. OSP Overview

14.1.1 1.1 Purpose

Organizational Security Policies (OSPs) define security rules and practices that: - Are mandated by the organization - Must be enforced or supported by the TOE - Apply independently of specific threats - Fulfill compliance requirements

14.1.2 1.2 OSP Categories

Policy Categories: - **Access Control Policies**: Access control policies - **Audit Policies**: Audit and logging policies - **Cryptographic Policies**: Cryptography policies - **Data Protection Policies**: Data protection policies - **Authentication Policies**: Authentication policies - **Configuration Policies**: Configuration policies - **Operational Policies**: Operational policies

14.1.3 1.3 Policy Scope

In Scope: [TODO: Which policies are enforced by the TOE?]

Out of Scope: [TODO: Which policies are not enforced by the TOE?]

14.2 2. Access Control Policies

14.2.1 P.ACCESS_CONTROL

Policy ID: P.ACCESS_CONTROL
Category: Access Control
Mandatory: [TODO: Yes/No]
Priority: [TODO: High/Medium/Low]

Description: [TODO: The TOE must implement access control mechanisms that ensure only authorized users can access protected resources]

Purpose: [TODO: Protection against unauthorized access to sensitive data and functions]

Requirements: - [TODO: Implementation of Role-Based Access Control (RBAC)] - [TODO: Enforcement of Least-Privilege principle] - [TODO: Regular review of access rights] - [TODO: Documentation of all access decisions]

Scope: [TODO: All users and administrators of the TOE]

Enforcement: - **TOE Responsibility:** [TODO: Implement access control mechanisms] - **Environment Responsibility:** [TODO: Define and assign user roles]

Compliance Requirements: - ISO 27001: A.9.1, A.9.2, A.9.4 - NIST 800-53: AC-2, AC-3, AC-6 - [TODO: Additional standards]

Verification: [TODO: How is compliance with this policy verified?]

14.2.2 P.NEED_TO_KNOW

Policy ID: P.NEED_TO_KNOW
Category: Access Control
Mandatory: [TODO: Yes/No]
Priority: [TODO: High/Medium/Low]

Description: [TODO: Access to information may only be granted when there is a legitimate need]

[TODO: Add more Access Control Policies]

14.3 3. Audit Policies

14.3.1 P.AUDIT_LOGGING

Policy ID: P.AUDIT_LOGGING
Category: Audit
Mandatory: [TODO: Yes/No]
Priority: [TODO: High/Medium/Low]

Description: [TODO: The TOE must log all security-relevant events and protect audit logs from unauthorized modification]

Purpose: [TODO: Traceability of actions and support for forensic analysis]

Requirements: - [TODO: Logging of all authentication attempts] - [TODO: Logging of all accesses to sensitive data] - [TODO: Logging of all administrative actions] - [TODO: Protection of audit logs from tampering] - [TODO: Regular review of audit logs] - [TODO: Retention of logs for [TODO: period]]

Scope: [TODO: All users and system components]

Enforcement: - **TOE Responsibility:** [TODO: Implement audit mechanisms] - **Environment Responsibility:** [TODO: Provide and monitor log storage]

Compliance Requirements: - ISO 27001: A.12.4 - NIST 800-53: AU-2, AU-3, AU-9 - [TODO: Additional standards]

Verification: [TODO: How is compliance with this policy verified?]

14.3.2 P.AUDIT_REVIEW

Policy ID: P.AUDIT_REVIEW
Category: Audit
Mandatory: [TODO: Yes/No]
Priority: [TODO: High/Medium/Low]

Description: [TODO: Audit logs must be regularly reviewed to detect security incidents]

[TODO: Add more Audit Policies]

14.4 4. Cryptographic Policies

14.4.1 P.CRYPTOGRAPHY

Policy ID: P.CRYPTOGRAPHY
Category: Cryptographic
Mandatory: [TODO: Yes/No]
Priority: [TODO: High/Medium/Low]

Description: [TODO: The TOE must use cryptographic mechanisms to ensure confidentiality and integrity]

Purpose: [TODO: Protection of sensitive data through encryption]

Requirements: - [TODO: Use of approved cryptographic algorithms] - [TODO: Minimum key lengths: AES-256, RSA-2048, etc.] - [TODO: Secure key management and storage] - [TODO: Regular key rotation] - [TODO: Use of TLS 1.2 or higher for communication] - [TODO: Use of FIPS 140-2 validated crypto modules]

Scope: [TODO: All encrypted data and communication channels]

Enforcement: - **TOE Responsibility:** [TODO: Implement cryptographic functions] - **Environment Responsibility:** [TODO: Manage cryptographic keys]

Compliance Requirements: - ISO 27001: A.10.1 - NIST 800-53: SC-12, SC-13 - FIPS 140-2 - [TODO: Additional standards]

Verification: [TODO: How is compliance with this policy verified?]

14.4.2 P.KEY_MANAGEMENT

Policy ID: P.KEY_MANAGEMENT
Category: Cryptographic
Mandatory: [TODO: Yes/No]
Priority: [TODO: High/Medium/Low]

Description: [TODO: Cryptographic keys must be securely generated, stored, and managed]

[TODO: Add more Cryptographic Policies]

14.5 5. Data Protection Policies

14.5.1 P.DATA_CLASSIFICATION

Policy ID: P.DATA_CLASSIFICATION
Category: Data Protection
Mandatory: [TODO: Yes/No]
Priority: [TODO: High/Medium/Low]

Description: [TODO: All data must be classified and protected according to its classification]

Purpose: [TODO: Appropriate protection of data based on its sensitivity]

Requirements: - [TODO: Classification scheme: Public, Internal, Confidential, Restricted] - [TODO: Labeling of all data with classification] - [TODO: Protection measures according to classification] - [TODO: Regular review of classification]

Scope: [TODO: All data processed in the TOE]

Enforcement: - **TOE Responsibility:** [TODO: Classification-based access control] - **Environment Responsibility:** [TODO: Perform data classification]

Compliance Requirements: - ISO 27001: A.8.2 - GDPR: Article 32 - [TODO: Additional standards]

Verification: [TODO: How is compliance with this policy verified?]

14.5.2 P.DATA_RETENTION

Policy ID: P.DATA_RETENTION
Category: Data Protection
Mandatory: [TODO: Yes/No]
Priority: [TODO: High/Medium/Low]

Description: [TODO: Data must be stored and deleted according to retention policies]

[TODO: Add more Data Protection Policies]

14.6 6. Authentication Policies

14.6.1 P.STRONG_AUTHENTICATION

Policy ID: P.STRONG_AUTHENTICATION
Category: Authentication
Mandatory: [TODO: Yes/No]
Priority: [TODO: High/Medium/Low]

Description: [TODO: The TOE must implement strong authentication mechanisms]

Purpose: [TODO: Ensuring user identity]

Requirements: - [TODO: Multi-Factor Authentication (MFA) for privileged accounts] - [TODO: Password policies: minimum length, complexity, expiration] - [TODO: Account lockout after failed login attempts] - [TODO: Secure storage of authentication data (hashing)] - [TODO: Session timeout after inactivity]

Scope: [TODO: All users of the TOE]

Enforcement: - **TOE Responsibility:** [TODO: Implement authentication mechanisms] - **Environment Responsibility:** [TODO: Train and monitor users]

Compliance Requirements: - ISO 27001: A.9.4 - NIST 800-53: IA-2, IA-5 - [TODO: Additional standards]

Verification: [TODO: How is compliance with this policy verified?]

14.6.2 P.PASSWORD_POLICY

Policy ID: P.PASSWORD_POLICY
Category: Authentication
Mandatory: [TODO: Yes/No]
Priority: [TODO: High/Medium/Low]

Description: [TODO: Passwords must meet certain complexity and security requirements]

[TODO: Add more Authentication Policies]

14.7 7. Configuration Policies

14.7.1 P.SECURE_CONFIGURATION

Policy ID: P.SECURE_CONFIGURATION
Category: Configuration
Mandatory: [TODO: Yes/No]
Priority: [TODO: High/Medium/Low]

Description: [TODO: The TOE must be operated in a secure configuration]

Purpose: [TODO: Minimizing attack surface through secure configuration]

Requirements: - [TODO: Disabling of unnecessary services and functions] - [TODO: Use of secure default settings] - [TODO: Regular review of configuration] - [TODO: Documentation of all configuration changes] - [TODO: Change management process for configuration changes]

Scope: [TODO: All TOE components]

Enforcement: - **TOE Responsibility:** [TODO: Provide secure default configuration] - **Environment Responsibility:** [TODO: Monitor and manage configuration]

Compliance Requirements: - ISO 27001: A.12.6 - NIST 800-53: CM-6, CM-7 - CIS Controls - [TODO: Additional standards]

Verification: [TODO: How is compliance with this policy verified?]

14.7.2 P.CONFIGURATION_MANAGEMENT

Policy ID: P.CONFIGURATION_MANAGEMENT
Category: Configuration
Mandatory: [TODO: Yes/No]
Priority: [TODO: High/Medium/Low]

Description: [TODO: Configuration changes must be controlled and documented]

[TODO: Add more Configuration Policies]

14.8 8. Operational Policies

14.8.1 P.SECURITY_UPDATES

Policy ID: P.SECURITY_UPDATES
Category: Operational
Mandatory: [TODO: Yes/No]
Priority: [TODO: High/Medium/Low]

Description: [TODO: Security updates must be installed promptly]

Purpose: [TODO: Protection against known vulnerabilities]

Requirements: - [TODO: Regular checking for available updates] - [TODO: Assessment and prioritization of updates] - [TODO: Timely installation of critical security updates] - [TODO: Testing of updates before production installation] - [TODO: Documentation of all installed updates]

Scope: [TODO: All TOE components]

Enforcement: - **TOE Responsibility:** [TODO: Provide update mechanism] - **Environment Responsibility:** [TODO: Install and manage updates]

Compliance Requirements: - ISO 27001: A.12.6.1 - NIST 800-53: SI-2 - [TODO: Additional standards]

Verification: [TODO: How is compliance with this policy verified?]

14.8.2 P.BACKUP_RECOVERY

Policy ID: P.BACKUP_RECOVERY
Category: Operational
Mandatory: [TODO: Yes/No]
Priority: [TODO: High/Medium/Low]

Description: [TODO: Regular backups must be created and tested]

[TODO: Add more Operational Policies]

14.9 9. Policy Compliance Matrix

14.9.1 9.1 Standards Mapping

Mapping to External Standards:

OSP ID	ISO 27001	NIST 800-53	PCI-DSS	GDPR	HIPAA	SOC 2
[TODO: P.001]	[TODO: A.9.1]	[TODO: AC-2]	[TODO: 7.1]	[TODO: Art. 32]	[TODO: §164.312]	[TODO: CC6.1]
[TODO: P.002]	[TODO: A.12.4]	[TODO: AU-2]	[TODO: 10.1]	[TODO: Art. 30]	[TODO: §164.312]	[TODO: CC7.2]

14.9.2 9.2 Regulatory Compliance

Regulatory Requirements:

Regulation	Applicable OSPs	Compliance Status
[TODO: GDPR]	[TODO: P.001, P.003, P.005]	[TODO: Compliant/Partial/Non-Compliant]
[TODO: HIPAA]	[TODO: P.002, P.004]	[TODO: Compliant/Partial/Non-Compliant]
[TODO: PCI-DSS]	[TODO: P.001, P.002, P.006]	[TODO: Compliant/Partial/Non-Compliant]

14.9.3 9.3 Industry Standards

Industry Standards:

Standard	Applicable OSPs	Compliance Status
[TODO: ISO 27001]	[TODO: All OSPs]	[TODO: Compliant/Partial/Non-Compliant]
[TODO: NIST 800-53]	[TODO: P.001-P.010]	[TODO: Compliant/Partial/Non-Compliant]
[TODO: CIS Controls]	[TODO: P.003, P.007]	[TODO: Compliant/Partial/Non-Compliant]

14.10 10. Policy Summary

14.10.1 10.1 Policy Statistics

Policy Statistics: - Total number of OSPs: [TODO: Number] - Mandatory policies: [TODO: Number] - Optional policies: [TODO: Number] - Access Control Policies: [TODO: Number] - Audit Policies: [TODO: Number] - Cryptographic Policies: [TODO: Number] - Data Protection Policies: [TODO: Number] - Authentication Policies: [TODO: Number] - Configuration Policies: [TODO: Number] - Operational Policies: [TODO: Number]

14.10.2 10.2 Enforcement Responsibility

Enforcement Responsibility:

Responsibility	Number of OSPs	OSP IDs
TOE Only	[TODO: Number]	[TODO: P.001, P.003]
Environment Only	[TODO: Number]	[TODO: P.005]
Shared (TOE + Environment)	[TODO: Number]	[TODO: P.002, P.004]

14.10.3 10.3 Priority Distribution

Priority Distribution: - High Priority: [TODO: Number] ([TODO: %]) - Medium Priority: [TODO: Number] ([TODO: %]) - Low Priority: [TODO: Number] ([TODO: %])

14.11 11. Traceability

14.11.1 11.1 OSP-to-Threat Mapping

Mapping OSPs to Threats:

OSP ID	Addresses Threats	Rationale
[TODO: P.001]	[TODO: T.001, T.003]	[TODO: Rationale]
[TODO: P.002]	[TODO: T.002, T.005]	[TODO: Rationale]

14.11.2 11.2 OSP-to-Asset Mapping

Mapping OSPs to Assets:

OSP ID	Protects Assets	Protection Type
[TODO: P.001]	[TODO: A.001, A.002]	[TODO: Confidentiality/Integrity/Availability]
[TODO: P.002]	[TODO: A.003]	[TODO: Integrity]

Next Steps: 1. Complete all [TODO] placeholders with organization-specific policies 2. Document all relevant OSPs 3. Map OSPs to external standards 4. Define enforcement mechanisms 5. Create compliance matrix 6. Verify consistency with Threats (Template 0210) and Security Objectives (Template 0300)

ewpage

Chapter 15

Assumptions

Document-ID: 0230
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

15.1 1. Assumptions Overview

15.1.1 1.1 Purpose

Assumptions define expectations about the TOE's operational environment: - **Physical Environment**: Assumptions about physical security and infrastructure - **Personnel**: Assumptions about users, administrators, and their behavior - **Connectivity**: Assumptions about network and communication infrastructure - **Technical Environment**: Assumptions about IT infrastructure and platforms

15.1.2 1.2 Assumption Categories

Assumption Categories: - **Physical Assumptions**: Physical security assumptions - **Personnel Assumptions**: Personnel assumptions - **Connectivity Assumptions**: Connectivity assumptions - **Platform Assumptions**: Platform assumptions - **Operational Assumptions**: Operational assumptions

15.1.3 1.3 Assumption Scope

In Scope: [TODO: Which aspects of the environment are covered by assumptions?]

Out of Scope: [TODO: Which aspects are not covered by assumptions?]

15.2 2. Physical Assumptions

15.2.1 A.PHYSICAL_SECURITY

Assumption ID: A.PHYSICAL_SECURITY
Category: Physical
Criticality: [TODO: High/Medium/Low]
Mandatory: [TODO: Yes/No]

Description: [TODO: The TOE is operated in a physically secure environment protected from unauthorized physical access]

Rationale: [TODO: Physical security is required to prevent hardware tampering and direct system access]

Requirements: - [TODO: Access control to server rooms] - [TODO: Video surveillance of critical areas] - [TODO: Alarm system for unauthorized access] - [TODO: Secure storage of backup media] - [TODO: Visitor log and escort requirement]

Impact if Not Met: [TODO: Describe security risks if this assumption is not met] - Risk: [TODO: e.g., Hardware tampering, theft] - Affected Assets: [TODO: A.001, A.002] - Affected Threats: [TODO: T.001, T.003]

Responsibility: - **Primary:** [TODO: Facility Management] - **Secondary:** [TODO: Security Team]

Verification: [TODO: How is it verified that this assumption is met?] - Method: [TODO: e.g., Physical inspection, audit] - Frequency: [TODO: e.g., Annually, Quarterly] - Documentation: [TODO: e.g., Audit report, checklist]

15.2.2 A.ENVIRONMENTAL_PROTECTION

Assumption ID: A.ENVIRONMENTAL_PROTECTION
Category: Physical
Criticality: [TODO: High/Medium/Low]
Mandatory: [TODO: Yes/No]

Description: [TODO: The TOE is operated in an environment protected from environmental hazards]

Rationale: [TODO: Protection from fire, water, temperature, humidity is required for availability]

Requirements: - [TODO: Air conditioning and temperature control] - [TODO: Fire detection and suppression system] - [TODO: Water protection and leak detection] - [TODO: Uninterruptible Power Supply (UPS)] - [TODO: Emergency power supply]

[TODO: Add more Physical Assumptions]

15.3 3. Personnel Assumptions

15.3.1 A.TRUSTED_ADMIN

Assumption ID: A.TRUSTED_ADMIN
Category: Personnel
Criticality: [TODO: High/Medium/Low]
Mandatory: [TODO: Yes/No]

Description: [TODO: Administrators are trustworthy, competent, and do not act maliciously]

Rationale: [TODO: Administrators have privileged access and can bypass security mechanisms]

Requirements: - [TODO: Background checks before hiring] - [TODO: Signing of confidentiality agreements] - [TODO: Regular security training] - [TODO: Four-eyes principle for critical operations] - [TODO: Monitoring of administrative activities] - [TODO: Regular review of administrator rights]

Impact if Not Met: [TODO: Describe security risks] - Risk: [TODO: e.g., Insider threat, sabotage, data theft] - Affected Assets: [TODO: All assets] - Affected Threats: [TODO: T.002, T.004, T.006]

Responsibility: - **Primary:** [TODO: HR Department] - **Secondary:** [TODO: Security Team, IT Management]

Verification: [TODO: How is it verified that this assumption is met?] - Method: [TODO: e.g., Background checks, audit log review] - Frequency: [TODO: e.g., At hiring, annually] - Documentation: [TODO: e.g., HR file, training records]

15.3.2 A.USER_TRAINING

Assumption ID: A.USER_TRAINING
Category: Personnel
Criticality: [TODO: High/Medium/Low]
Mandatory: [TODO: Yes/No]

Description: [TODO: Users are trained and follow security policies]

Rationale: [TODO: Users must understand and correctly use security mechanisms]

Requirements: - [TODO: Security training before system access] - [TODO: Regular refresher training] - [TODO: Phishing awareness training] - [TODO: Training on password policies] - [TODO: Training on data classification] - [TODO: Incident reporting training]

[TODO: Add more Personnel Assumptions]

15.4 4. Connectivity Assumptions

15.4.1 A.NETWORK_SECURITY

Assumption ID: A.NETWORK_SECURITY
Category: Connectivity

Criticality: [TODO: High/Medium/Low]
Mandatory: [TODO: Yes/No]

Description: [TODO: The network in which the TOE operates is protected by firewalls and other security mechanisms]

Rationale: [TODO: Network security is required to defend against external attacks]

Requirements: - [TODO: Firewall between TOE and Internet] - [TODO: Network segmentation] - [TODO: Intrusion Detection/Prevention System (IDS/IPS)] - [TODO: Regular network scans] - [TODO: VPN for remote access] - [TODO: DDoS protection]

Impact if Not Met: [TODO: Describe security risks] - Risk: [TODO: e.g., Network attacks, data exfiltration] - Affected Assets: [TODO: A.003, A.004] - Affected Threats: [TODO: T.005, T.007]

Responsibility: - **Primary:** [TODO: Network Team] - **Secondary:** [TODO: Security Team]

Verification: [TODO: How is it verified that this assumption is met?] - Method: [TODO: e.g., Network audit, penetration test] - Frequency: [TODO: e.g., Quarterly] - Documentation: [TODO: e.g., Network diagram, firewall rules]

15.4.2 A.SECURE_COMMUNICATION

Assumption ID: A.SECURE_COMMUNICATION
Category: Connectivity
Criticality: [TODO: High/Medium/Low]
Mandatory: [TODO: Yes/No]

Description: [TODO: Communication channels between TOE and external systems are encrypted]

Rationale: [TODO: Encryption protects against eavesdropping and man-in-the-middle attacks]

Requirements: - [TODO: TLS 1.2 or higher for all connections] - [TODO: Certificate validation] - [TODO: Secure cipher suites] - [TODO: Regular certificate renewal]

[TODO: Add more Connectivity Assumptions]

15.5 5. Platform Assumptions

15.5.1 A.TRUSTED_PLATFORM

Assumption ID: A.TRUSTED_PLATFORM
Category: Platform
Criticality: [TODO: High/Medium/Low]
Mandatory: [TODO: Yes/No]

Description: [TODO: The platform on which the TOE runs is trustworthy and securely configured]

Rationale: [TODO: TOE security depends on the security of the underlying platform]

Requirements: - [TODO: Current and patched operating system] - [TODO: Hardening according to best practices (e.g., CIS Benchmarks)] - [TODO: Disabling of unnecessary services] - [TODO:

Host-based firewall] - [TODO: Antivirus/Endpoint Protection] - [TODO: Regular vulnerability scans]

Impact if Not Met: [TODO: Describe security risks] - Risk: [TODO: e.g., Platform compromise, privilege escalation] - Affected Assets: [TODO: All assets] - Affected Threats: [TODO: T.008, T.009]

Responsibility: - **Primary:** [TODO: System Administration] - **Secondary:** [TODO: Security Team]

Verification: [TODO: How is it verified that this assumption is met?] - Method: [TODO: e.g., Configuration audit, vulnerability scan] - Frequency: [TODO: e.g., Monthly] - Documentation: [TODO: e.g., Scan reports, configuration documentation]

15.5.2 A.PLATFORM_AVAILABILITY

Assumption ID: A.PLATFORM_AVAILABILITY
Category: Platform
Criticality: [TODO: High/Medium/Low]
Mandatory: [TODO: Yes/No]

Description: [TODO: The platform provides sufficient resources and availability for TOE operation]

Rationale: [TODO: TOE requires sufficient resources for proper operation]

Requirements: - [TODO: Sufficient CPU capacity] - [TODO: Sufficient memory] - [TODO: Sufficient storage space] - [TODO: High availability architecture (if required)] - [TODO: Regular capacity planning]

[TODO: Add more Platform Assumptions]

15.6 6. Operational Assumptions

15.6.1 A.SECURITY_MONITORING

Assumption ID: A.SECURITY_MONITORING
Category: Operational
Criticality: [TODO: High/Medium/Low]
Mandatory: [TODO: Yes/No]

Description: [TODO: Security events are continuously monitored and analyzed]

Rationale: [TODO: Early detection of security incidents is critical]

Requirements: - [TODO: 24/7 Security Operations Center (SOC)] - [TODO: SIEM system for log aggregation and analysis] - [TODO: Automatic alerting for critical events] - [TODO: Defined incident response processes] - [TODO: Regular review of security events]

Impact if Not Met: [TODO: Describe security risks] - Risk: [TODO: e.g., Delayed detection of attacks] - Affected Assets: [TODO: All assets] - Affected Threats: [TODO: All threats]

Responsibility: - **Primary:** [TODO: Security Operations Team] - **Secondary:** [TODO: IT Operations]

Verification: [TODO: How is it verified that this assumption is met?] - Method: [TODO: e.g., SOC audit, incident response test] - Frequency: [TODO: e.g., Quarterly] - Documentation: [TODO: e.g., SOC reports, incident logs]

15.6.2 A.BACKUP_RECOVERY

Assumption ID: A.BACKUP_RECOVERY
Category: Operational
Criticality: [TODO: High/Medium/Low]
Mandatory: [TODO: Yes/No]

Description: [TODO: Regular backups are created and recovery processes are tested]

Rationale: [TODO: Backups are required for disaster recovery and business continuity]

Requirements: - [TODO: Daily incremental backups] - [TODO: Weekly full backups] - [TODO: Offsite storage of backups] - [TODO: Encryption of backup data] - [TODO: Regular recovery tests] - [TODO: Documented recovery procedures]

[TODO: Add more Operational Assumptions]

15.7 7. Assumption Summary

15.7.1 7.1 Assumption Statistics

Assumption Statistics: - Total number of assumptions: [TODO: Number] - Physical Assumptions: [TODO: Number] - Personnel Assumptions: [TODO: Number] - Connectivity Assumptions: [TODO: Number] - Platform Assumptions: [TODO: Number] - Operational Assumptions: [TODO: Number]

15.7.2 7.2 Criticality Distribution

Criticality Distribution: - High Criticality: [TODO: Number] ([TODO: %]) - Medium Criticality: [TODO: Number] ([TODO: %]) - Low Criticality: [TODO: Number] ([TODO: %])

15.7.3 7.3 Mandatory vs. Optional

Mandatory vs. Optional Assumptions: - Mandatory: [TODO: Number] ([TODO: %]) - Optional: [TODO: Number] ([TODO: %])

15.8 8. Assumption Validation

15.8.1 8.1 Validation Methods

Validation Methods:

Assumption ID	Validation Method	Frequency	Responsible Party
[TODO: A.001]	[TODO: Method]	[TODO: Frequency]	[TODO: Responsible]

Assumption ID	Validation Method	Frequency	Responsible Party
[TODO: A.002]	[TODO: Method]	[TODO: Frequency]	[TODO: Responsible]

15.8.2 8.2 Validation Schedule

Validation Schedule: - [TODO: Monthly]: [TODO: A.001, A.003] - [TODO: Quarterly]: [TODO: A.002, A.004, A.005] - [TODO: Annually]: [TODO: A.006, A.007]

15.8.3 8.3 Validation Documentation

Validation Documentation: [TODO: Describe how validation results are documented]

15.9 9. Responsibility Matrix

15.9.1 9.1 Primary Responsibilities

Primary Responsibilities:

Organization Unit	Assumptions	Count
[TODO: Facility Management]	[TODO: A.001, A.002]	[TODO: 2]
[TODO: HR Department]	[TODO: A.003, A.004]	[TODO: 2]
[TODO: Network Team]	[TODO: A.005, A.006]	[TODO: 2]
[TODO: System Administration]	[TODO: A.007, A.008]	[TODO: 2]
[TODO: Security Operations]	[TODO: A.009, A.010]	[TODO: 2]

15.9.2 9.2 Shared Responsibilities

Shared Responsibilities: [TODO: Describe assumptions with shared responsibilities]

15.10 10. Traceability

15.10.1 10.1 Assumption-to-Threat Mapping

Mapping Assumptions to Threats:

Assumption ID	Mitigates Threats	Rationale
[TODO: A.001]	[TODO: T.001, T.003]	[TODO: Rationale]
[TODO: A.002]	[TODO: T.002, T.005]	[TODO: Rationale]

15.10.2 10.2 Assumption-to-Asset Mapping

Mapping Assumptions to Assets:

Assumption ID	Protects Assets	Protection Type
[TODO: A.001]	[TODO: A.001, A.002]	[TODO: Physical Protection]
[TODO: A.002]	[TODO: A.003]	[TODO: Availability]

15.10.3 10.3 Assumption-to-OSP Mapping

Mapping Assumptions to OSPs:

Assumption ID	Supports OSPs	Relationship
[TODO: A.001]	[TODO: P.001, P.003]	[TODO: Enables enforcement]
[TODO: A.002]	[TODO: P.002]	[TODO: Prerequisite]

Next Steps: 1. Complete all [TODO] placeholders with environment-specific assumptions 2. Document all relevant assumptions 3. Define validation methods 4. Assign responsibilities 5. Create validation schedule 6. Verify consistency with Threats (Template 0210), OSPs (Template 0220), and Security Objectives (Template 0300)

ewpage

Chapter 16

Threat Agents and Assets

Document-ID: 0240
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

16.1 1. Overview

16.1.1 1.1 Purpose

This document defines: - **Threat Agents**: Potential attackers with their capabilities and motivations - **Assets**: Resources, data, and functions to be protected

16.1.2 1.2 Scope

In Scope: [TODO: What is covered in this document?]

Out of Scope: [TODO: What is not covered?]

16.2 2. Assets

16.2.1 2.1 Asset Identification

16.2.1.1 2.1.1 Asset Categories

Asset Categories: - **Data Assets**: Data and information - **Service Assets**: Services and functions - **System Assets**: System components and infrastructure - **Credential Assets**: Authentication and authorization data - **Configuration Assets**: Configuration data and settings

16.2.1.2 2.1.2 Asset Inventory

Asset Inventory:

Asset ID	Asset Name	Category	Owner	Location	Description
[TODO: A.001]	[TODO: Name]	[TODO: Data/Service/System]	[TODO: Owner]	[TODO: Location]	[TODO: Description]
[TODO: A.002]	[TODO: Name]	[TODO: Category]	[TODO: Owner]	[TODO: Location]	[TODO: Description]
[TODO: A.003]	[TODO: Name]	[TODO: Category]	[TODO: Owner]	[TODO: Location]	[TODO: Description]

16.2.2 2.2 Data Assets

16.2.2.1 A.USER_DATA

Asset ID: A.USER_DATA
Category: Data
Type: [TODO: Personal Data / Business Data / Technical Data]

Description: [TODO: User data including personal information, preferences, and profile data]

Properties: - **Confidentiality:** [TODO: High/Medium/Low] - **Integrity:** [TODO: High/Medium/Low] - **Availability:** [TODO: High/Medium/Low] - **Data Volume:** [TODO: e.g., 1 TB] - **Data Format:** [TODO: e.g., JSON, XML, Database]

Protection Needs: - **Confidentiality:** [TODO: Rationale for protection need] - **Integrity:** [TODO: Rationale for protection need] - **Availability:** [TODO: Rationale for protection need]

Regulatory Requirements: - [TODO: GDPR Article 32 - Security of processing] - [TODO: HIPAA §164.312 - Technical safeguards] - [TODO: Additional requirements]

Value: - **Business Value:** [TODO: High/Medium/Low] - **Monetary Value:** [TODO: Estimate] - **Reputation Value:** [TODO: High/Medium/Low]

Lifecycle: - **Creation:** [TODO: How is data created?] - **Storage:** [TODO: Where is data stored?] - **Processing:** [TODO: How is data processed?] - **Transmission:** [TODO: How is data transmitted?] - **Archiving:** [TODO: How is data archived?] - **Deletion:** [TODO: How is data deleted?]

16.2.2.2 A.AUTHENTICATION_DATA

Asset ID: A.AUTHENTICATION_DATA
Category: Credential
Type: [TODO: Passwords / Tokens / Certificates]

Description: [TODO: Authentication data such as passwords, tokens, certificates]

[TODO: Add more Data Assets]

16.2.3 2.3 Service Assets

16.2.3.1 A.AUTHENTICATION_SERVICE

Asset ID: A.AUTHENTICATION_SERVICE
Category: Service

Type: [TODO: Authentication / Authorization / Identity Management]

Description: [TODO: Authentication service that verifies user identities]

Properties: - **Availability:** [TODO: 99.9% SLA] - **Performance:** [TODO: < 100ms Response Time] - **Capacity:** [TODO: 1000 req/sec]

Protection Needs: - **Availability:** [TODO: High - Critical for system access] - **Integrity:** [TODO: High - False authentication compromises security] - **Confidentiality:** [TODO: Medium - Metadata can be sensitive]

Dependencies: - [TODO: A.AUTHENTICATION_DATA] - [TODO: A.USER_DATABASE] - [TODO: A.NETWORK_CONNECTIVITY]

Value: - **Business Value:** [TODO: High - Fundamental security function] - **Criticality:** [TODO: High - System unusable without authentication]

16.2.3.2 A.DATA_PROCESSING_SERVICE

Asset ID: A.DATA_PROCESSING_SERVICE
Category: Service
Type: [TODO: Processing / Computation / Transformation]

Description: [TODO: Service for processing business data]

[TODO: Add more Service Assets]

16.2.4 2.4 System Assets

16.2.4.1 A.TOE_PLATFORM

Asset ID: A.TOE_PLATFORM
Category: System
Type: [TODO: Hardware / Software / Firmware]

Description: [TODO: The platform on which the TOE runs]

Components: - [TODO: Operating system] - [TODO: Hardware platform] - [TODO: Virtualization layer] - [TODO: Container runtime]

Protection Needs: - **Availability:** [TODO: High] - **Integrity:** [TODO: High] - **Confidentiality:** [TODO: Medium]

Criticality: [TODO: High - Platform compromise endangers all assets]

16.2.4.2 A.CRYPTOGRAPHIC_KEYS

Asset ID: A.CRYPTOGRAPHIC_KEYS
Category: System
Type: [TODO: Encryption Keys / Signing Keys / Certificates]

Description: [TODO: Cryptographic keys for encryption and signing]

[TODO: Add more System Assets]

16.2.5 2.5 Asset Classification

16.2.5.1 2.5.1 Classification Scheme

Classification Scheme:

Classification	Confidentiality	Integrity	Availability	Examples
Critical	High	High	High	[TODO: A.001, A.003]
High	High	High	Medium	[TODO: A.002, A.005]
Medium	Medium	Medium	Medium	[TODO: A.004, A.006]
Low	Low	Low	Low	[TODO: A.007]

16.2.5.2 2.5.2 Asset Value Matrix

Asset Value Matrix:

Asset ID	Business Value	Regulatory Value	Reputation Value	Total Value
[TODO: A.001]	[TODO: High]	[TODO: High]	[TODO: High]	[TODO: Critical]
[TODO: A.002]	[TODO: Medium]	[TODO: High]	[TODO: Medium]	[TODO: High]

16.2.6 2.6 Asset Dependencies

16.2.6.1 2.6.1 Dependency Graph

Asset Dependencies:

[TODO: Create a diagram showing asset dependencies]

```
[TODO: Insert asset dependency diagram]
```

16.2.6.2 2.6.2 Dependency Matrix

Dependency Matrix:

Asset	Depends On	Impact if Unavailable
[TODO: A.001]	[TODO: A.003, A.005]	[TODO: Service unavailable]
[TODO: A.002]	[TODO: A.004]	[TODO: Data processing not possible]

16.3 3. Threat Agents

16.3.1 3.1 Threat Agent Identification

16.3.1.1 3.1.1 Agent Categories

Agent Categories: - **External Attackers**: External attackers without legitimate access - **Insiders**: Employees with legitimate access - **Privileged Insiders**: Administrators with privileged access - **Nation-State Actors**: State-sponsored attackers - **Organized Crime**: Organized crime - **Hacktivists**: Ideologically motivated attackers - **Script Kiddies**: Inexperienced attackers with pre-made tools

16.3.1.2 3.1.2 Agent Inventory

Agent Inventory:

Agent ID	Agent Type	Motivation	Capability	Resources	Description
[TODO: TA.001]	[TODO: External Attacker]	[TODO: Financial]	[TODO: High]	[TODO: High]	[TODO: Description]
[TODO: TA.002]	[TODO: Insider]	[TODO: Revenge]	[TODO: Medium]	[TODO: Medium]	[TODO: Description]
[TODO: TA.003]	[TODO: Nation-State]	[TODO: Espionage]	[TODO: Very High]	[TODO: Very High]	[TODO: Description]

16.3.2 3.2 Threat Agent Profiles

16.3.2.1 TA.EXTERNAL_ATTACKER

Agent ID: TA.EXTERNAL_ATTACKER
Type: External Attacker
Skill Level: [TODO: Expert / Proficient / Layman]

Description: [TODO: External attacker without legitimate system access attempting to intrude via network or other external interfaces]

Motivation: - **Primary:** [TODO: e.g., Financial gain, data theft] - **Secondary:** [TODO: e.g., Reputation, challenge]

Capabilities: - **Technical Expertise:** [TODO: High - Knowledge in network security, exploitation] - **Tools:** [TODO: Metasploit, Burp Suite, Custom Scripts] - **Knowledge:** [TODO: Publicly available information, OSINT] - **Access:** [TODO: Network access, no physical access]

Resources: - **Time:** [TODO: Weeks to months] - **Budget:** [TODO: $10,000 - $100,000] - **Team:** [TODO: 1-5 people] - **Infrastructure:** [TODO: Cloud resources, botnets]

Attack Vectors: - [TODO: Network attacks (SQL Injection, XSS, etc.)] - [TODO: Social engineering (phishing)] - [TODO: Exploitation of known vulnerabilities] - [TODO: Brute-force attacks] - [TODO: DDoS attacks]

Attack Potential: [TODO: High - Based on CCRA Attack Potential Methodology]

Example Scenarios: 1. [TODO: Scenario 1] 2. [TODO: Scenario 2]

16.3.2.2 TA.MALICIOUS_INSIDER

Agent ID: TA.MALICIOUS_INSIDER
Type: Insider
Skill Level: [TODO: Expert / Proficient / Layman]

Description: [TODO: Malicious employee with legitimate system access]

Motivation: - **Primary:** [TODO: e.g., Revenge, financial gain] - **Secondary:** [TODO: e.g., Ideology, blackmail]

Capabilities: - **Technical Expertise:** [TODO: Medium - Basic IT knowledge] - **Tools:** [TODO: Standard user tools, USB drives] - **Knowledge:** [TODO: Insider knowledge of systems and processes] - **Access:** [TODO: Legitimate user access, physical access]

Resources: - **Time:** [TODO: Days to weeks] - **Budget:** [TODO: Minimal] - **Team:** [TODO: Individual] - **Infrastructure:** [TODO: Company resources]

Attack Vectors: - [TODO: Data exfiltration via USB or email] - [TODO: Sabotage of systems or data] - [TODO: Abuse of access rights] - [TODO: Sharing credentials with external parties]

Attack Potential: [TODO: Medium-High - Insider access compensates for lower technical skills]

16.3.2.3 TA.PRIVILEGED_ADMIN

Agent ID: TA.PRIVILEGED_ADMIN
Type: Privileged Insider
Skill Level: [TODO: Expert]

Description: [TODO: Malicious administrator with privileged access]

Motivation: - **Primary:** [TODO: e.g., Financial gain, blackmail] - **Secondary:** [TODO: e.g., Revenge, ideology]

Capabilities: - **Technical Expertise:** [TODO: High - Deep system understanding] - **Tools:** [TODO: Administrative tools, root access] - **Knowledge:** [TODO: Complete insider knowledge, access to documentation] - **Access:** [TODO: Privileged access, physical access]

Resources: - **Time:** [TODO: Hours to days] - **Budget:** [TODO: Minimal] - **Team:** [TODO: Individual] - **Infrastructure:** [TODO: Full access to company resources]

Attack Vectors: - [TODO: Direct data manipulation] - [TODO: Disabling security mechanisms] - [TODO: Creating backdoors] - [TODO: Manipulating audit logs] - [TODO: Privilege escalation for other accounts]

Attack Potential: [TODO: Very High - Privileged access enables almost all attacks]

16.3.2.4 TA.NATION_STATE

Agent ID: TA.NATION_STATE
Type: Nation-State Actor
Skill Level: [TODO: Expert]

Description: [TODO: State-sponsored attacker with extensive resources]

[TODO: Add more Threat Agents]

16.3.3 3.3 Attack Potential Assessment

16.3.3.1 3.3.1 CCRA Methodology

Common Criteria Recognition Arrangement (CCRA) Attack Potential:

Factor	Level	Points	Description
Elapsed Time	< 1 day	0	[TODO]
	< 1 week	1	[TODO]
	< 1 month	4	[TODO]
	< 6 months	10	[TODO]
	> 6 months	17	[TODO]
Expertise	Layman	0	[TODO]
	Proficient	3	[TODO]
	Expert	6	[TODO]
Knowledge	Public	0	[TODO]
	Restricted	3	[TODO]
	Sensitive	7	[TODO]
Window of Opportunity	Unnecessary	0	[TODO]
	Easy	1	[TODO]
	Moderate	4	[TODO]
	Difficult	10	[TODO]
Equipment	Standard	0	[TODO]
	Specialized	4	[TODO]
	Bespoke	7	[TODO]

16.3.3.2 3.3.2 Attack Potential Ratings

Attack Potential Ratings:

Agent ID	Elapsed Time	Expertise	Knowledge	Window	Equipment	Total	Rating
[TODO: TA.001]	[TODO: 4]	[TODO: 6]	[TODO: 3]	[TODO: 1]	[TODO: 4]	[TODO: 18]	[TODO: Moderate]
[TODO: TA.002]	[TODO: 1]	[TODO: 3]	[TODO: 7]	[TODO: 0]	[TODO: 0]	[TODO: 11]	[TODO: Enhanced-Basic]

Rating Scale: - **0-9 points:** Basic - **10-13 points:** Enhanced-Basic - **14-19 points:** Moderate - **20-24 points:** High - **25 points:** Beyond High

16.3.4 3.4 Threat Agent Capabilities Matrix

Capabilities Matrix:

Agent	Network Access	Physical Access	Insider Knowledge	Technical Skills	Resources	Persistence
[TODO: TA.001]	[TODO: Yes]	[TODO: No]	[TODO: No]	[TODO: High]	[TODO: High]	[TODO: High]
[TODO: TA.002]	[TODO: Yes]	[TODO: Yes]	[TODO: Yes]	[TODO: Medium]	[TODO: Low]	[TODO: Medium]
[TODO: TA.003]	[TODO: Yes]	[TODO: No]	[TODO: No]	[TODO: Expert]	[TODO: Very High]	[TODO: Very High]

16.4 4. Asset-Agent Relationships

16.4.1 4.1 Asset-Agent Threat Matrix

Which agents threaten which assets:

Asset	TA.001	TA.002	TA.003	TA.004	TA.005
[TODO: A.001]	[TODO: High]	[TODO: Medium]	[TODO: High]	[TODO: Low]	[TODO: Medium]
[TODO: A.002]	[TODO: Medium]	[TODO: High]	[TODO: Medium]	[TODO: Low]	[TODO: Low]

16.4.2 4.2 High-Risk Combinations

High-Risk Combinations:

Asset	Agent	Risk Level	Rationale
[TODO: A.001]	[TODO: TA.003]	[TODO: Critical]	[TODO: High-value data + highly skilled attacker]
[TODO: A.002]	[TODO: TA.002]	[TODO: High]	[TODO: Critical service + insider access]

16.5 5. Summary

16.5.1 5.1 Asset Summary

Asset Summary: - Total number of assets: [TODO: Number] - Critical assets: [TODO: Number] - High-value assets: [TODO: Number] - Medium-value assets: [TODO: Number] - Low-value assets: [TODO: Number]

16.5.2 5.2 Threat Agent Summary

Agent Summary: - Total number of agents: [TODO: Number] - External attackers: [TODO: Number] - Insiders: [TODO: Number] - Privileged insiders: [TODO: Number] - Nation-state actors: [TODO: Number] - Other: [TODO: Number]

16.5.3 5.3 Risk Overview

Risk Overview: - Critical risk combinations: [TODO: Number] - High risk combinations: [TODO: Number] - Medium risk combinations: [TODO: Number] - Low risk combinations: [TODO: Number]

Next Steps: 1. Complete all [TODO] placeholders with TOE-specific assets and agents 2. Conduct complete asset identification 3. Document all relevant threat agents 4. Assess attack potential for all agents 5. Create asset dependency diagrams 6. Verify consistency with Threats (Template 0210) and Security Objectives (Template 0300)

ewpage

Chapter 17

Security Objectives

Document-ID: 0300
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and adapt the content to your specific TOE (Target of Evaluation).

17.1 1. Introduction

This document defines the security objectives for the TOE **{{ meta.toe_name }}** and its operational environment. The security objectives are derived from the security problem definition and describe the intended security properties required to counter identified threats, comply with organizational security policies, and fulfill assumptions.

17.1.1 1.1 Purpose

The security objectives serve as a bridge between: - The security problem definition (threats, OSPs, assumptions) - The security requirements (SFRs and SARs)

They describe **what** should be achieved, not **how** it will be implemented.

17.1.2 1.2 Structure

The security objectives are divided into two categories: - **Security objectives for the TOE (O.xxx)**: Objectives achieved by the TOE itself - **Security objectives for the environment (OE.xxx)**: Objectives that must be fulfilled by the operational environment

17.2 2. Security Objectives for the TOE

17.2.1 2.1 Access Control and Authentication

17.2.1.1 O.ACCESS_CONTROL

Description: The TOE must control access to protected resources based on user identity and permissions.

Rationale: This objective addresses the threats T.UNAUTHORIZED_ACCESS and T.PRIVILEGE_ESCALATI as well as the organizational security policy P.ACCESS_CONTROL.

[**TODO: Adapt the description to your specific TOE**]

17.2.1.2 O.IDENTIFICATION_AUTHENTICATION

Description: The TOE must uniquely identify and authenticate all users before granting access to protected functions.

Rationale: This objective addresses the threat T.MASQUERADE and supports O.ACCESS_CONTROL.

[**TODO: Add additional authentication objectives if required**]

17.2.2 2.2 Audit and Accountability

17.2.2.1 O.AUDIT_GENERATION

Description: The TOE must record security-relevant events, including user actions, security violations, and system events.

Rationale: This objective addresses the threat T.AUDIT_COMPROMISE and the organizational security policy P.ACCOUNTABILITY.

[**TODO: Define specific audit requirements**]

17.2.2.2 O.AUDIT_PROTECTION

Description: The TOE must protect audit records from unauthorized modification and deletion.

Rationale: This objective addresses the threat T.AUDIT_COMPROMISE and ensures the integrity of audit data.

[**TODO: Describe protection mechanisms for audit data**]

17.2.3 2.3 Data Protection and Confidentiality

17.2.3.1 O.DATA_CONFIDENTIALITY

Description: The TOE must protect sensitive user data from unauthorized disclosure.

Rationale: This objective addresses the threats T.DATA_DISCLOSURE and T.EAVESDROPPING as well as the organizational security policy P.CONFIDENTIALITY.

[**TODO: Define which data must be protected**]

17.2.3.2 O.CRYPTOGRAPHIC_OPERATIONS

Description: The TOE must perform cryptographic operations for encryption and integrity protection of data.

Rationale: This objective supports O.DATA_CONFIDENTIALITY and O.DATA_INTEGRITY by providing cryptographic mechanisms.

[**TODO: Specify required cryptographic functions**]

17.2.4 2.4 Data Integrity

17.2.4.1 O.DATA_INTEGRITY

Description: The TOE must protect the integrity of user data and system data against unauthorized modification.

Rationale: This objective addresses the threats T.DATA_MODIFICATION and T.DATA_CORRUPTION as well as the organizational security policy P.INTEGRITY.

[**TODO: Describe integrity protection mechanisms**]

17.2.5 2.5 Security Management

17.2.5.1 O.SECURITY_MANAGEMENT

Description: The TOE must enable authorized administrators to manage security functions and policies.

Rationale: This objective addresses the organizational security policy P.MANAGEMENT and enables configuration and maintenance of the TOE.

[**TODO: Define management functions**]

17.2.5.2 O.SECURE_STATE

Description: The TOE must start in a secure state and transition to a secure state upon errors.

Rationale: This objective addresses the threat T.MALFUNCTION and ensures that the TOE remains secure even during errors.

[**TODO: Describe secure states and error handling**]

17.2.6 2.6 Self-Protection

17.2.6.1 O.TSF_PROTECTION

Description: The TOE must protect its own security functions (TSF) from tampering and bypass.

Rationale: This objective addresses the threats T.TSF_COMPROMISE and T.TSF_BYPASS and ensures the integrity of security functions.

[**TODO: Describe TSF protection mechanisms**]

17.2.7 2.7 Additional TOE Security Objectives

[**TODO: Add additional specific security objectives for your TOE**]

17.2.7.1 O.[CUSTOM_OBJECTIVE_1]

Description: [TODO: Description]

Rationale: [TODO: Justification and reference to threats/OSPs]

17.2.7.2 O.[CUSTOM_OBJECTIVE_2]

Description: [TODO: Description]

Rationale: [TODO: Justification and reference to threats/OSPs]

17.3 3. Security Objectives for the Environment

17.3.1 3.1 Physical Security

17.3.1.1 OE.PHYSICAL_PROTECTION

Description: The operational environment must protect the TOE from physical access by unauthorized persons.

Rationale: This objective fulfills the assumption A.PHYSICAL_SECURITY and addresses the threat T.PHYSICAL_ATTACK.

[**TODO: Define required physical protection measures**]

17.3.2 3.2 Personnel and Trust

17.3.2.1 OE.TRUSTED_ADMIN

Description: The operational environment must ensure that administrators are trustworthy, trained, and competent.

Rationale: This objective fulfills the assumption A.TRUSTED_ADMIN and reduces the risk of insider threats.

[**TODO: Describe requirements for administrators**]

17.3.2.2 OE.USER_TRAINING

Description: The operational environment must ensure that users are trained in the secure use of the TOE.

Rationale: This objective fulfills the assumption A.USER_TRAINING and reduces the risk of user errors.

[**TODO: Define training requirements**]

17.3.3 3.3 Network and Connectivity

17.3.3.1 OE.NETWORK_PROTECTION

Description: The operational environment must protect the TOE from network attacks through firewalls, intrusion detection, and other protection mechanisms.

Rationale: This objective fulfills the assumption A.NETWORK_SECURITY and addresses threats from the network.

[**TODO: Specify required network protection measures**]

17.3.4 3.4 External Systems and Services

17.3.4.1 OE.EXTERNAL_SYSTEMS

Description: The operational environment must ensure that external systems with which the TOE interacts are trustworthy and secure.

Rationale: This objective fulfills the assumption A.EXTERNAL_SYSTEMS and reduces risks from third-party components.

[**TODO: Define requirements for external systems**]

17.3.5 3.5 Time Services

17.3.5.1 OE.TIME_STAMPS

Description: The operational environment must provide reliable timestamps for audit records and security events.

Rationale: This objective fulfills the assumption A.TIME_SOURCE and supports O.AUDIT_GENERATION.

[**TODO: Describe requirements for time sources**]

17.3.6 3.6 Additional Environment Objectives

[**TODO: Add additional specific security objectives for the environment**]

17.3.6.1 OE.[CUSTOM_ENV_OBJECTIVE_1]

Description: [TODO: Description]

Rationale: [TODO: Justification and reference to assumptions]

17.3.6.2 OE.[CUSTOM_ENV_OBJECTIVE_2]

Description: [TODO: Description]

Rationale: [TODO: Justification and reference to assumptions]

17.4 4. Summary of Security Objectives

17.4.1 4.1 TOE Security Objectives (Overview)

Objective ID	Brief Description	Category
O.ACCESS_CONTROL	Access control to resources	Access Control
O.IDENTIFICATION_AUTHENTICATION	User identification and authentication	Access Control
O.AUDIT_GENERATION	Recording of security-relevant events	Audit
O.AUDIT_PROTECTION	Protection of audit records	Audit

Objective ID	Brief Description	Category
O.DATA_CONFIDENTIALITY	Protection of sensitive data from disclosure	Data Protection
O.CRYPTOGRAPHIC_OPERATIONS	Cryptographic operations	Data Protection
O.DATA_INTEGRITY	Protection of data integrity	Integrity
O.SECURITY_MANAGEMENT	Management of security functions	Management
O.SECURE_STATE	Secure state at startup and errors	Self-Protection
O.TSF_PROTECTION	Protection of security functions	Self-Protection
[**TODO: Additional objectives**]		

17.4.2 4.2 Environment Objectives (Overview)

Objective ID	Brief Description	Category
OE.PHYSICAL_PROTECTION	Physical protection of the TOE	Physical Security
OE.TRUSTED_ADMIN	Trustworthy administrators	Personnel
OE.USER_TRAINING	User training	Personnel
OE.NETWORK_PROTECTION	Network protection	Network
OE.EXTERNAL_SYSTEMS	Secure external systems	Integration
OE.TIME_STAMPS	Reliable timestamps	Infrastructure
[**TODO: Additional objectives**]		

17.5 5. Next Steps

After defining the security objectives: 1. Create the rationale (justification) for the security objectives (see Template 0310) 2. Create the Coverage Matrix (see Template 0320) 3. Derive the security requirements (SFRs and SARs) from the objectives

17.6 6. References

- ISO/IEC 15408-1: Security Target Evaluation
- ISO/IEC 15408-2: Security Functional Components
- ISO/IEC 15408-3: Security Assurance Components
- Template 0200-0240: Security Problem Definition
- Template 0310: Security Objectives Rationale
- Template 0320: Security Objectives Coverage Matrix

Document History:

Version	Date	Author	Changes
{{ meta.version }}	{{ meta.date }}	{{ meta.owner }}	Initial version

ewpage

Chapter 18

Security Objectives Rationale

Document-ID: 0310
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and adapt the content to your specific TOE (Target of Evaluation).

18.1 1. Introduction

This document provides the rationale (justification) for the security objectives of the TOE **{{ meta.toe_name }}** and its operational environment. The rationale demonstrates that the defined security objectives are sufficient and appropriate to:

- Counter all identified threats
- Implement all organizational security policies (OSPs)
- Fulfill all assumptions about the operational environment

18.1.1 1.1 Purpose

The rationale serves as proof of: - **Completeness**: All elements of the security problem definition are covered by objectives - **Appropriateness**: Each objective is suitable to address the assigned threats/OSPs/assumptions - **Traceability**: Clear connection between security problems and objectives

18.1.2 1.2 Methodology

For each security objective, the following is documented: 1. Which threats, OSPs, or assumptions it addresses 2. How it counters these security problems 3. Why it is appropriate and sufficient

18.2 2. Rationale for TOE Security Objectives

18.2.1 2.1 O.ACCESS_CONTROL

Addressed Threats: - T.UNAUTHORIZED_ACCESS: Unauthorized access to protected resources - T.PRIVILEGE_ESCALATION: Gaining higher privileges

Addressed OSPs: - P.ACCESS_CONTROL: Access must be controlled based on permissions

Rationale: The objective O.ACCESS_CONTROL counters the threats T.UNAUTHORIZED_ACCESS and T.PRIVILEGE_ESCALATION by ensuring that the TOE controls access to protected resources based on user identity and assigned permissions. Only authenticated users with appropriate permissions can access resources. This implements the organizational security policy P.ACCESS_CONTROL, which mandates role-based access control.

[**TODO: Adapt the rationale to your specific TOE**]

18.2.2 2.2 O.IDENTIFICATION_AUTHENTICATION

Addressed Threats: - T.MASQUERADE: Impersonating a false identity

Rationale: The objective O.IDENTIFICATION_AUTHENTICATION counters the threat T.MASQUERADE by ensuring that all users are uniquely identified and authenticated before access to protected functions is granted. This prevents attackers from impersonating legitimate users. The objective also supports O.ACCESS_CONTROL, as reliable identification is a prerequisite for effective access control.

[**TODO: Add additional details about authentication**]

18.2.3 2.3 O.AUDIT_GENERATION

Addressed Threats: - T.AUDIT_COMPROMISE: Manipulation or deletion of audit data

Addressed OSPs: - P.ACCOUNTABILITY: User actions must be traceable

Rationale: The objective O.AUDIT_GENERATION partially counters the threat T.AUDIT_COMPROMISE by ensuring that security-relevant events are recorded. Recording enables traceability of user actions and security events, which implements the organizational security policy P.ACCOUNTABILITY. In combination with O.AUDIT_PROTECTION, complete protection of audit data is achieved.

[**TODO: Define which events are recorded**]

18.2.4 2.4 O.AUDIT_PROTECTION

Addressed Threats: - T.AUDIT_COMPROMISE: Manipulation or deletion of audit data

Rationale: The objective O.AUDIT_PROTECTION counters the threat T.AUDIT_COMPROMISE by ensuring that audit records are protected from unauthorized modification and deletion. This guarantees the integrity and availability of audit data required for forensic analysis and compliance evidence. The objective complements O.AUDIT_GENERATION and ensures complete audit protection.

[**TODO: Describe protection mechanisms**]

18.2.5 2.5 O.DATA_CONFIDENTIALITY

Addressed Threats: - T.DATA_DISCLOSURE: Unauthorized disclosure of sensitive data - T.EAVESDROPPING: Eavesdropping on data transmissions

Addressed OSPs: - P.CONFIDENTIALITY: Sensitive data must be treated confidentially

Rationale: The objective O.DATA_CONFIDENTIALITY counters the threats T.DATA_DISCLOSURE and T.EAVESDROPPING by ensuring that sensitive user data is protected from unauthorized disclosure. This is achieved through access control, encryption, and secure data transmission. The objective implements the organizational security policy P.CONFIDENTIALITY, which mandates the protection of confidential information.

[**TODO: Specify protected data types**]

18.2.6 2.6 O.CRYPTOGRAPHIC_OPERATIONS

Addressed Threats: - T.DATA_DISCLOSURE: Unauthorized disclosure of sensitive data - T.DATA_MODIFICATION: Unauthorized modification of data

Rationale: The objective O.CRYPTOGRAPHIC_OPERATIONS supports O.DATA_CONFIDENTIALITY and O.DATA_INTEGRITY by providing cryptographic mechanisms for encryption and integrity protection of data. Cryptographic operations protect data both at rest and in transit from disclosure and manipulation.

[**TODO: Define required cryptographic algorithms**]

18.2.7 2.7 O.DATA_INTEGRITY

Addressed Threats: - T.DATA_MODIFICATION: Unauthorized modification of data - T.DATA_CORRUPTION: Corruption of data

Addressed OSPs: - P.INTEGRITY: Data integrity must be ensured

Rationale: The objective O.DATA_INTEGRITY counters the threats T.DATA_MODIFICATION and T.DATA_CORRUPTION by ensuring that user data and system data are protected from unauthorized modification. This is achieved through integrity checks, access control, and cryptographic mechanisms. The objective implements the organizational security policy P.INTEGRITY.

[**TODO: Describe integrity protection mechanisms**]

18.2.8 2.8 O.SECURITY_MANAGEMENT

Addressed OSPs: - P.MANAGEMENT: Security functions must be manageable

Rationale: The objective O.SECURITY_MANAGEMENT implements the organizational security policy P.MANAGEMENT by enabling authorized administrators to manage security functions and policies. This includes configuration of access control policies, audit settings, and other security parameters. Effective management is a prerequisite for maintaining security throughout the TOE lifecycle.

[**TODO: Define management functions**]

18.2.9 2.9 O.SECURE_STATE

Addressed Threats: - T.MALFUNCTION: Malfunction of the TOE

Rationale: The objective O.SECURE_STATE counters the threat T.MALFUNCTION by ensuring that the TOE starts in a secure state and transitions to a secure state upon errors. This prevents malfunctions from leading to security violations. The TOE must maintain its security properties even during unexpected events.

[**TODO: Describe secure states**]

18.2.10 2.10 O.TSF_PROTECTION

Addressed Threats: - T.TSF_COMPROMISE: Tampering with security functions - T.TSF_BYPASS: Bypassing security functions

Rationale: The objective O.TSF_PROTECTION counters the threats T.TSF_COMPROMISE and T.TSF_BYPASS by ensuring that the security functions (TSF) of the TOE are protected from tampering and bypass. This is fundamental to the effectiveness of all other security objectives, as compromised security functions would render all protection mechanisms ineffective.

[**TODO: Describe TSF protection mechanisms**]

18.2.11 2.11 Additional TOE Security Objectives

[**TODO: Add rationale for additional specific security objectives**]

18.2.11.1 O.[CUSTOM_OBJECTIVE_1]

Addressed Threats/OSPs: - [TODO: List threats/OSPs]

Rationale: [TODO: Explain how the objective counters the threats/OSPs]

18.3 3. Rationale for Environment Objectives

18.3.1 3.1 OE.PHYSICAL_PROTECTION

Fulfilled Assumptions: - A.PHYSICAL_SECURITY: The TOE is operated in a physically secured environment

Addressed Threats: - T.PHYSICAL_ATTACK: Physical attack on the TOE

Rationale: The objective OE.PHYSICAL_PROTECTION fulfills the assumption A.PHYSICAL_SECURITY by ensuring that the operational environment protects the TOE from physical access by unauthorized persons. This also counters the threat T.PHYSICAL_ATTACK. Physical protection measures such as access controls, surveillance, and secure facilities prevent attackers from gaining direct access to the hardware.

[**TODO: Define required physical protection measures**]

18.3.2 3.2 OE.TRUSTED_ADMIN

Fulfilled Assumptions: - A.TRUSTED_ADMIN: Administrators are trustworthy and competent

Rationale: The objective OE.TRUSTED_ADMIN fulfills the assumption A.TRUSTED_ADMIN by ensuring that administrators are trustworthy, trained, and competent. This reduces the risk of insider threats and misconfigurations. Trustworthy administrators are essential as they have extensive privileges and could bypass security mechanisms.

[**TODO: Describe requirements for administrators**]

18.3.3 3.3 OE.USER_TRAINING

Fulfilled Assumptions: - A.USER_TRAINING: Users are trained in the secure use of the TOE

Rationale: The objective OE.USER_TRAINING fulfills the assumption A.USER_TRAINING by ensuring that users are trained in the secure use of the TOE. This reduces the risk of user errors, social engineering, and unintentional security violations. Trained users understand security policies and can recognize suspicious activities.

[**TODO: Define training requirements**]

18.3.4 3.4 OE.NETWORK_PROTECTION

Fulfilled Assumptions: - A.NETWORK_SECURITY: The network is protected by firewalls and other mechanisms

Rationale: The objective OE.NETWORK_PROTECTION fulfills the assumption A.NETWORK_SECURITY by ensuring that the operational environment protects the TOE from network attacks. Firewalls, intrusion detection systems, and network segmentation reduce the attack surface and prevent unauthorized network access to the TOE.

[**TODO: Specify required network protection measures**]

18.3.5 3.5 OE.EXTERNAL_SYSTEMS

Fulfilled Assumptions: - A.EXTERNAL_SYSTEMS: External systems are trustworthy and secure

Rationale: The objective OE.EXTERNAL_SYSTEMS fulfills the assumption A.EXTERNAL_SYSTEMS by ensuring that external systems with which the TOE interacts are trustworthy and secure. This reduces risks from compromised third-party components or insecure interfaces. The environment must assess and monitor the security of external systems.

[**TODO: Define requirements for external systems**]

18.3.6 3.6 OE.TIME_STAMPS

Fulfilled Assumptions: - A.TIME_SOURCE: A reliable time source is available

Rationale: The objective OE.TIME_STAMPS fulfills the assumption A.TIME_SOURCE by ensuring that the operational environment provides reliable timestamps for audit records and security events. Accurate timestamps are essential for forensic analysis, event correlation, and compliance evidence. The objective supports O.AUDIT_GENERATION.

[**TODO: Describe requirements for time sources**]

18.3.7 3.7 Additional Environment Objectives

[TODO: Add rationale for additional environment objectives]

18.3.7.1 OE.[CUSTOM_ENV_OBJECTIVE]

Fulfilled Assumptions: - [TODO: List assumptions]

Rationale: [TODO: Explain how the objective fulfills the assumptions]

18.4 4. Completeness Proof

18.4.1 4.1 Threat Coverage

The following table shows that each identified threat is addressed by at least one security objective:

Threat	Addressing Objectives	Status
T.UNAUTHORIZED_ACCESS	O.ACCESS_CONTROL	Covered
T.PRIVILEGE_ESCALATION	O.ACCESS_CONTROL	Covered
T.MASQUERADE	O.IDENTIFICATION_AUTHENTICATION	Covered
T.AUDIT_COMPROMISE	O.AUDIT_GENERATION, O.AUDIT_PROTECTION	Covered
T.DATA_DISCLOSURE	O.DATA_CONFIDENTIALITY, O.CRYPTOGRAPHIC_OPERATIONS	Covered
T.EAVESDROPPING	O.DATA_CONFIDENTIALITY, O.CRYPTOGRAPHIC_OPERATIONS	Covered
T.DATA_MODIFICATION	O.DATA_INTEGRITY, O.CRYPTOGRAPHIC_OPERATIONS	Covered
T.DATA_CORRUPTION	O.DATA_INTEGRITY	Covered
T.MALFUNCTION	O.SECURE_STATE	Covered
T.TSF_COMPROMISE	O.TSF_PROTECTION	Covered
T.TSF_BYPASS	O.TSF_PROTECTION	Covered
T.PHYSICAL_ATTACK	O.PHYSICAL_PROTECTION	Covered
[TODO: Additional threats]		

Result: All threats are covered by security objectives.

18.4.2 4.2 OSP Coverage

The following table shows that each OSP is implemented by at least one security objective:

OSP	Implementing Objectives	Status
P.ACCESS_CONTROL	O.ACCESS_CONTROL	Covered
P.ACCOUNTABILITY	O.AUDIT_GENERATION, O.AUDIT_PROTECTION	Covered
P.CONFIDENTIALITY	O.DATA_CONFIDENTIALITY	Covered
P.INTEGRITY	O.DATA_INTEGRITY	Covered

OSP	Implementing Objectives	Status
P.MANAGEMENT	O.SECURITY_MANAGEMENT	Covered
[**TODO: Additional OSPs**]		

Result: All OSPs are implemented by security objectives.

18.4.3 4.3 Assumption Coverage

The following table shows that each assumption is fulfilled by at least one environment objective:

Assumption	Fulfilling Objectives	Status
A.PHYSICAL_SECURITY	OE.PHYSICAL_PROTECTION	Covered
A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN	Covered
A.USER_TRAINING	OE.USER_TRAINING	Covered
A.NETWORK_SECURITY	OE.NETWORK_PROTECTION	Covered
A.EXTERNAL_SYSTEMS	OE.EXTERNAL_SYSTEMS	Covered
A.TIME_SOURCE	OE.TIME_STAMPS	Covered
[**TODO: Additional assumptions**]		

Result: All assumptions are fulfilled by environment objectives.

18.4.4 4.4 Security Objective Traceability

The following table shows that each security objective can be traced back to at least one threat, OSP, or assumption:

Security Objective	Threats	OSPs	Assumptions	Status
O.ACCESS_CONTROL	T.UNAUTHORIZED_ACCESS, T.PRIVILEGE_ESCALATION	P.ACCESS_CONTROL	-	Justified
O.IDENTIFICATION_AUTHENTICATION	T.MASQUERADE	-	-	Justified
O.AUDIT_GENERATION	T.AUDIT_COMPROMISE	P.ACCOUNTABILITY	-	Justified
O.AUDIT_PROTECTION	T.AUDIT_COMPROMISE	-	-	Justified
O.DATA_CONFIDENTIALITY	T.DATA_DISCLOSURE, T.EAVESDROPPING	P.CONFIDENTIALITY	-	Justified
O.CRYPTOGRAPHIC_OPERATIONS	T.DATA_DISCLOSURE, T.DATA_MODIFICATION	-	-	Justified
O.DATA_INTEGRITY	T.DATA_MODIFICATION, T.DATA_CORRUPTION	P.INTEGRITY	-	Justified
O.SECURITY_MANAGEMENT	-	P.MANAGEMENT	-	Justified
O.SECURE_STATE	T.MALFUNCTION	-	-	Justified
O.TSF_PROTECTION	T.TSF_COMPROMISE, T.TSF_BYPASS	-	-	Justified
OE.PHYSICAL_PROTECTION	T.PHYSICAL_ATTACK	-	A.PHYSICAL_SECURITY	Justified

Security Objective	Threats	OSPs	Assumptions	Status
OE.TRUSTED_ADMIN	-	-	A.TRUSTED_ADMIN	Justified
OE.USER_TRAINING	-	-	A.USER_TRAINING	Justified
OE.NETWORK_PROTECTION	-	-	A.NETWORK_SECURITY	Justified
OE.EXTERNAL_SYSTEMS	-	-	A.EXTERNAL_SYSTEMS	Justified
OE.TIME_STAMPS	-	-	A.TIME_SOURCE	Justified
[TODO: Additional objectives]				

Result: All security objectives are justified.

18.5 5. Summary

The rationale demonstrates that the defined security objectives are:

1. **Complete**: All threats, OSPs, and assumptions are covered
2. **Appropriate**: Each objective is suitable to counter the assigned security problems
3. **Traceable**: Each objective can be traced back to security problems
4. **Consistent**: No contradictions between objectives

The security objectives form a solid foundation for deriving the security requirements (SFRs and SARs) in the next step of the Security Target.

18.6 6. Next Steps

After the rationale for security objectives: 1. Create the Coverage Matrix (see Template 0320) 2. Derive the security requirements (SFRs and SARs) from the objectives (see Template 0400-0450)

18.7 7. References

- ISO/IEC 15408-1: Security Target Evaluation
- Template 0200-0240: Security Problem Definition
- Template 0300: Security Objectives
- Template 0320: Security Objectives Coverage Matrix
- Template 0400-0450: Security Requirements

Document History:

Version	Date	Author	Changes
{{ meta.version }}	{{ meta.date }}	{{ meta.owner }}	Initial version

ewpage

Chapter 19

Security Objectives Coverage Matrix

Document-ID: 0320
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and adapt the content to your specific TOE (Target of Evaluation).

19.1 1. Introduction

This document presents the Coverage Matrix for the security objectives of the TOE **{{ meta.toe_name }}**. The matrix visualizes the relationships between:

- Security objectives and threats
- Security objectives and organizational security policies (OSPs)
- Environment objectives and assumptions

19.1.1 1.1 Purpose

The Coverage Matrix serves as: - **Completeness proof**: All elements of the security problem definition are covered - **Traceability tool**: Quick identification of relationships - **Audit documentation**: Evidence for evaluators and auditors - **Change management**: Identification of impacts during changes

19.1.2 1.2 Legend

Symbol	Meaning
X	Primary mapping - The objective directly addresses the threat/OSP/assumption

Symbol	Meaning
•	Supporting mapping - The objective indirectly supports
-	No mapping

19.2 2. Threats vs. Security Objectives

The following matrix shows which security objectives address which threats:

Threat	O.ACCESS_CONTROL	O.IDENTIFICATION_AUTHENTICATION	O.ACCOUNTABILITY	O.CONFIDENTIALITY	O.INTEGRITY	O.MANAGEMENT	O.PROTECTION	[TODO: Additional objectives]
T.UNAUTHORIZED_ACCESS	X	-	-	-	-	-	-	
T.PRIVILEGE_ESCALATION	X	-	-	-	-	-	-	
T.MASQUERADE	-	X	-	-	-	-	-	
T.AUDIT_COMPROMISE	-	-	X	-	-	-	-	
T.DATA_DISCLOSURE	-	X	X	-	-	-	-	
T.EAVESDROPPING	-	X	X	-	-	-	-	
T.DATA_MODIFICATION	-	-	X	X	-	-	-	
T.DATA_CORRUPTION	-	-	-	X	-	-	-	
T.MALFUNCTION	-	-	-	-	-	X	-	
T.TSF_COMPROMISE	-	-	-	-	-	-	X	
T.TSF_BYPASS	-	-	-	-	-	-	X	
T.PHYSICAL_ATTACK	-	-	-	-	-	-	-	X
[**TODO: Additional threats**]								

Analysis: - All threats are covered by at least one security objective - Multiple coverage shows Defense-in-Depth approach - [**TODO: Add specific analyses for your TOE**]

19.3 3. Organizational Security Policies vs. Security Objectives

The following matrix shows which security objectives implement which OSPs:

OSP	O.ACCESS_CONTROL	O.IDENTIFICATION_AUTHENTICATION	O.ACCOUNTABILITY	O.CONFIDENTIALITY	O.INTEGRITY	O.MANAGEMENT	O.PROTECTION	[TODO: Additional objectives]
P.ACCESS_CONTROL	•	-	-	-	-	-	-	
P.ACCOUNTABILITY	-	X	-	-	-	-	-	
P.CONFIDENTIALITY	-	-	X	•	-	-	-	
P.INTEGRITY	-	-	-	•	X	-	-	
P.MANAGEMENT	-	-	-	-	-	X	-	

OSP	O.ACCESS_CONTROL	O.SECURE_ADMIN	O.AUDIT_LOGGING	O.DATA_INTEGRITY	[TODO: Additional OSPs]
[**TODO: Additional OSPs**]					

Analysis: - All OSPs are implemented by at least one security objective - Clear mapping between policies and technical objectives - [**TODO: Add specific analyses for your TOE**]

19.4 4. Assumptions vs. Environment Objectives

The following matrix shows which environment objectives fulfill which assumptions:

Assumption	OE.PHYSICAL_PROTECTION	OE.TRUSTED_ADMIN	OE.USER_TRAINING	OE.NETWORK_PROTECTION	OE.EXTERNAL_SYSTEMS	[TODO: Additional OEs]
A.PHYSICAL_SECURITY	X	-	-	-	-	
A.TRUSTED_ADMIN	-	X	-	-	-	
A.USER_TRAINING	-	-	X	-	-	
A.NETWORK_SECURITY	-	-	-	X	-	
A.EXTERNAL_SYSTEMS	-	-	-	-	X	
A.TIME_SOURCE	-	-	-	-	-	X
[**TODO: Additional assumptions**]						

Analysis: - All assumptions are fulfilled by at least one environment objective - Clear separation between TOE and environment responsibilities - [**TODO: Add specific analyses for your TOE**]

19.5 5. Reverse Traceability: Security Objectives to Security Problems

The following matrix shows the reverse perspective - which threats/OSPs/assumptions justify each security objective:

19.5.1 5.1 TOE Security Objectives

Security Objective	Addressed Threats	Implemented OSPs	Justification
O.ACCESS_CONTROL	T.UNAUTHORIZED_ACCESS, T.PRIVILEGE_ESCALATION	P.ACCESS_CONTROL	Controls access to resources

Security Objective	Addressed Threats	Implemented OSPs	Justification
O.IDENTIFICATION_AUTHENTICATION	T.UNAUTHORIZED_ACCESS	-	Prevents identity impersonation
O.AUDIT_GENERATION	T.AUDIT_COMPROMISE	P.ACCOUNTABILITY	Records security-relevant events
O.AUDIT_PROTECTION	T.AUDIT_COMPROMISE	-	Protects audit data from tampering
O.DATA_CONFIDENTIALITY	T.UNAUTHORIZED_DISCLOSURE, T.EAVESDROPPING	P.CONFIDENTIALITY	Protects sensitive data from disclosure
O.CRYPTOGRAPHIC_OPERATIONS	T.UNAUTHORIZED_DISCLOSURE, T.DATA_MODIFICATION	-	Provides cryptographic mechanisms
O.DATA_INTEGRITY	T.DATA_MODIFICATION, T.DATA_CORRUPTION	P.INTEGRITY	Protects data integrity
O.SECURITY_MANAGEMENT	-	P.MANAGEMENT	Enables management of security functions
O.SECURE_STATE	T.MALFUNCTION	-	Ensures secure state during errors
O.TSF_PROTECTION	T.TSF_COMPROMISE, T.TSF_BYPASS	-	Protects security functions themselves
[TODO: Additional objectives]			

Result: All TOE security objectives are justified by threats or OSPs

19.5.2 5.2 Environment Objectives

Environment Objective	Fulfilled Assumptions	Addressed Threats	Justification
OE.PHYSICAL_PROTECTION	A.PHYSICAL_SECURITY	T.PHYSICAL_ATTACK	Protects TOE from physical access
OE.TRUSTED_ADMIN	A.TRUSTED_ADMIN	-	Ensures trustworthy administrators
OE.USER_TRAINING	A.USER_TRAINING	-	Trains users in secure usage
OE.NETWORK_PROTECTION	A.NETWORK_SECURITY	-	Protects TOE from network attacks

Environment Objective	Fulfilled Assumptions	Addressed Threats	Justification
OE.EXTERNAL_SYSTEMS	A.EXTERNAL_SYSTEMS	-	Ensures security of external systems
OE.TIME_STAMPS	A.TIME_SOURCE	-	Provides reliable timestamps
[TODO: Additional objectives]			

Result: All environment objectives are justified by assumptions

19.6 6. Completeness Analysis

19.6.1 6.1 Threat Coverage

Total number of threats: 12 **[TODO: Update count]**
Covered threats: 12 **[TODO: Update count]**
Uncovered threats: 0 **[TODO: Update count]**

Status: Fully covered

[TODO: List uncovered threats if any]

19.6.2 6.2 OSP Coverage

Total number of OSPs: 5 **[TODO: Update count]**
Implemented OSPs: 5 **[TODO: Update count]**
Unimplemented OSPs: 0 **[TODO: Update count]**

Status: Fully implemented

[TODO: List unimplemented OSPs if any]

19.6.3 6.3 Assumption Coverage

Total number of assumptions: 6 **[TODO: Update count]**
Fulfilled assumptions: 6 **[TODO: Update count]**
Unfulfilled assumptions: 0 **[TODO: Update count]**

Status: Fully fulfilled

[TODO: List unfulfilled assumptions if any]

19.6.4 6.4 Objective Justification

Total number of security objectives: 16 **[TODO: Update count]**
Justified objectives: 16 **[TODO: Update count]**
Unjustified objectives: 0 **[TODO: Update count]**

Status: All objectives justified

[TODO: List unjustified objectives if any]

19.7 7. Gap Analysis

19.7.1 7.1 Identified Gaps

[**TODO: Document identified gaps in coverage**]

Example: - **Gap 1:** Threat T.XXX is not covered by security objectives - **Impact:** [Description] - **Recommended Action:** Add security objective O.XXX

- **Gap 2:** Security objective O.YYY is not justified by threats/OSPs
  - **Impact:** [Description]
  - **Recommended Action:** Remove objective or identify justifying threat

Current Status: No gaps identified

19.7.2 7.2 Redundancies and Overlaps

[**TODO: Document redundancies between security objectives**]

Example: - **Overlap 1:** O.XXX and O.YYY both address T.ZZZ - **Analysis:** [Is this intentional? Defense-in-Depth?] - **Recommendation:** [Consolidate or maintain]

Current Status: Overlaps are intentional (Defense-in-Depth)

19.8 8. Change Management

19.8.1 8.1 Impact Analysis for Changes

When changes are made to the security problem definition or security objectives, the Coverage Matrix must be updated:

When adding a new threat: 1. Add row in Matrix 2 2. Identify addressing security objectives 3. If no objectives exist: Create new security objective 4. Update completeness analysis

When adding a new security objective: 1. Add column in Matrix 2 and 3 2. Identify addressed threats/OSPs 3. If no threats/OSPs: Review necessity of objective 4. Update reverse traceability

When removing a threat: 1. Remove row from Matrix 2 2. Check if assigned security objectives are still justified 3. Update completeness analysis

When removing a security objective: 1. Remove column from matrices 2. Check if all threats/OSPs are still covered 3. If not: Identify alternative objective or create new objective

19.8.2 8.2 Change History

Date	Change	Impact	Editor
{{ meta.date }} [**TODO**]	Initial version	-	{{ meta.owner }}

19.9 9. Summary

The Coverage Matrix demonstrates:

1. **Completeness:**
   - All threats are covered by security objectives
   - All OSPs are implemented by security objectives
   - All assumptions are fulfilled by environment objectives
2. **Traceability:**
   - All security objectives are justified by threats/OSPs
   - All environment objectives are justified by assumptions
3. **Consistency:**
   - No gaps in coverage
   - No unjustified objectives

The security objectives form a complete and consistent foundation for deriving the security requirements (SFRs and SARs).

19.10 10. Next Steps

After the Coverage Matrix: 1. Derive security requirements (SFRs) from TOE security objectives (see Template 0400-0450) 2. Define security requirements for the environment based on environment objectives 3. Create rationale for security requirements

19.11 11. References

- ISO/IEC 15408-1: Security Target Evaluation
- ISO/IEC 15408-2: Security Functional Components
- Template 0200-0240: Security Problem Definition
- Template 0300: Security Objectives
- Template 0310: Security Objectives Rationale
- Template 0400-0450: Security Requirements

Document History:

Version	Date	Author	Changes
{{ meta.version }}	{{ meta.date }}	{{ meta.owner }}	Initial version

ewpage

Chapter 20

Security Objectives Summary

Document-ID: 0330
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and adapt the content to your specific TOE (Target of Evaluation).

20.1 1. Introduction

This document provides a compact summary of all security objectives for the TOE **{{ meta.toe_name }}** and its operational environment. The security objectives describe the intended security properties required to counter identified threats, comply with organizational security policies, and fulfill assumptions.

20.1.1 1.1 Purpose

This summary serves as: - **Quick reference** for all security objectives - **Executive summary** for management decisions - **Communication tool** for stakeholders - **Audit documentation** for evaluators

20.1.2 1.2 Document Structure

- Section 2: Overview of TOE security objectives
- Section 3: Overview of environment objectives
- Section 4: Categorization by security domains
- Section 5: Coverage statistics
- Section 6: Graphical representations

20.2 2. TOE Security Objectives (Overview)

The following security objectives are fulfilled by the TOE itself:

ID	Objective	Brief Description	Category	Priority
O.ACCESS_CONTROL	Access Control	Controls access to protected resources based on user identity and permissions	Access Control	High
O.IDENTIFICATION_AUTHENTICATION	Identification & Authentication	Identifies and authenticates all users before granting access to protected functions	Access Control	High
O.AUDIT_GENERATION	Audit Generation	Records security-relevant events	Audit & Accountability	High
O.AUDIT_PROTECTION	Audit Protection	Protects audit records from unauthorized modification and deletion	Audit & Accountability	High
O.DATA_CONFIDENTIALITY	Data Confidentiality	Protects sensitive user data from unauthorized disclosure	Data Protection	High
O.CRYPTOGRAPHIC_OPERATIONS	Cryptographic Operations	Performs cryptographic operations for encryption and integrity protection	Data Protection	Medium
O.DATA_INTEGRITY	Data Integrity	Protects data integrity against unauthorized modification	Integrity	High
O.SECURITY_MANAGEMENT	Security Management	Enables authorized administrators to manage security functions	Management	Medium
O.SECURE_STATE	Secure State	Starts in secure state and transitions to secure state upon errors	Self-Protection	High
O.TSF_PROTECTION	TSF Protection	Protects own security functions from tampering and bypass	Self-Protection	High

[**TODO**]

Total TOE Security Objectives: 10 [**TODO: Update count**]

20.2.1 2.1 Categorization of TOE Security Objectives

Access Control (2 objectives): - O.ACCESS_CONTROL - O.IDENTIFICATION_AUTHENTICATION

Audit & Accountability (2 objectives): - O.AUDIT_GENERATION - O.AUDIT_PROTECTION

Data Protection (2 objectives): - O.DATA_CONFIDENTIALITY - O.CRYPTOGRAPHIC_OPERATIONS

Integrity (1 objective): - O.DATA_INTEGRITY

Management (1 objective): - O.SECURITY_MANAGEMENT

Self-Protection (2 objectives): - O.SECURE_STATE - O.TSF_PROTECTION

[**TODO: Add additional categories**]

20.3 3. Environment Objectives (Overview)

The following security objectives must be fulfilled by the operational environment:

ID	Objective	Brief Description	Category	Responsible
OE.PHYSICAL_PROTECTION	Physical Protection	Protects TOE from physical access by unauthorized persons	Physical Security	Operator
OE.TRUSTED_ADMIN	Trustworthy Administrators	Ensures that administrators are trustworthy, trained, and competent	Personnel	Organization
OE.USER_TRAINING	User Training	Ensures that users are trained in secure use of the TOE	Personnel	Organization
OE.NETWORK_PROTECTION	Network Protection	Protects TOE from network attacks through firewalls and other mechanisms	Network	IT Department
OE.EXTERNAL_SYSTEMS	Secure External Systems	Ensures that external systems are trustworthy and secure	Integration	IT Department
OE.TIME_STAMPS	Reliable Timestamps	Provides reliable timestamps for audit records	Infrastructure	IT Department

[**TODO**]

Total Environment Objectives: 6 [**TODO: Update count**]

20.3.1 3.1 Categorization of Environment Objectives

Physical Security (1 objective): - OE.PHYSICAL_PROTECTION

Personnel (2 objectives): - OE.TRUSTED_ADMIN - OE.USER_TRAINING

Network (1 objective): - OE.NETWORK_PROTECTION

Integration (1 objective): - OE.EXTERNAL_SYSTEMS

Infrastructure (1 objective): - OE.TIME_STAMPS

[**TODO: Add additional categories**]

20.4 4. Security Objectives by Security Domains

20.4.1 4.1 Access Control and Authentication

TOE Objectives: - O.ACCESS_CONTROL: Access control to resources - O.IDENTIFICATION_AUTHENTICA
User identification and authentication

Environment Objectives: - OE.TRUSTED_ADMIN: Trustworthy administrators

Summary: The TOE implements technical access control and authentication mechanisms, while the environment provides trustworthy administrators.

20.4.2 4.2 Audit and Accountability

TOE Objectives: - O.AUDIT_GENERATION: Recording of security-relevant events - O.AUDIT_PROTECTION: Protection of audit records

Environment Objectives: - OE.TIME_STAMPS: Reliable timestamps

Summary: The TOE records events and protects audit data, while the environment provides reliable timestamps.

20.4.3 4.3 Data Protection and Confidentiality

TOE Objectives: - O.DATA_CONFIDENTIALITY: Protection of sensitive data from disclosure - O.CRYPTOGRAPHIC_OPERATIONS: Cryptographic operations

Environment Objectives: - OE.NETWORK_PROTECTION: Network protection

Summary: The TOE protects data through access control and encryption, while the environment provides network protection.

20.4.4 4.4 Data Integrity

TOE Objectives: - O.DATA_INTEGRITY: Protection of data integrity - O.CRYPTOGRAPHIC_OPERATION Cryptographic integrity protection

Environment Objectives: - No direct environment objectives

Summary: The TOE is primarily responsible for integrity protection.

20.4.5 4.5 Security Management

TOE Objectives: - O.SECURITY_MANAGEMENT: Management of security functions

Environment Objectives: - OE.TRUSTED_ADMIN: Trustworthy administrators - OE.USER_TRAINING: User training

Summary: The TOE provides management functions, while the environment provides trained personnel.

20.4.6 4.6 Self-Protection and Availability

TOE Objectives: - O.SECURE_STATE: Secure state at startup and errors - O.TSF_PROTECTION: Protection of security functions

Environment Objectives: - OE.PHYSICAL_PROTECTION: Physical protection - OE.EXTERNAL_SYSTEM Secure external systems

Summary: The TOE protects itself, while the environment provides physical protection and secure integration.

[**TODO: Add additional security domains**]

20.5 5. Coverage Statistics

20.5.1 5.1 Threat Coverage

Category	Count	Covered by TOE Objectives	Covered by Environment Objectives
Access Control	3	3	0
Data Disclosure	2	2	0
Data Manipulation	2	2	0
Audit Compromise	1	1	0
System Failure	1	1	0
TSF Compromise	2	2	0
Physical Attacks	1	0	1
Total	**12**	**11**	**1**

[TODO: Update statistics based on your threats]

20.5.2 5.2 OSP Coverage

OSP	Implementing TOE Objectives	Status
P.ACCESS_CONTROL	O.ACCESS_CONTROL	Implemented
P.ACCOUNTABILITY	O.AUDIT_GENERATION, O.AUDIT_PROTECTION	Implemented
P.CONFIDENTIALITY	O.DATA_CONFIDENTIALITY	Implemented
P.INTEGRITY	O.DATA_INTEGRITY	Implemented
P.MANAGEMENT	O.SECURITY_MANAGEMENT	Implemented
[**TODO**]		

Total OSPs: 5 [**TODO: Update count**]
Implemented OSPs: 5 (100%)

20.5.3 5.3 Assumption Coverage

Assumption	Fulfilling Environment Objective	Status
A.PHYSICAL_SECURITY	OE.PHYSICAL_PROTECTION	Fulfilled
A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN	Fulfilled
A.USER_TRAINING	OE.USER_TRAINING	Fulfilled
A.NETWORK_SECURITY	OE.NETWORK_PROTECTION	Fulfilled
A.EXTERNAL_SYSTEMS	OE.EXTERNAL_SYSTEMS	Fulfilled

Assumption	Fulfilling Environment Objective	Status
A.TIME_SOURCE [**TODO**]	OE.TIME_STAMPS	Fulfilled

Total Assumptions: 6 [**TODO: Update count**]
Fulfilled Assumptions: 6 (100%)

20.5.4 5.4 Completeness Assessment

Criterion	Status	Percentage
All threats covered	Yes	100%
All OSPs implemented	Yes	100%
All assumptions fulfilled	Yes	100%
All objectives justified	Yes	100%

Overall Assessment: Complete and consistent

20.6 6. Graphical Representations

20.6.1 6.1 Distribution of TOE Security Objectives by Category

```
Access Control:                 (20%)
Audit & Accountability:         (20%)
Data Protection:                (20%)
Integrity:                    (10%)
Management:                   (10%)
Self-Protection:                (20%)
```

[**TODO: Create diagram with actual values**]

20.6.2 6.2 Distribution of Environment Objectives by Responsibility

```
Operator (Physical):              (17%)
Organization (Personnel):                 (33%)
IT Department (Technical):                          (50%)
```

[**TODO: Create diagram with actual values**]

20.6.3 6.3 Relationship Diagram (simplified)

```
Threats (12)        TOE Objectives (10)        SFRs
                                                        (next step)
OSPs (5)            TOE Objectives (10)

Assumptions (6)      Environment Objectives (6)    Environment
                                                      Requirements
```

[**TODO: Create detailed diagram**]

20.7 7. Priorities and Dependencies

20.7.1 7.1 High-Priority Security Objectives

The following security objectives have highest priority and must be implemented first:

1. **O.TSF_PROTECTION** - Fundamental for all other objectives
2. **O.ACCESS_CONTROL** - Basis for access control
3. **O.IDENTIFICATION_AUTHENTICATION** - Prerequisite for access control
4. **O.DATA_CONFIDENTIALITY** - Protection of sensitive data
5. **O.DATA_INTEGRITY** - Protection of data integrity
6. **O.AUDIT_GENERATION** - Accountability
7. **O.SECURE_STATE** - Secure operation

[**TODO: Adapt priorities to your TOE**]

20.7.2 7.2 Dependencies Between Security Objectives

Objective	Depends On	Justification
O.ACCESS_CONTROL	O.IDENTIFICATION_AUTHENTICATION	Access control requires authentication
O.AUDIT_GENERATION	OE.TIME_STAMPS	Audit records need timestamps
O.DATA_CONFIDENTIALITY	O.ACCESS_CONTROL	Confidentiality requires access control
O.DATA_INTEGRITY	O.ACCESS_CONTROL	Integrity requires access control
O.SECURITY_MANAGEMENT	OE.TRUSTED_ADMIN	Management requires trustworthy admins

[**TODO**]

20.8 8. Summary and Assessment

20.8.1 8.1 Strengths of Security Objectives

1. **Complete Coverage:** All threats, OSPs, and assumptions are addressed
2. **Clear Separation:** TOE and environment responsibilities are clearly defined
3. **Defense-in-Depth:** Multiple protection layers through overlapping objectives
4. **Traceability:** All objectives are justified by security problems
5. **Balance:** Good balance between different security domains

[**TODO: Add specific strengths for your TOE**]

20.8.2 8.2 Potential Challenges

1. **Complexity:** Many security objectives require careful implementation
2. **Dependencies:** Some objectives depend on each other
3. **Environment Requirements:** Success depends on correct environment configuration

[**TODO: Identify specific challenges for your TOE**]

20.8.3 8.3 Recommendations

1. Prioritize implementation of high-priority objectives

2. Consider dependencies in implementation planning
3. Ensure environment requirements are achievable
4. Document implementation decisions for evaluators

[TODO: Add specific recommendations]

20.9 9. Next Steps

After the summary of security objectives:

1. **Derive Security Requirements** (Template 0400-0450)
   - Derive Security Functional Requirements (SFRs) from TOE objectives
   - Define Security Assurance Requirements (SARs)
   - Select Evaluation Assurance Level (EAL)
2. **Create Rationale for Requirements**
   - Show how SFRs fulfill security objectives
   - Document SFR dependencies
3. **Develop TOE Summary Specification**
   - Describe how the TOE implements the SFRs

20.10 10. References

- ISO/IEC 15408-1: Security Target Evaluation
- ISO/IEC 15408-2: Security Functional Components
- ISO/IEC 15408-3: Security Assurance Components
- Template 0200-0240: Security Problem Definition
- Template 0300: Security Objectives
- Template 0310: Security Objectives Rationale
- Template 0320: Security Objectives Coverage Matrix
- Template 0400-0450: Security Requirements

Document History:

Version	Date	Author	Changes
{{ meta.version }}	{{ meta.date }}	{{ meta.owner }}	Initial version

ewpage

Chapter 21

Security Requirements

Document-ID: 0400
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and adapt the content to your specific Target of Evaluation (TOE).

21.1 1. Introduction

This chapter specifies the security requirements for the TOE according to ISO/IEC 15408 (Common Criteria). The security requirements are divided into:

- **Security Functional Requirements (SFRs)**: Functional security requirements that the TOE must fulfill
- **Security Assurance Requirements (SARs)**: Assurance requirements for the evaluation of the TOE

All security requirements are derived from the security objectives defined in Chapter 0300 and address the threats, organizational security policies, and assumptions identified in Chapter 0200.

21.2 2. Security Functional Requirements (SFRs)

21.2.1 2.1 Overview of SFRs

The following Security Functional Requirements from ISO/IEC 15408-2 have been selected for the TOE:

SFR-ID	Class	Family	Component	Description
[TODO]	[TODO: e.g., FAU]	[TODO: e.g., FAU_GEN]	[TODO: e.g., FAU_GEN.1]	[TODO: Brief description]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

21.2.2 2.2 Security Audit (FAU)

21.2.2.1 FAU_GEN.1 Audit data generation

Hierarchical to: None
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: - [assignment: list of auditable events] - [TODO: Specify concrete events]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: - Date and time of the event - Type of event - Subject identity - Outcome (success or failure) of the event - [assignment: other audit relevant information]

21.2.3 2.3 Cryptographic Support (FCS)

21.2.3.1 FCS_COP.1 Cryptographic operation

Hierarchical to: None
Dependencies: - FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation

FCS_COP.1.1 The TSF shall perform [assignment: cryptographic operation] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: key sizes] that meet the following: [selection: standards, rules, guidelines].

[TODO: Specify concrete cryptographic operations, algorithms, and key sizes]

21.2.4 2.4 User Data Protection (FDP)

21.2.4.1 FDP_ACC.1 Subset access control

Hierarchical to: None
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: access control policy] on [assignment: subjects, objects, and operations].

[TODO: Define access control policy, subjects, objects, and operations]

21.2.5 2.5 Identification and Authentication (FIA)

21.2.5.1 FIA_UID.1 Timing of identification

Hierarchical to: None
Dependencies: None

FIA_UID.1.1 The TSF shall allow [selection: no other actions, [assignment: list of TSF-mediated actions]] on behalf of the user to be performed before the user is identified.

[TODO: Specify exceptions if any]

21.2.6 2.6 Security Management (FMT)

21.2.6.1 FMT_SMF.1 Specification of Management Functions

Hierarchical to: None
Dependencies: None

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: - [assignment: list of security management functions]

[TODO: List all security management functions]

21.2.7 2.7 Protection of the TSF (FPT)

21.2.7.1 FPT_STM.1 Reliable time stamps

Hierarchical to: None
Dependencies: None

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

21.2.8 2.8 TOE Access (FTA)

21.2.9 2.9 Trusted Path/Channels (FTP)

21.2.10 2.10 Additional SFR Classes

21.3 3. Security Assurance Requirements (SARs)

21.3.1 3.1 Overview of SARs

The Security Assurance Requirements define the assurance requirements for the evaluation of the TOE. The SARs are determined by the selection of the Evaluation Assurance Level (EAL).

Selected EAL: [TODO: e.g., EAL4]

21.3.2 3.2 Assurance Class: Security Target Evaluation (ASE)

The following ASE components are required for all EALs:

- **ASE_CCL.1** Conformance claims
- **ASE_ECD.1** Extended components definition
- **ASE_INT.1** ST introduction
- **ASE_OBJ.2** Security objectives
- **ASE_REQ.2** Derived security requirements
- **ASE_SPD.1** Security problem definition
- **ASE_TSS.1** TOE summary specification

[TODO: Adapt to selected EAL]

21.3.3 3.3 Assurance Class: Development (ADV)

For EAL [TODO: X], the following ADV components are required:

- **ADV_ARC.1** Security architecture description
- **ADV_FSP.4** Complete functional specification
- **ADV_IMP.1** Implementation representation of the TSF
- **ADV_TDS.3** Basic modular design

[TODO: Adapt to selected EAL]

21.3.4 3.4 Assurance Class: Guidance Documents (AGD)

- **AGD_OPE.1** Operational user guidance
- **AGD_PRE.1** Preparative procedures

21.3.5 3.5 Assurance Class: Life-cycle Support (ALC)

For EAL [TODO: X], the following ALC components are required:

- **ALC_CMC.4** Production support, acceptance procedures and automation
- **ALC_CMS.4** Problem tracking CM coverage
- **ALC_DEL.1** Delivery procedures
- **ALC_DVS.1** Identification of security measures
- **ALC_LCD.1** Developer defined life-cycle model
- **ALC_TAT.1** Well-defined development tools

[TODO: Adapt to selected EAL]

21.3.6 3.6 Assurance Class: Tests (ATE)

- **ATE_COV.2** Analysis of coverage
- **ATE_DPT.1** Testing: high-level design
- **ATE_FUN.1** Functional testing
- **ATE_IND.2** Independent testing - sample

[TODO: Adapt to selected EAL]

21.3.7 3.7 Assurance Class: Vulnerability Assessment (AVA)

- **AVA_VAN.3** Focused vulnerability analysis

[TODO: Adapt to selected EAL]

21.4 4. Security Requirements Rationale

The rationale for the selection of security requirements is detailed in document 0420.

Summary: - All SFRs are derived from the security objectives for the TOE - All SFR dependencies are satisfied (see document 0430) - The selected SARs correspond to Evaluation Assurance Level [TODO: X] - The security requirements are complete, consistent, and internally non-contradictory

21.5 5. Operations on SFRs

According to ISO/IEC 15408-2, the following operations can be performed on SFRs:

- **Assignment**: Specification of parameters (marked with [assignment: …])
- **Selection**: Selection from predefined options (marked with [selection: …])
- **Refinement**: Refinement of the requirement (displayed in italics)
- **Iteration**: Multiple use of a component (indicated by suffix, e.g., FDP_ACC.1/1, FDP_ACC.1/2)

All operations performed are documented in the SFR specifications above.

21.6 6. References

- ISO/IEC 15408-2:2022 - Security functional requirements
- ISO/IEC 15408-3:2022 - Security assurance requirements
- [TODO: Other relevant standards and specifications]

21.7 7. Appendices

21.7.1 7.1 SFR Overview Table

A complete overview of all SFRs with dependencies can be found in document 0430.

21.7.2 7.2 SAR Overview Table

A complete overview of all SARs according to the selected EAL can be found in document 0410.

Next Steps: 1. Complete all [TODO] placeholders 2. Specify all assignments and selections in the SFRs 3. Verify completeness of SFR dependencies (see document 0430) 4. Ensure all SFRs are derived from security objectives 5. Document the rationale in document 0420

ewpage

Chapter 22

Evaluation Assurance Level (EAL)

Document-ID: 0410
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and adapt the content to your specific Target of Evaluation (TOE).

22.1 1. Introduction

This document describes the selection and justification of the Evaluation Assurance Level (EAL) for the TOE. The EAL defines the depth and rigor of the security evaluation according to ISO/IEC 15408-3.

22.2 2. EAL Overview

Common Criteria defines seven predefined Evaluation Assurance Levels:

EAL	Designation	Description	Typical Application
EAL1	Functionally tested	Basic functional testing	Commercial off-the-shelf products
EAL2	Structurally tested	Structural testing with developer documentation	Commercial products with security functions
EAL3	Methodically tested and checked	Methodical testing and checking	Security products with moderate requirements
EAL4	Methodically designed, tested, and reviewed	Methodical design, testing, and review	Security products for commercial environments
EAL5	Semiformally designed and tested	Semiformal design and testing	High-security products

EAL	Designation	Description	Typical Application
EAL6	Semiformally verified design and tested	Semiformal verification and testing	High-security environments with high risk
EAL7	Formally verified design and tested	Formal verification and testing	Extremely high security requirements

22.3 3. Selected EAL

Selected Evaluation Assurance Level: [TODO: e.g., EAL4]

22.3.1 3.1 Justification for EAL Selection

[TODO: Justify the EAL selection based on:] - Threat landscape and risk assessment - Protection needs of assets to be protected - Operational environment of the TOE - Cost-benefit ratio - Market requirements and regulatory mandates - Development resources and timeline

Example:

```
EAL4 was selected as it provides a balanced ratio between security assurance and
development effort. The TOE will be deployed in commercial environments with moderate to
high security requirements. EAL4 requires methodical design, testing, and review, which
corresponds to the security requirements of the target environment without requiring the
formal verification requirements of higher EALs.
```

22.3.2 3.2 Alternatives and Trade-offs

[TODO: Discuss alternative EALs and why they were not selected]

Lower EALs (e.g., EAL3): - [TODO: Why not sufficient?]

Higher EALs (e.g., EAL5+): - [TODO: Why not required or not practical?]

22.4 4. Security Assurance Requirements (SARs) for Selected EAL

22.4.1 4.1 Mandatory SARs for EAL [TODO: X]

The following Security Assurance Requirements are mandatory for EAL [TODO: X]:

22.4.1.1 4.1.1 Security Target Evaluation (ASE)

- **ASE_CCL.1** Conformance claims
- **ASE_ECD.1** Extended components definition
- **ASE_INT.1** ST introduction
- **ASE_OBJ.2** Security objectives
- **ASE_REQ.2** Derived security requirements
- **ASE_SPD.1** Security problem definition
- **ASE_TSS.1** TOE summary specification

22.4.1.2 4.1.2 Development (ADV)

[TODO: Add ADV components for selected EAL]

For EAL4: - **ADV_ARC.1** Security architecture description - **ADV_FSP.4** Complete functional specification - **ADV_IMP.1** Implementation representation of the TSF - **ADV_TDS.3** Basic modular design

22.4.1.3 4.1.3 Guidance Documents (AGD)

- **AGD_OPE.1** Operational user guidance
- **AGD_PRE.1** Preparative procedures

22.4.1.4 4.1.4 Life-cycle Support (ALC)

[TODO: Add ALC components for selected EAL]

For EAL4: - **ALC_CMC.4** Production support, acceptance procedures and automation - **ALC_CMS.4** Problem tracking CM coverage - **ALC_DEL.1** Delivery procedures - **ALC_DVS.1** Identification of security measures - **ALC_LCD.1** Developer defined life-cycle model - **ALC_TAT.1** Well-defined development tools

22.4.1.5 4.1.5 Tests (ATE)

[TODO: Add ATE components for selected EAL]

For EAL4: - **ATE_COV.2** Analysis of coverage - **ATE_DPT.1** Testing: high-level design - **ATE_FUN.1** Functional testing - **ATE_IND.2** Independent testing - sample

22.4.1.6 4.1.6 Vulnerability Assessment (AVA)

[TODO: Add AVA components for selected EAL]

For EAL4: - **AVA_VAN.3** Focused vulnerability analysis

22.4.2 4.2 Augmentation (Additional SARs)

[TODO: If additional SARs beyond the selected EAL are used, list and justify them here]

Example:

```
In addition to the EAL4 requirements, the following SARs are added:
- ALC_FLR.2 Flaw reporting procedures (from EAL5)
  Justification: Enhanced vulnerability management for production environments
```

22.5 5. Development and Evaluation Effort

22.5.1 5.1 Development Effort

[TODO: Estimate the additional development effort for the selected EAL]

Documentation Effort: - [TODO: Required documents and estimated effort]

Process Requirements: - [TODO: Required development processes and tools]

Testing Effort: - [TODO: Required tests and test coverage]

22.5.2 5.2 Evaluation Effort

[TODO: Estimate duration and costs of evaluation]

Estimated Evaluation Duration: [TODO: e.g., 6-12 months]
Estimated Evaluation Costs: [TODO: Cost range]
Evaluation Laboratory: [TODO: Planned or selected laboratory]

22.6 6. Compliance and Certification

22.6.1 6.1 Certification Scheme

[TODO: Specify the certification scheme]

Examples: - Common Criteria Recognition Arrangement (CCRA) - National scheme (e.g., BSI Germany, ANSSI France) - [TODO: Specific scheme]

22.6.2 6.2 Mutual Recognition

[TODO: Describe Mutual Recognition Agreements if relevant]

The selected EAL and certification scheme enables recognition in the following countries: - [TODO: List of countries with Mutual Recognition]

22.7 7. Timeline and Milestones

[TODO: Create a rough timeline for the evaluation]

Milestone	Planned Date	Status
ST Completion	[TODO]	[TODO]
Evaluation Start	[TODO]	[TODO]
ADV Phase Completed	[TODO]	[TODO]
ATE Phase Completed	[TODO]	[TODO]
AVA Phase Completed	[TODO]	[TODO]
Certification	[TODO]	[TODO]

22.8 8. Risks and Mitigation

[TODO: Identify risks for the evaluation]

Risk	Probability	Impact	Mitigation
[TODO: e.g., Delays in documentation]	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]

22.9 9. References

- ISO/IEC 15408-3:2022 - Security assurance requirements
- Common Criteria for Information Technology Security Evaluation - Evaluation Assurance Levels
- [TODO: National certification guidelines]
- [TODO: Other relevant documents]

Next Steps: 1. Complete all [TODO] placeholders 2. Validate EAL selection with stakeholders 3. Confirm availability of resources for evaluation 4. Contact potential evaluation laboratories 5. Create detailed project plan for evaluation

ewpage

Chapter 23

Requirements Rationale

Document-ID: 0420
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and adapt the content to your specific Target of Evaluation (TOE).

23.1 1. Introduction

This document justifies the selection of security requirements (Security Functional Requirements and Security Assurance Requirements) for the TOE. The rationale demonstrates that:

1. All SFRs are necessary and sufficient to meet the security objectives for the TOE
2. All SFR dependencies are satisfied
3. The selected SARs correspond to the Evaluation Assurance Level
4. The security requirements are internally consistent and non-contradictory

23.2 2. Derivation of SFRs from Security Objectives

23.2.1 2.1 Mapping: Security Objectives → SFRs

The following table shows the mapping between security objectives for the TOE (from document 0300) and Security Functional Requirements (from document 0400):

Security Objective	Assigned SFRs	Rationale
[TODO: O.AUDIT]	FAU_GEN.1, FAU_SAR.1, FPT_STM.1	[TODO: Rationale for assignment]
[TODO: O.CRYPTO]	FCS_COP.1, FCS_CKM.1	[TODO: Rationale for assignment]

Security Objective	Assigned SFRs	Rationale
[TODO: O.ACCESS]	FDP_ACC.1, FDP_ACF.1, FIA_UID.1, FIA_UAU.1	[TODO: Rationale for assignment]
[TODO]	[TODO]	[TODO]

23.2.2 2.2 Detailed Rationale per Security Objective

23.2.2.1 2.2.1 [TODO: Security Objective 1]

Security Objective: [TODO: Description from document 0300]

Assigned SFRs: - [TODO: SFR-ID]: [TODO: Rationale for how this SFR fulfills the objective] - [TODO: SFR-ID]: [TODO: Rationale]

Completeness: [TODO: Explanation why these SFRs are sufficient]

23.2.2.2 2.2.2 [TODO: Security Objective 2]

Security Objective: [TODO: Description from document 0300]

Assigned SFRs: - [TODO: SFR-ID]: [TODO: Rationale]

Completeness: [TODO: Explanation]

23.2.3 2.3 Completeness Analysis

Coverage of Security Objectives: - Number of security objectives for TOE: [TODO: X] - Number of objectives addressed by SFRs: [TODO: X] - Coverage rate: [TODO: 100%]

Objectives Not Addressed by SFRs: [TODO: If any, list and justify why no SFRs are required]

23.3 3. Necessity of SFRs

23.3.1 3.1 Rationale per SFR

Each selected SFR must be necessary to fulfill at least one security objective.

23.3.1.1 3.1.1 [TODO: SFR-ID 1]

SFR: [TODO: Name and description]

Addressed Security Objectives: - [TODO: Objective-ID]: [TODO: How the SFR contributes to the objective]

Necessity: [TODO: Why this SFR is indispensable]

Alternatives: [TODO: Why alternative SFRs were not selected]

23.3.1.2 3.1.2 [TODO: SFR-ID 2]

SFR: [TODO: Name and description]

Addressed Security Objectives: - [TODO: Objective-ID]: [TODO: Rationale]

Necessity: [TODO: Rationale]

23.3.2 3.2 Superfluous SFRs

[TODO: Confirm that no superfluous SFRs are included]

All selected SFRs are necessary and contribute to fulfilling at least one security objective. No superfluous SFRs have been identified.

23.4 4. SFR Dependencies

23.4.1 4.1 Overview of Dependencies

The following table shows all SFR dependencies and their satisfaction:

SFR	Dependency	Satisfied by	Status
FAU_GEN.1	FPT_STM.1	FPT_STM.1	Satisfied
FCS_COP.1	FCS_CKM.1 or FDP_ITC.1/2	FCS_CKM.1	Satisfied
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	Satisfied
[TODO]	[TODO]	[TODO]	[TODO]

23.4.2 4.2 Satisfaction of All Dependencies

Summary: - Number of SFRs with dependencies: [TODO: X] - Number of satisfied dependencies: [TODO: X] - Number of unsatisfied dependencies: [TODO: 0]

[TODO: If dependencies are not satisfied, justify this in detail]

23.4.3 4.3 Detailed Rationale for Critical Dependencies

[TODO: For complex or critical dependencies, provide detailed explanations]

Example:

```
FCS_COP.1 requires FCS_CKM.1 (Cryptographic key generation) because cryptographic
operations can only be performed securely with correctly generated keys. This dependency
is satisfied by the implementation of FCS_CKM.1, which specifies the generation of keys
according to [Standard].
```

23.5 5. Internal Consistency of SFRs

23.5.1 5.1 Consistency Check

[TODO: Demonstrate that the SFRs are internally consistent]

Checked Aspects: - No contradictory requirements - Compatible operations (Assignments, Selections) - Consistent terminology - No overlaps or redundancies

Result: [TODO: Confirmation of consistency]

23.5.2 5.2 Identified Conflicts and Resolution

[TODO: If conflicts were identified, describe their resolution]

Example:

```
Conflict: FDP_ACC.1 and FMT_MSA.1 could have different interpretations of
"security attributes".

Resolution: The security attributes were clearly defined in section X.Y and
both SFRs use this consistent definition.
```

23.6 6. Rationale for SARs

23.6.1 6.1 EAL Selection

Selected EAL: [TODO: e.g., EAL4]

Rationale: [TODO: Reference to document 0410 and summary]

The selection of EAL [TODO: X] is appropriate because: - [TODO: Rationale 1] - [TODO: Rationale 2] - [TODO: Rationale 3]

23.6.2 6.2 Augmentation

[TODO: If additional SARs beyond the EAL package are used]

Additional SARs: - [TODO: SAR-ID]: [TODO: Rationale for addition]

No Augmentation: [TODO: If no augmentation, confirm this]

The standard SARs for EAL [TODO: X] are sufficient for the evaluation of the TOE. No additional SARs are required.

23.7 7. Addressing Security Objectives for the Environment

23.7.1 7.1 Non-TOE Security Requirements

[TODO: Explain how security objectives for the environment are addressed]

The security objectives for the environment (from document 0300) are not addressed by SFRs, but by: - Organizational measures - Physical security measures - Environmental assumptions

Example:

```
O.ENV_PHYSICAL (Physical protection) is addressed by organizational measures such as
access controls and monitoring, not by TOE functionality.
```

23.8 8. Traceability

23.8.1 8.1 Traceability Matrix

Complete traceability between threats, security objectives, and SFRs is shown in the following matrix:

Threat	Security Objective	SFR	Rationale
T.UNAUTH_ACCESS	O.ACCESS	FIA_UID.1, FIA_UAU.1, FDP_ACC.1	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]

23.8.2 8.2 Coverage Matrix

A detailed Coverage Matrix can be found in document 0440.

23.9 9. Summary

23.9.1 9.1 Completeness

The selected security requirements are complete: - All security objectives for the TOE are addressed by SFRs - All SFR dependencies are satisfied - The SARs correspond to the selected EAL

23.9.2 9.2 Consistency

The security requirements are consistent: - No contradictory requirements - Internal consistency of SFRs - Consistent terminology

23.9.3 9.3 Appropriateness

The security requirements are appropriate: - Necessary to fulfill security objectives - Sufficient to address threats - Practically implementable in the TOE

23.10 10. References

- Document 0200: Security Problem Definition
- Document 0300: Security Objectives
- Document 0400: Security Requirements
- Document 0410: Evaluation Assurance Level
- Document 0430: SFR Dependencies
- Document 0440: Coverage Matrix
- ISO/IEC 15408-2:2022 - Security functional requirements
- ISO/IEC 15408-3:2022 - Security assurance requirements

Next Steps: 1. Complete all [TODO] placeholders 2. Create complete mapping tables 3. Verify all dependencies 4. Conduct peer review of rationale 5. Update when objectives or requirements change

ewpage

Chapter 24

SFR Dependencies

Document-ID: 0430
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and adapt the content to your specific Target of Evaluation (TOE).

24.1 1. Introduction

This document documents all dependencies between the Security Functional Requirements (SFRs) of the TOE and demonstrates their satisfaction. According to ISO/IEC 15408-2, SFRs may have dependencies on other SFRs that must be satisfied for the requirement to function correctly.

24.2 2. Overview of SFR Dependencies

24.2.1 2.1 Summary

Statistics: - Number of selected SFRs: [TODO: X] - Number of SFRs with dependencies: [TODO: X] - Total number of dependencies: [TODO: X] - Number of satisfied dependencies: [TODO: X] - Number of unsatisfied dependencies: [TODO: 0]

Status: [TODO: All dependencies satisfied / Dependencies not satisfied]

24.2.2 2.2 Complete Dependency Table

SFR-ID	SFR-Name	Dependency	Satisfied by	Status	Notes
FAU_GEN.1	Audit data generation	FPT_STM.1	FPT_STM.1		Time stamps for audit records
FAU_SAR.1	Audit review	FAU_GEN.1	FAU_GEN.1		Audit data must be generated
FCS_CKM.1	Cryptographic key generation	[FCS_CKM.2 or FCS_COP.1]	FCS_COP.1		Keys for cryptographic operations
FCS_COP.1	Cryptographic operation	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1		Key generation
FDP_ACC.1	Subset access control	FDP_ACF.1	FDP_ACF.1		Access control functions
FDP_ACF.1	Security attribute based access control	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3		Access control policy and attribute management
FIA_UAU.1	Timing of authentication	FIA_UID.1	FIA_UID.1		Identification before authentication
FIA_UID.1	Timing of identification	None	N/A		No dependencies
FMT_MSA.1	Management of security attributes	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1		Access control and role management
FMT_MSA.3	Static attribute initialisation	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1		Attribute management and roles
FMT_SMF.1	Specification of Management Functions	None	N/A		No dependencies

SFR-ID	SFR-Name	Dependency	Satisfied by	Status	Notes
FMT_SMR.1	Security roles	FIA_UID.1	FIA_UID.1		Identification for role assignment
FPT_STM.1	Reliable time stamps	None	N/A		No dependencies
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

24.3 3. Detailed Dependency Analysis

24.3.1 3.1 Security Audit (FAU)

24.3.1.1 FAU_GEN.1 Audit data generation

Dependencies: - FPT_STM.1 Reliable time stamps

Satisfaction: FPT_STM.1 is included in the Security Target and provides reliable time stamps for audit records.

Rationale: Audit records must be timestamped with precise time information to ensure chronological traceability of security events.

24.3.1.2 FAU_SAR.1 Audit review

Dependencies: - FAU_GEN.1 Audit data generation

Satisfaction: FAU_GEN.1 is included in the Security Target and generates the audit data that is reviewed by FAU_SAR.1.

Rationale: Audit data must exist before it can be reviewed.

24.3.2 3.2 Cryptographic Support (FCS)

24.3.2.1 FCS_CKM.1 Cryptographic key generation

Dependencies: - [FCS_CKM.2 Cryptographic key distribution] or FCS_COP.1 Cryptographic operation

Satisfaction: FCS_COP.1 is included in the Security Target. Generated keys are used for cryptographic operations.

Rationale: Keys must be generated for a purpose. In this case, they are used for cryptographic operations (FCS_COP.1).

24.3.2.2 FCS_COP.1 Cryptographic operation

Dependencies: - [FDP_ITC.1 Import of user data without security attributes] or [FDP_ITC.2 Import of user data with security attributes] or FCS_CKM.1 Cryptographic key generation

Satisfaction: FCS_CKM.1 is included in the Security Target and generates the keys required for cryptographic operations.

Rationale: Cryptographic operations require keys that must either be imported or generated.

24.3.3 3.3 User Data Protection (FDP)

24.3.3.1 FDP_ACC.1 Subset access control

Dependencies: - FDP_ACF.1 Security attribute based access control

Satisfaction: FDP_ACF.1 is included in the Security Target and defines the access control functions.

Rationale: An access control policy (FDP_ACC.1) requires access control functions (FDP_ACF.1) for enforcement.

24.3.3.2 FDP_ACF.1 Security attribute based access control

Dependencies: - FDP_ACC.1 Subset access control - FMT_MSA.3 Static attribute initialisation

Satisfaction: Both dependencies are included in the Security Target.

Rationale: - FDP_ACC.1: Access control functions require an access control policy - FMT_MSA.3: Security attributes must be initialized before they can be used for access decisions

24.3.4 3.4 Identification and Authentication (FIA)

24.3.4.1 FIA_UID.1 Timing of identification

Dependencies: None

Satisfaction: N/A

24.3.4.2 FIA_UAU.1 Timing of authentication

Dependencies: - FIA_UID.1 Timing of identification

Satisfaction: FIA_UID.1 is included in the Security Target.

Rationale: Users must be identified before they can be authenticated.

24.3.5 3.5 Security Management (FMT)

24.3.5.1 FMT_MSA.1 Management of security attributes

Dependencies: - FDP_ACC.1 Subset access control or [FDP_IFC.1 Subset information flow control] - FMT_SMR.1 Security roles - FMT_SMF.1 Specification of Management Functions

Satisfaction: All dependencies are included in the Security Target.

Rationale: - FDP_ACC.1: Security attributes are used for access control - FMT_SMR.1: Management of attributes requires role definitions - FMT_SMF.1: Management functions must be specified

24.3.5.2 FMT_MSA.3 Static attribute initialisation

Dependencies: - FMT_MSA.1 Management of security attributes - FMT_SMR.1 Security roles

Satisfaction: Both dependencies are included in the Security Target.

Rationale: Attribute initialization requires attribute management and role definitions.

24.3.5.3 FMT_SMF.1 Specification of Management Functions

Dependencies: None

Satisfaction: N/A

24.3.5.4 FMT_SMR.1 Security roles

Dependencies: - FIA_UID.1 Timing of identification

Satisfaction: FIA_UID.1 is included in the Security Target.

Rationale: Roles can only be assigned to identified users.

24.3.6 3.6 Protection of the TSF (FPT)

24.3.6.1 FPT_STM.1 Reliable time stamps

Dependencies: None

Satisfaction: N/A

24.3.7 3.7 [TODO: Additional SFR Classes]

[TODO: Add dependency analyses for all other used SFRs]

24.4 4. Dependency Graph

24.4.1 4.1 Visualization

[TODO: Create a dependency graph that visualizes the relationships between SFRs]

```
Example Graph (as text):

FIA_UID.1    > FIA_UAU.1
              > FMT_SMR.1    > FMT_MSA.1  > FDP_ACF.1
                               > FMT_MSA.3

FPT_STM.1  > FAU_GEN.1  > FAU_SAR.1

FCS_CKM.1   > FCS_COP.1                          FDP_ACC.1
```

24.4.2 4.2 Critical Paths

[TODO: Identify critical dependency paths]

Critical Path 1: Access Control

```
FIA_UID.1 → FMT_SMR.1 → FMT_MSA.1 → FDP_ACF.1   FDP_ACC.1
```

Critical Path 2: Audit

```
FPT_STM.1 → FAU_GEN.1 → FAU_SAR.1
```

24.5 5. Unsatisfied Dependencies

24.5.1 5.1 Overview

[TODO: If dependencies are not satisfied, document them here]

Status: [TODO: No unsatisfied dependencies / X unsatisfied dependencies]

24.5.2 5.2 Rationale for Unsatisfied Dependencies

[TODO: For each unsatisfied dependency, provide a detailed rationale]

Example (if applicable):

```
SFR: FCS_CKM.1
Dependency: FCS_CKM.2 or FCS_COP.1
Status: Partially satisfied (only FCS_COP.1)

Rationale: FCS_CKM.2 (Key distribution) is not required because the TOE does not
perform key distribution to external entities. All keys are generated and used
internally (FCS_COP.1).
```

24.6 6. Hierarchical Relationships

24.6.1 6.1 Use of Hierarchical Components

[TODO: Document if hierarchically higher SFR components are used]

According to ISO/IEC 15408-2, a hierarchically higher component automatically satisfies the dependencies of lower components.

Example:

```
If FDP_ACC.2 (Complete access control) is used, it automatically satisfies
the dependency on FDP_ACC.1 (Subset access control).
```

24.7 7. Iterations

24.7.1 7.1 Iterated SFRs

[TODO: If SFRs are used multiple times (iteration), document the dependencies for each iteration]

Iterated SFR	Iteration	Dependencies	Satisfaction
[TODO: e.g., FDP_ACC.1/1]	1	FDP_ACF.1/1	
[TODO: e.g., FDP_ACC.1/2]	2	FDP_ACF.1/2	

24.8 8. Validation

24.8.1 8.1 Validation Checklist

☐ All SFRs are listed in the dependency table

☐ All dependencies are correctly identified according to ISO/IEC 15408-2
☐ All dependencies are satisfied or justified
☐ Hierarchical relationships are correctly considered
☐ Iterations are fully documented
☐ Dependency graph is consistent with the table

24.8.2 8.2 Peer Review

Reviewer: [TODO: Name]
Date: [TODO: Date]
Status: [TODO: Approved / Changes requested]
Comments: [TODO: Comments]

24.9 9. References

- Document 0400: Security Requirements
- Document 0420: Requirements Rationale
- ISO/IEC 15408-2:2022 - Security functional requirements (Annex B: Dependencies)
- [TODO: Other relevant documents]

Next Steps: 1. Complete all [TODO] placeholders 2. Create complete dependency table 3. Verify all dependencies against ISO/IEC 15408-2 4. Create dependency graph 5. Conduct peer review 6. Update when SFRs change

ewpage

Chapter 25

Coverage Matrix

Document-ID: 0440
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and adapt the content to your specific Target of Evaluation (TOE).

25.1 1. Introduction

This document provides comprehensive coverage matrices that demonstrate traceability between all elements of the Security Target:

- Threats
- Organizational Security Policies (OSPs)
- Assumptions
- Security Objectives
- Security Requirements

The matrices ensure complete coverage and consistency of the Security Target.

25.2 2. Threats → Security Objectives

25.2.1 2.1 Threat Coverage Matrix

This matrix shows how each identified threat is addressed by security objectives.

Threat	Description	Addressing Security Objectives	Coverage
T.UNAUTH_ACCESS	Unauthorized access to TOE functions	O.ACCESS, O.IDENTIFY, O.AUTHENTICATE	Complete
T.DATA_DISCLOSURE	Unauthorized disclosure of data	O.CRYPTO, O.ACCESS	Complete
T.DATA_MANIPULATION	Unauthorized manipulation of data	O.INTEGRITY, O.ACCESS, O.AUDIT	Complete
T.MASQUERADE	Identity spoofing	O.AUTHENTICATE, O.IDENTIFY	Complete
T.AUDIT_COMPROMISE	Compromise of audit data	O.AUDIT, O.PROTECT_TSF	Complete
[TODO]	[TODO]	[TODO]	[TODO]

25.2.2 2.2 Completeness Analysis

Statistics: - Number of identified threats: [TODO: X] - Number of fully addressed threats: [TODO: X] - Number of partially addressed threats: [TODO: 0] - Number of unaddressed threats: [TODO: 0]

Status: [TODO: All threats addressed / Gaps present]

25.2.3 2.3 Unaddressed Threats

[TODO: If threats are not fully addressed, justify this]

Example (if applicable):

```
Threat: T.PHYSICAL_ATTACK
Status: Not addressed by TOE
Rationale: Physical attacks are addressed by environmental assumptions
(A.PHYSICAL_PROTECTION) and organizational measures, not by TOE functionality.
```

25.3 3. OSPs → Security Objectives

25.3.1 3.1 OSP Coverage Matrix

This matrix shows how organizational security policies are implemented through security objectives.

OSP	Description	Addressing Security Objectives	Coverage
P.ACCOUNTABILITY	Users actions must be traceable	O.AUDIT, O.IDENTIFY	Complete
P.AUTHORIZED_USERS	Only authorized users may access TOE	O.ACCESS, O.AUTHENTICATE	Complete
P.CRYPTOGRAPHY	Sensitive data must be encrypted	O.CRYPTO	Complete
[TODO]	[TODO]	[TODO]	[TODO]

25.3.2 3.2 Completeness Analysis

Statistics: - Number of defined OSPs: [TODO: X] - Number of fully implemented OSPs: [TODO: X] - Number of partially implemented OSPs: [TODO: 0] - Number of unimplemented OSPs: [TODO: 0]

Status: [TODO: All OSPs implemented / Gaps present]

25.4 4. Assumptions → Security Objectives for the Environment

25.4.1 4.1 Assumption Coverage Matrix

This matrix shows how assumptions are addressed by security objectives for the environment.

Assumption	Description	Addressing Environmental Objectives	Coverage
A.PHYSICAL_PROTECTION	The TOE is physically protected	OE.PHYSICAL	Complete
A.TRUSTED_ADMIN	Administrators are trustworthy	OE.ADMIN_TRAINING, OE.ADMIN_VETTING	Complete
A.NETWORK_PROTECTION	The network is protected against external attacks	OE.NETWORK_SECURITY	Complete
[TODO]	[TODO]	[TODO]	[TODO]

25.4.2 4.2 Completeness Analysis

Statistics: - Number of defined assumptions: [TODO: X] - Number of fully addressed assumptions: [TODO: X] - Number of partially addressed assumptions: [TODO: 0] - Number of unaddressed assumptions: [TODO: 0]

Status: [TODO: All assumptions addressed / Gaps present]

25.5 5. Security Objectives for TOE → SFRs

25.5.1 5.1 Security Objectives to SFRs Matrix

This matrix shows how security objectives for the TOE are fulfilled by Security Functional Requirements.

Security Objective	Description	Fulfilling SFRs	Coverage
O.ACCESS	Access control to TOE resources	FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3	Complete
O.IDENTIFY	Identification of users	FIA_UID.1	Complete

Security Objective	Description	Fulfilling SFRs	Coverage
O.AUTHENTICATE	Authentication of users	FIA_UAU.1, FIA_AFL.1	Complete
O.AUDIT	Audit recording of security-relevant events	FAU_GEN.1, FAU_SAR.1, FPT_STM.1	Complete
O.CRYPTO	Cryptographic protection of sensitive data	FCS_CKM.1, FCS_COP.1	Complete
O.INTEGRITY	Protection of data integrity	FDP_SDI.1, FPT_TST.1	Complete
O.PROTECT_TSF	Protection of TSF functionality	FPT_STM.1, FPT_TST.1	Complete
O.MANAGE	Secure management of TOE	FMT_SMF.1, FMT_SMR.1, FMT_MOF.1	Complete
[TODO]	[TODO]	[TODO]	[TODO]

25.5.2 5.2 Completeness Analysis

Statistics: - Number of security objectives for TOE: [TODO: X] - Number of fully fulfilled objectives: [TODO: X] - Number of partially fulfilled objectives: [TODO: 0] - Number of unfulfilled objectives: [TODO: 0]

Status: [TODO: All objectives fulfilled / Gaps present]

25.5.3 5.3 Unfulfilled Security Objectives

[TODO: If security objectives are not fully fulfilled by SFRs, justify this]

25.6 6. Reverse Traceability: SFRs → Security Objectives

25.6.1 6.1 SFRs to Security Objectives Matrix

This matrix shows reverse traceability: Each SFR must fulfill at least one security objective.

SFR	Fulfilled Security Objectives	Necessity
FAU_GEN.1	O.AUDIT	Necessary
FAU_SAR.1	O.AUDIT	Necessary
FCS_CKM.1	O.CRYPTO	Necessary
FCS_COP.1	O.CRYPTO	Necessary
FDP_ACC.1	O.ACCESS	Necessary
FDP_ACF.1	O.ACCESS	Necessary
FDP_SDI.1	O.INTEGRITY	Necessary
FIA_AFL.1	O.AUTHENTICATE	Necessary
FIA_UAU.1	O.AUTHENTICATE	Necessary
FIA_UID.1	O.IDENTIFY	Necessary

SFR	Fulfilled Security Objectives	Necessity
FMT_MOF.1	O.MANAGE	Necessary
FMT_MSA.1	O.ACCESS, O.MANAGE	Necessary
FMT_MSA.3	O.ACCESS	Necessary
FMT_SMF.1	O.MANAGE	Necessary
FMT_SMR.1	O.MANAGE	Necessary
FPT_STM.1	O.AUDIT, O.PROTECT_TSF	Necessary
FPT_TST.1	O.INTEGRITY, O.PROTECT_TSF	Necessary
[TODO]	[TODO]	[TODO]

25.6.2 6.2 Superfluous SFRs

[TODO: Identify SFRs that do not fulfill any security objective (should be none)]

Status: [TODO: No superfluous SFRs / Superfluous SFRs identified]

25.7 7. Complete Traceability Matrix

25.7.1 7.1 End-to-End Traceability

This matrix shows complete traceability from threats to SFRs.

Threat/OSP/Assumption	Security Objective	SFR	Rationale
T.UNAUTH_ACCESS	O.ACCESS	FDP_ACC.1, FDP_ACF.1	Access control prevents unauthorized access
T.UNAUTH_ACCESS	O.IDENTIFY	FIA_UID.1	Identification required before access
T.UNAUTH_ACCESS	O.AUTHENTICATE	FIA_UAU.1	Authentication verifies identity
T.DATA_DISCLOSURE	O.CRYPTO	FCS_COP.1	Encryption protects against disclosure
T.DATA_DISCLOSURE	O.ACCESS	FDP_ACC.1	Access control limits data access
T.DATA_MANIPULATION	O.INTEGRITY	FDP_SDI.1	Integrity checking detects manipulation
T.DATA_MANIPULATION	O.ACCESS	FDP_ACC.1	Access control prevents unauthorized changes

Threat/OSP/Assumption	Security Objective	SFR	Rationale
T.DATA_MANIPULATION	O.AUDIT	FAU_GEN.1	Audit recording documents changes
[TODO]	[TODO]	[TODO]	[TODO]

25.8 8. Coverage Gaps Analysis

25.8.1 8.1 Identified Gaps

[TODO: Identify and document gaps in coverage]

Gap Types: - Threats without security objectives - Security objectives without SFRs - SFRs without security objectives - OSPs without implementation

Status: [TODO: No gaps / X gaps identified]

25.8.2 8.2 Rationale for Gaps

[TODO: For each identified gap, provide a rationale]

Example (if applicable):

```
Gap: Threat T.PHYSICAL_ATTACK has no TOE security objective
Rationale: Physical threats are addressed by environmental assumptions and objectives,
not by TOE functionality. See A.PHYSICAL_PROTECTION and OE.PHYSICAL.
```

25.9 9. Visualization

25.9.1 9.1 Traceability Diagram

[TODO: Create a diagram that visualizes traceability]

```
Example (as text):

Threats              Security Objectives      SFRs

T.UNAUTH_ACCESS    > O.ACCESS        > FDP_ACC.1
                                           > FDP_ACF.1
                     > O.IDENTIFY      > FIA_UID.1
                     > O.AUTHENTICATE   > FIA_UAU.1

T.DATA_DISCLOSURE   > O.CRYPTO        > FCS_CKM.1
                                           > FCS_COP.1
                     > O.ACCESS       > FDP_ACC.1

T.DATA_MANIPULATION > O.INTEGRITY     > FDP_SDI.1
                     > O.ACCESS       > FDP_ACC.1
                     > O.AUDIT         > FAU_GEN.1
                                           > FPT_STM.1
```

25.10 10. Validation and Maintenance

25.10.1 10.1 Validation Checklist

- ☐ All threats are addressed by security objectives
- ☐ All OSPs are implemented by security objectives
- ☐ All assumptions are addressed by environmental objectives
- ☐ All security objectives for TOE are fulfilled by SFRs
- ☐ All SFRs fulfill at least one security objective
- ☐ No gaps in coverage (or justified)
- ☐ Traceability is bidirectionally complete

25.10.2 10.2 Maintenance Notes

When Changes Occur: - New threat → Add security objective → Add SFR - New SFR → Assign to security objective → Assign to threat/OSP - Removed threat → Check if security objective still needed - Removed SFR → Check if security objective still fulfilled

Update Frequency: - With every change to threats, objectives, or requirements - Before each review milestone - Before submission for evaluation

25.11 11. Summary

25.11.1 11.1 Coverage Summary

Completeness: - All threats addressed: [TODO: X/X] - All OSPs implemented: [TODO: X/X] - All assumptions addressed: [TODO: X/X] - All security objectives fulfilled: [TODO: X/X] - All SFRs necessary: [TODO: X/X]

Overall Status: [TODO: Complete / Gaps present]

25.11.2 11.2 Audit Readiness

[TODO: Confirm readiness for audit]

The coverage matrices demonstrate complete and consistent traceability between all elements of the Security Target. The TOE is ready for evaluation.

25.12 12. References

- Document 0200: Security Problem Definition
- Document 0300: Security Objectives
- Document 0400: Security Requirements
- Document 0420: Requirements Rationale
- Document 0430: SFR Dependencies
- ISO/IEC 15408-1:2022 - Introduction and general model
- ISO/IEC 15408-2:2022 - Security functional requirements
- ISO/IEC 15408-3:2022 - Security assurance requirements

Next Steps: 1. Complete all [TODO] placeholders 2. Create complete coverage matrices 3. Identify and justify gaps 4. Create traceability diagram 5. Conduct peer review 6. Keep matrices updated when changes occur

ewpage

Chapter 26

TOE Summary Specification

Document-ID: 0500
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and adapt the content to your specific TOE (Target of Evaluation).

26.1 1. Introduction

26.1.1 1.1 Purpose

This document describes the TOE Summary Specification (TSS) for [**TODO: TOE Name**]. The TSS shows how the TOE fulfills the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) defined in Chapter 4 (Security Requirements).

26.1.2 1.2 Structure of the TSS

The TOE Summary Specification is structured as follows:

- **Chapter 2**: Overview of TOE Security Functions (TSFs)
- **Chapter 3**: Detailed description of security functions
- **Chapter 4**: Mapping of security functions to SFRs (Coverage Matrix)
- **Chapter 5**: Assurance Measures
- **Chapter 6**: Strength of Function (SOF)

26.2 2. Overview of TOE Security Functions

26.2.1 2.1 Security Functions - Overview

The TOE implements the following security functions (TSFs):

TSF-ID	Security Function	Description	Associated SFRs
TSF-1	[TODO: Name]	[TODO: Brief description]	[TODO: SFR-IDs]
TSF-2	[TODO: Name]	[TODO: Brief description]	[TODO: SFR-IDs]
TSF-3	[TODO: Name]	[TODO: Brief description]	[TODO: SFR-IDs]

26.2.2 2.2 Architecture of Security Functions

`[TODO: Insert diagram - Architecture of TSFs]`

`Example:`

```
           TOE Security Functions


    TSF-1: I&A       TSF-2: Access
                     Control


    TSF-3: Audit     TSF-4: Crypto
```

Description:

[TODO: Describe the architecture of the security functions. Explain how the various TSFs work together and what dependencies exist.]

26.3 3. Detailed Description of Security Functions

26.3.1 3.1 TSF-1: [TODO: Name of Security Function]

TSF-ID: TSF-1
Associated SFRs: [TODO: e.g., FIA_UID.1, FIA_UAU.1]

26.3.1.1 3.1.1 Function Description

[TODO: Describe the security function in detail. Explain: - What the function does - How it works (at an appropriate level of abstraction) - What inputs it processes - What outputs it produces - What security properties it ensures]

Example: The Identification and Authentication function (TSF-1) ensures that all users are identified and authenticated before accessing TOE functions. The function uses a username for identification and a password for authentication. Passwords are stored hashed with SHA-256 and salted.

26.3.1.2 3.1.2 Fulfillment of SFRs

[TODO: For each associated SFR, explain how this security function fulfills the requirement.]

SFR [TODO: ID]: - [TODO: Description of how the SFR is fulfilled]

SFR [TODO: ID]: - [TODO: Description of how the SFR is fulfilled]

26.3.1.3 3.1.3 Interfaces

[TODO: Describe the interfaces of this TSF to other TSFs or external components.]

- **Interface to TSF-X:** [TODO: Description]
- **External Interfaces:** [TODO: Description]

26.3.2 3.2 TSF-2: [TODO: Name of Security Function]

TSF-ID: TSF-2
Associated SFRs: [TODO: SFR-IDs]

26.3.2.1 3.2.1 Function Description

[TODO: Description analogous to 3.1.1]

26.3.2.2 3.2.2 Fulfillment of SFRs

[TODO: Description analogous to 3.1.2]

26.3.2.3 3.2.3 Interfaces

[TODO: Description analogous to 3.1.3]

26.3.3 3.3 TSF-3: [TODO: Name of Security Function]

[TODO: Describe additional security functions following the same schema]

26.4 4. Mapping of Security Functions to SFRs

26.4.1 4.1 Coverage Matrix

The following table shows the mapping between security functions (TSFs) and Security Functional Requirements (SFRs):

SFR-ID	SFR-Name	TSF-1	TSF-2	TSF-3	TSF-4	TSF-5
[TODO]	[TODO]	X				
[TODO]	[TODO]	X	X			
[TODO]	[TODO]		X			
[TODO]	[TODO]			X		

26.4.2 4.2 Completeness Check

Coverage of SFRs: - Number of SFRs: [TODO: Number] - Number of covered SFRs: [TODO: Number] - Coverage rate: [TODO: Percentage]

Uncovered SFRs: [TODO: List all SFRs that are not covered by TSFs. If all are covered, write "None".]

26.5 5. Assurance Measures

26.5.1 5.1 Overview

The following Assurance Measures are implemented to fulfill the Security Assurance Requirements (SARs):

SAR-ID	SAR-Name	Assurance Measure	Description
[TODO]	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]

26.5.2 5.2 Mapping to Evaluation Assurance Level

The TOE is evaluated at **[TODO: EAL level, e.g., EAL4]**. The following Assurance Measures support this EAL:

[TODO: List the Assurance Measures required for the chosen EAL.]

Example for EAL4: - Configuration Management (ACM_CAP.4, ACM_SCP.2) - Delivery and Operation (ADO_DEL.2, ADO_IGS.1) - Development (ADV_FSP.2, ADV_IMP.1, ADV_TDS.2) - Guidance Documents (AGD_ADM.1, AGD_USR.1) - Life Cycle Support (ALC_DVS.1, ALC_LCD.1, ALC_TAT.1) - Tests (ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2) - Vulnerability Assessment (AVA_MSU.2, AVA_SOF.1, AVA_VLA.2)

26.6 6. Strength of Function (SOF)

26.6.1 6.1 SOF-Claim

The TOE claims the following Strength of Function:

SOF-Claim: [TODO: SOF-basic / SOF-medium / SOF-high]

26.6.2 6.2 SOF-Analysis

The following table shows the strength of individual probabilistic or permutation-based security mechanisms:

TSF-ID	Mechanism	SOF-Level	Rationale
[TODO]	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]

26.6.3 6.3 Fulfillment of SOF-Claim

[TODO: Explain how the analyzed mechanisms fulfill the SOF-Claim. Show that all relevant mechanisms achieve at least the claimed SOF level.]

Summary: - Number of analyzed mechanisms: [TODO] - Lowest SOF level: [TODO] - Fulfillment of SOF-Claim: [TODO: Yes/No]

26.7 7. Summary

26.7.1 7.1 Completeness of TSS

The TOE Summary Specification is complete and covers all aspects:

- All SFRs are covered by TSFs
- All SARs are covered by Assurance Measures
- SOF-Claim is analyzed and justified
- All security functions are described in detail

26.7.2 7.2 Reference to Additional Documents

For detailed information see:

- **0510_Assurance_Measures.md**: Detailed description of assurance measures
- **0520_Functions_Rationale.md**: Rationale for mapping TSFs to SFRs
- **0530_Coverage_Matrix.md**: Complete Coverage Matrix
- **0540_Strength_of_Function.md**: Detailed SOF analysis

Document History:

Version	Date	Author	Changes
0.1	[TODO]	[TODO]	Initial version
1.0	[TODO]	[TODO]	[TODO]

ewpage

Chapter 27

Assurance Measures

Document-ID: 0510
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and adapt the content to your specific TOE (Target of Evaluation).

27.1 1. Introduction

27.1.1 1.1 Purpose

This document describes the Assurance Measures implemented to fulfill the Security Assurance Requirements (SARs) for [**TODO: TOE Name**].

The Assurance Measures demonstrate that: - The TOE has been correctly developed - The TOE has been adequately tested - The TOE is properly documented - The TOE can be securely delivered and operated

27.1.2 1.2 Evaluation Assurance Level

The TOE is evaluated at [**TODO: EAL level, e.g., EAL4**].

Rationale for EAL Selection: [TODO: Explain why this EAL is appropriate for the TOE. Consider: - The threat landscape - The criticality of the TOE - Stakeholder requirements - Cost-benefit considerations]

27.2 2. Assurance Measures by SAR Classes

27.2.1 2.1 Configuration Management (ACM)

27.2.1.1 2.1.1 ACM_CAP: CM Capabilities

SAR: [TODO: e.g., ACM_CAP.4 - Generation support and acceptance procedures]

Assurance Measure:

[TODO: Describe the Configuration Management Capabilities. Example:]

The project uses Git as a version control system. All TOE components (source code, configuration files, build scripts) and documentation are versioned in the repository.

CM Process: 1. All changes are developed in feature branches 2. Code reviews are required before merging 3. Automated tests must pass 4. Releases are marked with Git tags 5. Each release has a unique version number

CM Tools: - Version Control: Git - Repository: [TODO: URL] - Issue Tracking: [TODO: System] - Build System: [TODO: System]

Evidence: - CM Plan: [TODO: Document path] - Repository Access: [TODO: URL] - Build Logs: [TODO: Location]

27.2.1.2 2.1.2 ACM_SCP: CM Scope

SAR: [TODO: e.g., ACM_SCP.2 - Problem tracking CM coverage]

Assurance Measure:

[TODO: Describe the scope of Configuration Management. Example:]

Configuration Management covers: - All TOE source code files - Build scripts and configuration files - Security Target and associated documentation - Test suites and test documentation - Evaluation artifacts

CM Items: | Item-ID | Description | Type | Repository Path | |———|————-|——|————–| | [TODO] | [TODO] | Source Code | [TODO] | | [TODO] | [TODO] | Documentation | [TODO] | | [TODO] | [TODO] | Test Suite | [TODO] |

Evidence: - CM Scope Document: [TODO: Document path] - Configuration Item List: [TODO: Document path]

27.2.2 2.2 Delivery and Operation (ADO)

27.2.2.1 2.2.1 ADO_DEL: Delivery

SAR: [TODO: e.g., ADO_DEL.2 - Detection of modification]

Assurance Measure:

[TODO: Describe the Delivery measures. Example:]

The TOE is delivered with the following security measures:

Integrity Protection: - All releases are hashed with SHA-256 - Hashes are published on the official website - Releases are digitally signed (GPG/PGP) - Signature keys are available through secure channels

Delivery Process: 1. Build TOE from versioned source code 2. Automated tests 3. Creation of checksums 4. Digital signature 5. Upload to secure download servers 6. Publication of checksums and signatures

Evidence: - Delivery Procedures: [TODO: Document path] - Example Checksums: [TODO: URL] - Public Key: [TODO: URL]

27.2.2.2 2.2.2 ADO_IGS: Installation, Generation, and Start-up

SAR: [TODO: e.g., ADO_IGS.1 - Installation, generation, and start-up procedures]

Assurance Measure:

[TODO: Describe the installation and start-up procedures. Example:]

Installation Guide: - Detailed step-by-step instructions - System requirements - Security configuration - Installation verification

Evidence: - Installation Guide: [TODO: Document path] - Administrator Guide: [TODO: Document path]

27.2.3 2.3 Development (ADV)

27.2.3.1 2.3.1 ADV_FSP: Functional Specification

SAR: [TODO: e.g., ADV_FSP.2 - Security-enforcing functional specification]

Assurance Measure:

[TODO: Describe the Functional Specification. Example:]

The Functional Specification describes all external interfaces of the TOE:

Documentation: - TOE Security Functions (TSFs) are fully specified - All TSF interfaces are documented - Parameters, return values, and error handling are described - Security-relevant effects are documented

Evidence: - Functional Specification: [TODO: Document path] - API Documentation: [TODO: Document path]

27.2.3.2 2.3.2 ADV_IMP: Implementation Representation

SAR: [TODO: e.g., ADV_IMP.1 - Implementation representation of the TSF]

Assurance Measure:

[TODO: Describe the Implementation Representation. Example:]

The TOE source code is available and documented:

Code Documentation: - Inline comments for complex logic - Function and class documentation - Architecture documentation - Mapping between design and code

Evidence: - Source Code: [TODO: Repository URL] - Code Documentation: [TODO: Document path] - Architecture Document: [TODO: Document path]

27.2.3.3 2.3.3 ADV_TDS: TOE Design

SAR: [TODO: e.g., ADV_TDS.2 - Architectural design]

Assurance Measure:

[TODO: Describe the TOE Design. Example:]

The TOE design is documented at multiple levels of abstraction:

Design Documentation: - High-Level Architecture - Subsystem Design - Module Design - Security Architecture

Evidence: - TOE Design Document: [TODO: Document path] - Architecture Diagrams: [TODO: Document path]

27.2.4 2.4 Guidance Documents (AGD)

27.2.4.1 2.4.1 AGD_ADM: Administrator Guidance

SAR: [TODO: e.g., AGD_ADM.1 - Administrator guidance]

Assurance Measure:

[TODO: Describe the Administrator Guidance. Example:]

Administrator Documentation includes: - Secure installation and configuration - Security parameters and their meaning - Maintenance and updates - Audit log management - Backup and recovery - Incident response

Evidence: - Administrator Guide: [TODO: Document path] - Security Configuration Guide: [TODO: Document path]

27.2.4.2 2.4.2 AGD_USR: User Guidance

SAR: [TODO: e.g., AGD_USR.1 - User guidance]

Assurance Measure:

[TODO: Describe the User Guidance. Example:]

User Documentation includes: - Secure use of the TOE - Security functions and their use - Security notices and warnings - User responsibilities

Evidence: - User Guide: [TODO: Document path] - Security User Manual: [TODO: Document path]

27.2.5 2.5 Life Cycle Support (ALC)

27.2.5.1 2.5.1 ALC_DVS: Development Security

SAR: [TODO: e.g., ALC_DVS.1 - Identification of security measures]

Assurance Measure:

[TODO: Describe the Development Security Measures. Example:]

Security Measures in Development: - Access control to development systems - Secure development environment - Code review process - Security testing during development - Confidentiality agreements for developers

Evidence: - Development Security Policy: [TODO: Document path] - Access Control Matrix: [TODO: Document path]

27.2.5.2 2.5.2 ALC_LCD: Life Cycle Definition

SAR: [TODO: e.g., ALC_LCD.1 - Developer defined life-cycle model]

Assurance Measure:

[TODO: Describe the Life Cycle Model. Example:]

Development Life Cycle: 1. Requirements Analysis 2. Design 3. Implementation 4. Testing 5. Release 6. Maintenance

Evidence: - Life Cycle Model Document: [TODO: Document path] - Development Process Description: [TODO: Document path]

27.2.5.3 2.5.3 ALC_TAT: Tools and Techniques

SAR: [TODO: e.g., ALC_TAT.1 - Well-defined development tools]

Assurance Measure:

[TODO: Describe the tools and techniques used. Example:]

Development Tools: | Tool | Version | Purpose | Security Relevance | |——|———|———|———————-| | [TODO] | [TODO] | [TODO] | [TODO] |

Evidence: - Tools and Techniques Document: [TODO: Document path]

27.2.6 2.6 Tests (ATE)

27.2.6.1 2.6.1 ATE_COV: Coverage

SAR: [TODO: e.g., ATE_COV.2 - Analysis of coverage]

Assurance Measure:

[TODO: Describe the Test Coverage. Example:]

Test Coverage: - All TSF interfaces are tested - All SFRs are covered by tests - Coverage analysis is performed

Test Coverage Matrix: | TSF-ID | Test-ID | SFR-ID | Coverage | |———|———|———|———-| | [TODO] | [TODO] | [TODO] | [TODO]% |

Evidence: - Test Coverage Report: [TODO: Document path] - Coverage Matrix: [TODO: Document path]

27.2.6.2 2.6.2 ATE_DPT: Depth

SAR: [TODO: e.g., ATE_DPT.1 - Testing: high-level design]

Assurance Measure:

[TODO: Describe the Test Depth. Example:]

Test Depth: - Unit tests for individual modules - Integration tests for subsystems - System tests for the entire TOE - Security tests for TSFs

Evidence: - Test Plan: [TODO: Document path] - Test Results: [TODO: Document path]

27.2.6.3 2.6.3 ATE_FUN: Functional Tests

SAR: [TODO: e.g., ATE_FUN.1 - Functional testing]

Assurance Measure:

[TODO: Describe the Functional Tests. Example:]

Functional Tests: - All TSFs are tested - Positive and negative test cases - Boundary value tests - Error handling tests

Evidence: - Test Specification: [TODO: Document path] - Test Results: [TODO: Document path]

27.2.6.4 2.6.4 ATE_IND: Independent Testing

SAR: [TODO: e.g., ATE_IND.2 - Independent testing - sample]

Assurance Measure:

[TODO: Describe the Independent Testing Measures. Example:]

Independent Testing: - Evaluator performs a selection of tests - Evaluator can develop own tests - Test environment is provided

Evidence: - Test Environment Description: [TODO: Document path] - Sample Test Results: [TODO: Document path]

27.2.7 2.7 Vulnerability Assessment (AVA)

27.2.7.1 2.7.1 AVA_MSU: Misuse

SAR: [TODO: e.g., AVA_MSU.2 - Validation of analysis]

Assurance Measure:

[TODO: Describe the Misuse Analysis. Example:]

Misuse Analysis: - Analysis of misconfigurations - Analysis of insecure usage - Documentation of security warnings

Evidence: - Misuse Analysis: [TODO: Document path] - Security Warnings: [TODO: Document path]

27.2.7.2 2.7.2 AVA_SOF: Strength of Function

SAR: [TODO: e.g., AVA_SOF.1 - Strength of TOE security function evaluation]

Assurance Measure:

[TODO: Describe the SOF Evaluation. Example:]

SOF Evaluation: - Analysis of all probabilistic mechanisms - Calculation of attack strength - Comparison with SOF-Claim

Evidence: - SOF Analysis: [TODO: Document path, see 0540_Strength_of_Function.md]

27.2.7.3 2.7.3 AVA_VLA: Vulnerability Analysis

SAR: [TODO: e.g., AVA_VLA.2 - Independent vulnerability analysis]

Assurance Measure:

[TODO: Describe the Vulnerability Analysis. Example:]

Vulnerability Analysis: - Analysis of known vulnerabilities - Penetration testing - Code analysis for security flaws - Analysis of public vulnerability databases

Evidence: - Vulnerability Analysis Report: [TODO: Document path] - Penetration Test Results: [TODO: Document path]

27.3 3. Summary of Assurance Measures

27.3.1 3.1 Completeness Check

The following table shows the mapping of all SARs to Assurance Measures:

SAR-ID	SAR-Name	Assurance Measure	Status
[TODO]	[TODO]	[TODO]	
[TODO]	[TODO]	[TODO]	

Summary: - Number of SARs: [TODO] - Number of covered SARs: [TODO] - Coverage rate: [TODO]%

27.3.2 3.2 Evidence and Artifacts

The following documents and artifacts serve as evidence for the Assurance Measures:

Document	Type	Location	SAR Mapping
[TODO]	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]

27.4 4. Evaluator Activities

27.4.1 4.1 Required Evaluator Activities

Specific evaluator activities are required for each SAR:

[TODO: List the evaluator activities for each SAR. Example:]

ACM_CAP.4: - Review of CM system - Verification of version control - Review of acceptance procedures

ADV_FSP.2: - Review of Functional Specification - Verification of TSF descriptions - Completeness check

27.4.2 4.2 Provision of Evidence

All required evidence will be provided to the evaluator:

Delivery Method: - [TODO: e.g., Secure File Transfer, Evaluator Portal, etc.]

System Access: - [TODO: Describe how the evaluator gains access to development systems, test environments, etc.]

Document History:

Version	Date	Author	Changes
0.1	[TODO]	[TODO]	Initial version
1.0	[TODO]	[TODO]	[TODO]

ewpage

Chapter 28

Functions Rationale

Document-ID: 0520
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and adapt the content to your specific TOE (Target of Evaluation).

28.1 1. Introduction

28.1.1 1.1 Purpose

This document provides the rationale for the mapping of TOE Security Functions (TSFs) to Security Functional Requirements (SFRs) for **[TODO: TOE Name]**.

The Functions Rationale demonstrates that: - Each SFR is fulfilled by at least one TSF - The TSFs implement the SFRs completely and correctly - No gaps exist in the security functionality - The mapping between TSFs and SFRs is traceable

28.1.2 1.2 Structure

This document is structured as follows:

- **Chapter 2**: Overview of TSF SFR mapping
- **Chapter 3**: Detailed rationale for each SFR
- **Chapter 4**: Completeness analysis
- **Chapter 5**: Summary

28.2 2. Mapping Overview

28.2.1 2.1 Mapping Matrix

The following matrix shows the mapping between TSFs and SFRs:

SFR-ID	SFR-Name	TSF-1	TSF-2	TSF-3	TSF-4	TSF-5	TSF-6
[TODO]	[TODO]						
[TODO]	[TODO]						
[TODO]	[TODO]						
[TODO]	[TODO]						
[TODO]	[TODO]						

Legend: - = TSF fulfills this SFR (completely or partially)

28.2.2 2.2 TSF Overview

TSF-ID	TSF-Name	Number of Associated SFRs	Description
TSF-1	[TODO]	[TODO]	[TODO: Brief description]
TSF-2	[TODO]	[TODO]	[TODO: Brief description]
TSF-3	[TODO]	[TODO]	[TODO: Brief description]

28.3 3. Detailed Rationale

28.3.1 3.1 Security Audit (FAU)

28.3.1.1 3.1.1 FAU_GEN.1: Audit Data Generation

SFR Description: [TODO: Brief description of the SFR. Example:] The TOE must be able to generate audit records for security-relevant events.

Associated TSFs: - TSF-[TODO]: [TODO: TSF Name]

Rationale:

[TODO: Detailed rationale. Example:]

TSF-3 (Audit Function) fulfills FAU_GEN.1 through the following mechanisms:

1. **Event Detection**: The audit function monitors all security-relevant events, including:
   - Authentication attempts (successful and failed)
   - Access to protected resources
   - Changes to security parameters
   - Administrative actions
2. **Audit Records**: For each event, an audit record is generated containing:
   - Timestamp
   - Event type
   - User ID
   - Result (Success/Failure)

- Additional event-specific information

3. **Completeness**: All events required by FAU_GEN.1 are captured.

Fulfillment Level: Completely fulfilled

28.3.1.2 3.1.2 FAU_SAR.1: Audit Review

SFR Description: [TODO: Description of the SFR]

Associated TSFs: - TSF-[TODO]: [TODO: TSF Name]

Rationale:

[TODO: Detailed rationale analogous to 3.1.1]

Fulfillment Level: [TODO: Completely fulfilled / Partially fulfilled / With limitations]

28.3.2 3.2 Cryptographic Support (FCS)

28.3.2.1 3.2.1 FCS_CKM.1: Cryptographic Key Generation

SFR Description: [TODO: Description of the SFR]

Associated TSFs: - TSF-[TODO]: [TODO: TSF Name]

Rationale:

[TODO: Detailed rationale]

Fulfillment Level: [TODO]

28.3.2.2 3.2.2 FCS_COP.1: Cryptographic Operation

SFR Description: [TODO: Description of the SFR]

Associated TSFs: - TSF-[TODO]: [TODO: TSF Name]

Rationale:

[TODO: Detailed rationale]

Fulfillment Level: [TODO]

28.3.3 3.3 User Data Protection (FDP)

28.3.3.1 3.3.1 FDP_ACC.1: Subset Access Control

SFR Description: [TODO: Description of the SFR]

Associated TSFs: - TSF-[TODO]: [TODO: TSF Name]

Rationale:

[TODO: Detailed rationale]

Fulfillment Level: [TODO]

28.3.3.2 3.3.2 FDP_ACF.1: Security Attribute Based Access Control

SFR Description: [TODO: Description of the SFR]

Associated TSFs: - TSF-[TODO]: [TODO: TSF Name]

Rationale:

[TODO: Detailed rationale]

Fulfillment Level: [TODO]

28.3.4 3.4 Identification and Authentication (FIA)

28.3.4.1 3.4.1 FIA_UID.1: Timing of Identification

SFR Description: [TODO: Description of the SFR]

Associated TSFs: - TSF-[TODO]: [TODO: TSF Name]

Rationale:

[TODO: Detailed rationale]

Fulfillment Level: [TODO]

28.3.4.2 3.4.2 FIA_UAU.1: Timing of Authentication

SFR Description: [TODO: Description of the SFR]

Associated TSFs: - TSF-[TODO]: [TODO: TSF Name]

Rationale:

[TODO: Detailed rationale]

Fulfillment Level: [TODO]

28.3.4.3 3.4.3 FIA_AFL.1: Authentication Failure Handling

SFR Description: [TODO: Description of the SFR]

Associated TSFs: - TSF-[TODO]: [TODO: TSF Name]

Rationale:

[TODO: Detailed rationale]

Fulfillment Level: [TODO]

28.3.5 3.5 Security Management (FMT)

28.3.5.1 3.5.1 FMT_SMF.1: Specification of Management Functions

SFR Description: [TODO: Description of the SFR]

Associated TSFs: - TSF-[TODO]: [TODO: TSF Name]

Rationale:

[TODO: Detailed rationale]

Fulfillment Level: [TODO]

28.3.5.2 3.5.2 FMT_SMR.1: Security Roles

SFR Description: [TODO: Description of the SFR]

Associated TSFs: - TSF-[TODO]: [TODO: TSF Name]

Rationale:

[TODO: Detailed rationale]

Fulfillment Level: [TODO]

28.3.6 3.6 Protection of the TSF (FPT)

28.3.6.1 3.6.1 FPT_STM.1: Reliable Time Stamps

SFR Description: [TODO: Description of the SFR]

Associated TSFs: - TSF-[TODO]: [TODO: TSF Name]

Rationale:

[TODO: Detailed rationale]

Fulfillment Level: [TODO]

28.3.7 3.7 TOE Access (FTA)

28.3.7.1 3.7.1 FTA_SSL.1: TSF-initiated Session Locking

SFR Description: [TODO: Description of the SFR]

Associated TSFs: - TSF-[TODO]: [TODO: TSF Name]

Rationale:

[TODO: Detailed rationale]

Fulfillment Level: [TODO]

28.3.8 3.8 Trusted Path/Channels (FTP)

28.3.8.1 3.8.1 FTP_TRP.1: Trusted Path

SFR Description: [TODO: Description of the SFR]

Associated TSFs: - TSF-[TODO]: [TODO: TSF Name]

Rationale:

[TODO: Detailed rationale]

Fulfillment Level: [TODO]

28.4 4. Completeness Analysis

28.4.1 4.1 Coverage of SFRs

Statistics: - Total number of SFRs: [TODO] - Completely fulfilled SFRs: [TODO] - Partially fulfilled SFRs: [TODO] - Unfulfilled SFRs: [TODO]

Coverage Rate: [TODO]%

28.4.2 4.2 Unfulfilled or Partially Fulfilled SFRs

[TODO: If SFRs are not completely fulfilled, list them here and justify:]

SFR-ID	Status	Rationale	Actions
[TODO]	Partially fulfilled	[TODO: Why only partially?]	[TODO: Planned actions]

Note: If all SFRs are completely fulfilled, write: "All SFRs are completely fulfilled."

28.4.3 4.3 Multiple Mappings

Some SFRs are fulfilled by multiple TSFs. This is the case in the following situations:

SFR-ID	Associated TSFs	Rationale for Multiple Mapping
[TODO]	TSF-X, TSF-Y	[TODO: Why multiple TSFs?]

28.4.4 4.4 TSF Coverage

The following table shows which TSFs fulfill how many SFRs:

TSF-ID	TSF-Name	Number of Fulfilled SFRs	Percentage
TSF-1	[TODO]	[TODO]	[TODO]%
TSF-2	[TODO]	[TODO]	[TODO]%
TSF-3	[TODO]	[TODO]	[TODO]%

Analysis: [TODO: Analyze the distribution. Are there TSFs that fulfill many SFRs? Is the distribution balanced?]

28.5 5. Summary

28.5.1 5.1 Completeness of Mapping

The mapping between TSFs and SFRs is complete:

- All SFRs are covered by at least one TSF
- All mappings are justified
- No gaps in security functionality
- Multiple mappings are explained

28.5.2 5.2 Correctness of Mapping

The rationales demonstrate that:

- The TSFs correctly implement the SFRs
- The TSFs provide the required functionality
- The TSFs ensure the security properties
- The mapping is traceable and convincing

28.5.3 5.3 Reference to Additional Documents

For further information see:

- **0500_TOE_Summary_Specification.md**: Detailed description of TSFs
- **0530_Coverage_Matrix.md**: Complete Coverage Matrix
- **Chapter 4 of the Security Target**: Definition of SFRs

Document History:

Version	Date	Author	Changes
0.1	[TODO]	[TODO]	Initial version
1.0	[TODO]	[TODO]	[TODO]

ewpage

Chapter 29

Coverage Matrix

Document-ID: 0530
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and adapt the content to your specific TOE (Target of Evaluation).

29.1 1. Introduction

29.1.1 1.1 Purpose

This document contains the complete Coverage Matrix for [**TODO: TOE Name**]. The matrix shows the mapping between:

- Security Objectives Threats, OSPs, Assumptions
- Security Functional Requirements (SFRs) Security Objectives
- TOE Security Functions (TSFs) SFRs
- Tests TSFs and SFRs
- Assurance Measures Security Assurance Requirements (SARs)

29.1.2 1.2 Legend

Coverage Levels: - = Complete coverage - = Partial coverage - = Supporting coverage - (empty) = No coverage

29.2 2. Security Objectives Coverage

29.2.1 2.1 Security Objectives for TOE Threats

This matrix shows how the Security Objectives for TOE address the identified Threats:

Threat-ID	Threat-Name	O.TOE-1	O.TOE-2	O.TOE-3	O.TOE-4	O.TOE-5
T.[TODO]	[TODO]					
T.[TODO]	[TODO]					
T.[TODO]	[TODO]					
T.[TODO]	[TODO]					
T.[TODO]	[TODO]					

Completeness Check: - Number of Threats: [TODO] - Number of covered Threats: [TODO] - Uncovered Threats: [TODO: List or “None”]

29.2.2 2.2 Security Objectives for TOE Organizational Security Policies

This matrix shows how the Security Objectives for TOE fulfill the OSPs:

OSP-ID	OSP-Name	O.TOE-1	O.TOE-2	O.TOE-3	O.TOE-4	O.TOE-5
P.[TODO]	[TODO]					
P.[TODO]	[TODO]					
P.[TODO]	[TODO]					

Completeness Check: - Number of OSPs: [TODO] - Number of covered OSPs: [TODO] - Uncovered OSPs: [TODO: List or “None”]

29.2.3 2.3 Security Objectives for Environment Threats

This matrix shows how the Security Objectives for Environment address the Threats:

Threat-ID	Threat-Name	O.ENV-1	O.ENV-2	O.ENV-3	O.ENV-4
T.[TODO]	[TODO]				
T.[TODO]	[TODO]				
T.[TODO]	[TODO]				

29.2.4 2.4 Security Objectives for Environment Assumptions

This matrix shows how the Security Objectives for Environment fulfill the Assumptions:

Assumption-ID	Assumption-Name	O.ENV-1	O.ENV-2	O.ENV-3	O.ENV-4
A.[TODO]	[TODO]				
A.[TODO]	[TODO]				
A.[TODO]	[TODO]				

Completeness Check: - Number of Assumptions: [TODO] - Number of covered Assumptions: [TODO] - Uncovered Assumptions: [TODO: List or “None”]

29.3 3. Security Functional Requirements Coverage

29.3.1 3.1 SFRs Security Objectives for TOE

This matrix shows how the SFRs fulfill the Security Objectives for TOE:

SFR-ID	SFR-Name	O.TOE-1	O.TOE-2	O.TOE-3	O.TOE-4	O.TOE-5
FAU_GEN.1	Audit data generation					
FAU_SAR.1	Audit review					
FCS_CKM.1	Cryptographic key generation					
FCS_COP.1	Cryptographic operation					
FDP_ACC.1	Subset access control					
FDP_ACF.1	Security attribute based access control					
FIA_UID.1	Timing of identification					
FIA_UAU.1	Timing of authentication					
FIA_AFL.1	Authentication failure handling					
FMT_SMF.1	Specification of management functions					
FMT_SMR.1	Security roles					
FPT_STM.1	Reliable time stamps					
FTA_SSL.1	TSF-initiated session locking					
FTP_TRP.1	Trusted path					

Completeness Check: - Number of SFRs: [TODO] - Number of Security Objectives for TOE: [TODO] - Uncovered SFRs: [TODO: List or “None”] - Uncovered Objectives: [TODO: List or “None”]

29.4 4. TOE Security Functions Coverage

29.4.1 4.1 TSFs SFRs

This matrix shows how the TSFs implement the SFRs:

SFR-ID	SFR-Name	TSF-1	TSF-2	TSF-3	TSF-4	TSF-5	TSF-6
FAU_GEN.1	Audit data generation						
FAU_SAR.1	Audit review						
FCS_CKM.1	Cryptographic key generation						
FCS_COP.1	Cryptographic operation						
FDP_ACC.1	Subset access control						
FDP_ACF.1	Security attribute based access control						
FIA_UID.1	Timing of identification						
FIA_UAU.1	Timing of authentication						
FIA_AFL.1	Authentication failure handling						
FMT_SMF.1	Specification of management functions						
FMT_SMR.1	Security roles						
FPT_STM.1	Reliable time stamps						
FTA_SSL.1	TSF-initiated session locking						
FTP_TRP.1	Trusted path						

SFR-ID	SFR-Name	TSF-1	TSF-2	TSF-3	TSF-4	TSF-5	TSF-6

TSF Descriptions:

TSF-ID	TSF-Name	Description
TSF-1	[TODO]	[TODO: Brief description]
TSF-2	[TODO]	[TODO: Brief description]
TSF-3	[TODO]	[TODO: Brief description]
TSF-4	[TODO]	[TODO: Brief description]
TSF-5	[TODO]	[TODO: Brief description]
TSF-6	[TODO]	[TODO: Brief description]

Completeness Check: - Number of SFRs: [TODO] - Number of covered SFRs: [TODO] - Uncovered SFRs: [TODO: List or “None”]

29.5 5. Test Coverage

29.5.1 5.1 Tests TSFs

This matrix shows how the tests verify the TSFs:

TSF-ID	TSF-Name	Test-1	Test-2	Test-3	Test-4	Test-5	Test-6
TSF-1	[TODO]						
TSF-2	[TODO]						
TSF-3	[TODO]						
TSF-4	[TODO]						
TSF-5	[TODO]						
TSF-6	[TODO]						

Test Descriptions:

Test-ID	Test-Name	Description	Test Type
Test-1	[TODO]	[TODO]	Unit / Integration / System
Test-2	[TODO]	[TODO]	Unit / Integration / System
Test-3	[TODO]	[TODO]	Unit / Integration / System
Test-4	[TODO]	[TODO]	Unit / Integration / System
Test-5	[TODO]	[TODO]	Unit / Integration / System
Test-6	[TODO]	[TODO]	Unit / Integration / System

Completeness Check: - Number of TSFs: [TODO] - Number of tested TSFs: [TODO] - Untested TSFs: [TODO: List or “None”]

29.5.2 5.2 Tests SFRs (indirect via TSFs)

This matrix shows the indirect coverage of SFRs by tests:

SFR-ID	SFR-Name	Test-1	Test-2	Test-3	Test-4	Test-5	Test-6
FAU_GEN.1	Audit data generation						
FAU_SAR.1	Audit review						
FCS_CKM.1	Cryptographic key generation						
FCS_COP.1	Cryptographic operation						
FDP_ACC.1	Subset access control						
FDP_ACF.1	Security attribute based access control						
FIA_UID.1	Timing of identification						
FIA_UAU.1	Timing of authentication						
FIA_AFL.1	Authentication failure handling						
FMT_SMF.1	Specification of management functions						
FMT_SMR.1	Security roles						
FPT_STM.1	Reliable time stamps						
FTA_SSL.1	TSF-initiated session locking						
FTP_TRP.1	Trusted path						

Completeness Check: - Number of SFRs: [TODO] - Number of tested SFRs: [TODO] - Untested SFRs: [TODO: List or “None”]

29.6 6. Assurance Measures Coverage

29.6.1 6.1 Assurance Measures SARs

This matrix shows how the Assurance Measures fulfill the SARs:

SAR-ID	SAR-Name	AM-1	AM-2	AM-3	AM-4	AM-5	AM-6
ACM_CAP.4	Generation support and acceptance procedures						
ACM_SCP.2	Problem tracking CM coverage						
ADO_DEL.2	Detection of modification						
ADO_IGS.1	Installation, generation, and start-up procedures						
ADV_FSP.2	Security-enforcing functional specification						
ADV_IMP.1	Implementation representation of the TSF						
ADV_TDS.2	Architectural design						
AGD_ADM.1	Administrator guidance						
AGD_USR.1	User guidance						
ALC_DVS.1	Identification of security measures						
ALC_LCD.1	Developer defined life-cycle model						
ALC_TAT.1	Well-defined development tools						
ATE_COV.2	Analysis of coverage						
ATE_DPT.1	Testing: high-level design						

SAR-ID	SAR-Name	AM-1	AM-2	AM-3	AM-4	AM-5	AM-6
ATE_FUN.1	Functional testing						
ATE_IND.2	Independent testing - sample						
AVA_MSU.2	Validation of analysis						
AVA_SOF.1	Strength of TOE security function evaluation						
AVA_VLA.2	Independent vulnerability analysis						

Assurance Measure Descriptions:

AM-ID	AM-Name	Description
AM-1	Configuration Management	[TODO]
AM-2	Delivery and Operation	[TODO]
AM-3	Development Documentation	[TODO]
AM-4	Guidance Documents	[TODO]
AM-5	Life Cycle Support	[TODO]
AM-6	Testing and Vulnerability Assessment	[TODO]

Completeness Check: - Number of SARs: [TODO] - Number of covered SARs: [TODO] - Uncovered SARs: [TODO: List or "None"]

29.7 7. Overall Summary

29.7.1 7.1 End-to-End Traceability

This overview shows the complete traceability from Threats to Tests:

```
Threats/OSPs/Assumptions
    ↓
Security Objectives (TOE & Environment)
    ↓
Security Functional Requirements (SFRs)
    ↓
TOE Security Functions (TSFs)
    ↓
Tests
```

Completeness Check: - All Threats are covered by Security Objectives - All Security Objectives are fulfilled by SFRs - All SFRs are implemented by TSFs - All TSFs are verified by Tests - All SARs are fulfilled by Assurance Measures

29.7.2 7.2 Statistics

Category	Count	Covered	Coverage Rate
Threats	[TODO]	[TODO]	[TODO]%
OSPs	[TODO]	[TODO]	[TODO]%
Assumptions	[TODO]	[TODO]	[TODO]%
Security Objectives (TOE)	[TODO]	[TODO]	[TODO]%
Security Objectives (ENV)	[TODO]	[TODO]	[TODO]%
SFRs	[TODO]	[TODO]	[TODO]%
TSFs	[TODO]	[TODO]	[TODO]%
Tests	[TODO]	[TODO]	[TODO]%
SARs	[TODO]	[TODO]	[TODO]%
Assurance Measures	[TODO]	[TODO]	[TODO]%

29.7.3 7.3 Identified Gaps

[TODO: List all identified gaps in coverage. If no gaps exist, write "No gaps identified".]

Category	Element	Gap	Action
[TODO]	[TODO]	[TODO]	[TODO]

29.8 8. Summary

The Coverage Matrix demonstrates:

- Complete traceability from Threats to Tests
- All security requirements are covered
- All security functions are tested
- All Assurance Requirements are fulfilled
- No critical gaps in coverage

Status: [TODO: Complete / With Gaps / In Progress]

Document History:

Version	Date	Author	Changes
0.1	[TODO]	[TODO]	Initial version
1.0	[TODO]	[TODO]	[TODO]

ewpage

Chapter 30

Strength of Function

Document-ID: 0540
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and adapt the content to your specific TOE (Target of Evaluation).

30.1 1. Introduction

30.1.1 1.1 Purpose

This document analyzes the Strength of Function (SOF) for [**TODO: TOE Name**]. The SOF analysis evaluates the strength of probabilistic or permutation-based security mechanisms against various types of attacks.

30.1.2 1.2 SOF Concept

Definition: The Strength of Function is a measure of the minimum strength that a TOE security mechanism provides against direct attacks. It is expressed as the probability that an attacker can overcome the mechanism in a given time with given resources.

SOF Levels: - **SOF-basic**: Protection against attackers with limited resources and capabilities - **SOF-medium**: Protection against attackers with moderate resources and capabilities - **SOF-high**: Protection against attackers with high resources and capabilities

30.1.3 1.3 Applicability

SOF applies to the following types of mechanisms: - Password-based authentication - Biometric authentication - Random number generators - Cryptographic key generation (for probabilistic methods) - Challenge-response mechanisms

SOF does NOT apply to: - Deterministic access control mechanisms - Cryptographic algorithms themselves (these are evaluated separately) - Audit mechanisms - Timestamp mechanisms

30.2 2. SOF-Claim

30.2.1 2.1 Claimed SOF Level

The TOE claims the following SOF level:

SOF-Claim: [TODO: SOF-basic / SOF-medium / SOF-high]

Rationale for SOF-Claim:

[TODO: Justify the choice of SOF level. Example:]

The TOE is deployed in an environment where the following threats exist: - [TODO: Describe relevant Threats from Chapter 2] - [TODO: Describe expected attacker capabilities] - [TODO: Describe security objectives]

Based on this analysis, SOF-[TODO] is appropriate because: - [TODO: Rationale 1] - [TODO: Rationale 2] - [TODO: Rationale 3]

30.3 3. Identification of Probabilistic Mechanisms

30.3.1 3.1 Overview

The following probabilistic or permutation-based mechanisms have been identified in the TOE:

Mechanism-ID	Mechanism-Name	TSF-ID	Type	SOF-relevant
M-1	[TODO]	TSF-[TODO]	[TODO: Password/Biometric/RNG/etc.]	Yes/No
M-2	[TODO]	TSF-[TODO]	[TODO]	Yes/No
M-3	[TODO]	TSF-[TODO]	[TODO]	Yes/No

30.3.2 3.2 Non-SOF-relevant Mechanisms

The following mechanisms are NOT SOF-relevant because they are deterministic:

Mechanism-ID	Mechanism-Name	TSF-ID	Rationale
[TODO]	[TODO]	TSF-[TODO]	[TODO: Why not SOF-relevant?]

30.4 4. SOF Analysis

30.4.1 4.1 Mechanism M-1: [TODO: Name]

Mechanism-ID: M-1
TSF-ID: TSF-[TODO]

Type: [TODO: e.g., Password Authentication]

30.4.1.1 4.1.1 Mechanism Description

[TODO: Describe the mechanism in detail. Example:]

The password authentication mechanism uses: - Password length: Minimum [TODO] characters, Maximum [TODO] characters - Character set: [TODO: e.g., Upper/lowercase letters, digits, special characters] - Password complexity rules: [TODO: Describe the rules] - Storage: [TODO: e.g., SHA-256 hash with salt] - Failed attempt handling: [TODO: e.g., Account lockout after X attempts]

30.4.1.2 4.1.2 Attack Scenarios

Possible Attack Types:

1. **Brute-Force Attack**
   - Description: Systematic trying of all possible passwords
   - Resources: [TODO: Describe required resources]
   - Time required: [TODO: Calculate time required]
2. **Dictionary Attack**
   - Description: Trying commonly used passwords
   - Resources: [TODO: Describe required resources]
   - Time required: [TODO: Calculate time required]
3. **Guessing Attack**
   - Description: Guessing passwords based on user information
   - Resources: [TODO: Describe required resources]
   - Success probability: [TODO: Estimate probability]

30.4.1.3 4.1.3 SOF Calculation

Assumptions: - [TODO: List all assumptions, e.g.:] - Users choose passwords randomly from the allowed character set - Attacker has no access to the password hash - Attacker can perform maximum [TODO] attempts per time unit

Calculation:

[TODO: Perform the SOF calculation. Example:]

Character Set Size: - Lowercase letters: 26 - Uppercase letters: 26 - Digits: 10 - Special characters: 10 - Total: 72 characters

Password Space: - Minimum password length: 8 characters - Number of possible passwords: 72^8 = 7.22 × 10^14

Brute-Force Attack: - Attempts per second: [TODO: e.g., 1000] - Time for complete enumeration: 7.22 × 10^14 / 1000 / 86400 / 365 = approx. 22.9 million years - Success probability after 1 year: 1 / 22,900,000 4.4 × 10^-8

Account Lockout: - Maximum failed attempts: [TODO: e.g., 5] - Success probability: 5 / 7.22 × 10^14 6.9 × 10^-15

Dictionary Attack: - Dictionary size: [TODO: e.g., 1 million common passwords] - Success probability (without lockout): 1,000,000 / 7.22 × 10^14 1.4 × 10^-9 - Success probability (with

lockout): 5 / 1,000,000 = 5 × 10^-6

30.4.1.4 4.1.4 SOF Evaluation

Determined SOF Level: [TODO: SOF-basic / SOF-medium / SOF-high]

Rationale:

[TODO: Justify the determined SOF level. Example:]

Based on the analysis: - Brute-force attacks are practically impossible (success probability < 10^-10) - Dictionary attacks are effectively prevented by account lockout (success probability < 10^-5) - The mechanism provides protection against attackers with [TODO: limited/moderate/high] resources

The determined SOF level is **SOF-[TODO]**.

Comparison with SOF-Claim: - SOF-Claim: SOF-[TODO] - Determined SOF: SOF-[TODO] - Fulfillment: Yes / No

30.4.2 4.2 Mechanism M-2: [TODO: Name]

Mechanism-ID: M-2
TSF-ID: TSF-[TODO]
Type: [TODO]

30.4.2.1 4.2.1 Mechanism Description

[TODO: Description analogous to 4.1.1]

30.4.2.2 4.2.2 Attack Scenarios

[TODO: Analysis analogous to 4.1.2]

30.4.2.3 4.2.3 SOF Calculation

[TODO: Calculation analogous to 4.1.3]

30.4.2.4 4.2.4 SOF Evaluation

[TODO: Evaluation analogous to 4.1.4]

30.4.3 4.3 Mechanism M-3: [TODO: Name]

[TODO: Analyze additional mechanisms following the same schema]

30.5 5. Summary of SOF Analysis

30.5.1 5.1 Overview of All Mechanisms

Mechanism-ID	Mechanism-Name	Determined SOF	SOF-Claim	Fulfillment
M-1	[TODO]	SOF-[TODO]	SOF-[TODO]	/
M-2	[TODO]	SOF-[TODO]	SOF-[TODO]	/

Mechanism-ID	Mechanism-Name	Determined SOF	SOF-Claim	Fulfillment
M-3	[TODO]	SOF-[TODO]	SOF-[TODO]	/

30.5.2 5.2 Fulfillment of SOF-Claim

SOF-Claim: SOF-[TODO]

Analysis:

[TODO: Analyze whether all mechanisms fulfill the SOF-Claim. Example:]

- Number of analyzed mechanisms: [TODO]
- Number of mechanisms fulfilling SOF-Claim: [TODO]
- Number of mechanisms not fulfilling SOF-Claim: [TODO]

Result:

[TODO: Choose one of the following options:]

All mechanisms fulfill the SOF-Claim - The SOF-Claim of SOF-[TODO] is met or exceeded by all analyzed mechanisms.

Not all mechanisms fulfill the SOF-Claim - The following mechanisms do not fulfill the SOF-Claim: [TODO: List] - Actions: [TODO: Describe planned actions]

30.5.3 5.3 Weakest Mechanism

Weakest Mechanism: [TODO: Mechanism-ID and Name]
SOF Level: SOF-[TODO]

Rationale: [TODO: Explain why this mechanism is the weakest and whether this is acceptable.]

30.5.4 5.4 Assumptions and Limitations

Assumptions: [TODO: List all assumptions made for the SOF analysis. Example:] - Users choose passwords randomly - Attacker has no physical access to the system - Attacker has no insider information - [TODO: Additional assumptions]

Limitations: [TODO: List all limitations of the analysis. Example:] - The analysis does not consider side-channel attacks - The analysis does not consider social engineering attacks - [TODO: Additional limitations]

30.6 6. Recommendations

30.6.1 6.1 Improvement Opportunities

[TODO: Provide recommendations for improving SOF. Example:]

1. **Increase Password Complexity**
   - Current minimum length: [TODO]
   - Recommended minimum length: [TODO]
   - Expected SOF improvement: [TODO]
2. **Multi-Factor Authentication**

- Implementation of a second factor (e.g., OTP, hardware token)
- Expected SOF improvement: [TODO]

3. **Adaptive Authentication**
   - Adjustment of security requirements based on risk assessment
   - Expected SOF improvement: [TODO]

30.6.2 6.2 Maintenance and Monitoring

[TODO: Describe measures to maintain SOF. Example:]

- Regular review of password policies
- Monitoring of authentication attempts
- Update of SOF analysis when TOE changes
- Consideration of new attack techniques

30.7 7. Summary

30.7.1 7.1 Result of SOF Analysis

The SOF analysis for **[TODO: TOE Name]** shows:

- All probabilistic mechanisms have been identified
- All mechanisms have been analyzed
- SOF calculations are documented
- SOF-Claim is fulfilled / SOF-Claim is not fulfilled

Overall Assessment: [TODO: Summary assessment]

30.7.2 7.2 Reference to Additional Documents

For further information see:

- **0500_TOE_Summary_Specification.md**: Detailed description of TSFs
- **0510_Assurance_Measures.md**: AVA_SOF.1 Assurance Measure
- **Chapter 4 of the Security Target**: Definition of SFRs

Document History:

Version	Date	Author	Changes
0.1	[TODO]	[TODO]	Initial version
1.0	[TODO]	[TODO]	[TODO]

ewpage

Chapter 31

Protection Profile Conformance

Document-ID: 0600
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and HTML comments with project-specific information.

31.1 Overview

This chapter documents the conformance of the Security Target (ST) with relevant Protection Profiles (PP) according to ISO/IEC 15408.

PP Conformance Claim: [TODO: Strict / Demonstrable / No Conformance]

31.2 Protection Profile Identification

31.2.1 PP 1: [TODO: PP Name]

- **PP Title:** [TODO: Full title of the Protection Profile]
- **PP Version:** [TODO: Version]
- **PP Date:** [TODO: Publication date]
- **PP Registration:** [TODO: Registration number if available]
- **PP Publisher:** [TODO: Organization]
- **Conformance Type:** [TODO: Strict / Demonstrable]

Description:

[TODO: Describe the Protection Profile and why it is relevant for this TOE]

31.2.2 PP 2: [TODO: PP Name] (if applicable)

- **PP Title:** [TODO: Full title]
- **PP Version:** [TODO: Version]
- **PP Date:** [TODO: Date]
- **PP Registration:** [TODO: Number]
- **PP Publisher:** [TODO: Organization]
- **Conformance Type:** [TODO: Strict / Demonstrable]

Description: [TODO: Description]

31.3 Conformance Claim

31.3.1 Strict Conformance

[TODO: Document that the ST adopts all PP requirements without modifications]

Conformance Statement: - All Security Functional Requirements (SFRs) from the PP are included in the ST - All Security Assurance Requirements (SARs) from the PP are included in the ST - All security objectives from the PP are included in the ST - No deviations from the PP

31.3.2 Demonstrable Conformance

[TODO: Document how the ST meets the PP requirements, even if adaptations were made]

Conformance Statement: - The ST meets the security objectives of the PP - The ST may contain additional requirements - The ST may refine or extend PP requirements - All deviations are documented and justified

31.3.3 No PP Conformance

[TODO: Justify why no PP conformance is claimed]

Justification: [TODO: Explain the reasons for the decision not to claim PP conformance]

31.4 Conformance Analysis

31.4.1 Conformance with [TODO: PP Name]

31.4.1.1 Security Functional Requirements (SFR)

PP SFR	ST SFR	Status	Comment
[TODO: PP-SFR-ID]	[TODO: ST-SFR-ID]	Identical / Extended / Refined	[TODO: Explanation]
[TODO]	[TODO]	[TODO]	[TODO]

Summary: [TODO: Summarize the SFR conformance]

31.4.1.2 Security Assurance Requirements (SAR)

PP SAR	ST SAR	Status	Comment
[TODO: PP-SAR-ID] [TODO]	[TODO: ST-SAR-ID] [TODO]	Identical / Extended [TODO]	[TODO: Explanation] [TODO]

Summary: [TODO: Summarize the SAR conformance]

31.4.1.3 Security Objectives

PP Security Objective	ST Security Objective	Status	Comment
[TODO: PP-Objective-ID] [TODO]	[TODO: ST-Objective-ID] [TODO]	Identical / Extended [TODO]	[TODO: Explanation] [TODO]

Summary: [TODO: Summarize the security objectives conformance]

31.5 Deviations from Protection Profile

31.5.1 Deviation 1: [TODO: Title]

- **Affected PP Section:** [TODO: Section/Requirement]
- **Type of Deviation:** [TODO: Addition / Refinement / Omission / Modification]
- **Description:** [TODO: Describe the deviation in detail]
- **Justification:** [TODO: Explain why this deviation is necessary]
- **Security Impact:** [TODO: Assess the security implications]
- **Reference to ST Section:** [TODO: Section number in ST]

31.5.2 Deviation 2: [TODO: Title] (if applicable)

- **Affected PP Section:** [TODO]
- **Type of Deviation:** [TODO]
- **Description:** [TODO]
- **Justification:** [TODO]
- **Security Impact:** [TODO]
- **Reference to ST Section:** [TODO]

31.6 Additional Requirements

31.6.1 Additional SFRs

ST SFR	Description	Justification
[TODO: SFR-ID] [TODO]	[TODO: Brief description] [TODO]	[TODO: Why was this SFR added?] [TODO]

31.6.2 Additional SARs

ST SAR	Description	Justification
[TODO: SAR-ID]	[TODO: Brief description]	[TODO: Why was this SAR added?]
[TODO]	[TODO]	[TODO]

31.6.3 Additional Security Objectives

ST Objective	Description	Justification
[TODO: Objective-ID]	[TODO: Brief description]	[TODO: Why was this objective added?]
[TODO]	[TODO]	[TODO]

31.7 Conformance Assessment

31.7.1 Conformance Status

Overall Assessment: [TODO: Conformant / Conformant with Deviations / Non-conformant]

Summary: [TODO: Summarize the conformance status and assess whether the ST meets the PP requirements]

31.7.2 Conformance Evidence

[TODO: Describe the methodology and evidence for PP conformance]

Evidence Documentation: - [TODO: Reference to relevant ST sections] - [TODO: Reference to mapping tables] - [TODO: Reference to rationale documents]

31.8 References

1. [TODO: PP Reference 1]
2. [TODO: PP Reference 2]
3. [TODO: Other relevant documents]

Next Steps: 1. Identify all relevant Protection Profiles 2. Document the conformance claim 3. Conduct detailed conformance analysis 4. Document all deviations and additional requirements 5. Create mapping tables between PP and ST 6. Have PP conformance reviewed by evaluators

ewpage

Chapter 32

Rationale for Security Objectives

Document-ID: 0610
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and HTML comments with project-specific information.

32.1 Overview

This chapter provides the rationale demonstrating that the defined security objectives completely and adequately address the identified security problems (threats, Organizational Security Policies, assumptions).

32.2 Rationale Methodology

32.2.1 Approach

[TODO: Describe the systematic approach to creating the rationale]

Steps: 1. Identification of all security problems (threats, OSPs, assumptions) 2. Mapping of security objectives to each security problem 3. Justification of completeness and adequacy 4. Review for gaps and redundancies

32.2.2 Completeness Criteria

[TODO: Define when the security objectives are considered complete]

Criteria: - Each threat is addressed by at least one TOE security objective - Each OSP is addressed by at least one TOE security objective - Each assumption is addressed by at least one environmental security objective - No security problems remain unaddressed

32.3 Rationale for Threats

32.3.1 Threat T.1: [TODO: Threat Name]

Threat Description: [TODO: Brief summary of the threat from section 0210]

Addressing Security Objectives:

32.3.1.1 Security Objective O.1: [TODO: Objective Name]

Justification: [TODO: Explain in detail how this security objective addresses the threat]

Adequacy: [TODO: Justify why this security objective is sufficient to mitigate the threat]

32.3.1.2 Security Objective O.2: [TODO: Objective Name] (if applicable)

Justification: [TODO: Explain the additional coverage by this objective]

Adequacy: [TODO: Justify the necessity of this additional objective]

Summary: [TODO: Summarize how the combination of security objectives completely addresses the threat]

32.3.2 Threat T.2: [TODO: Threat Name]

Threat Description: [TODO: Brief summary]

Addressing Security Objectives:

32.3.2.1 Security Objective O.X: [TODO: Objective Name]

Justification: [TODO: Detailed explanation]

Adequacy: [TODO: Justification of adequacy]

Summary: [TODO: Summary of coverage]

32.3.3 Additional Threats

[TODO: Document the rationale for all additional threats]

32.4 Rationale for Organizational Security Policies (OSPs)

32.4.1 OSP P.1: [TODO: OSP Name]

OSP Description: [TODO: Brief summary of the OSP from section 0220]

Addressing Security Objectives:

32.4.1.1 Security Objective O.X: [TODO: Objective Name]

Justification: [TODO: Explain how this security objective implements or supports the OSP]

Adequacy: [TODO: Justify why this security objective is sufficient to fulfill the OSP]

Summary: [TODO: Summarize the fulfillment of the OSP]

32.4.2 OSP P.2: [TODO: OSP Name]

OSP Description: [TODO: Brief summary]

Addressing Security Objectives:

32.4.2.1 Security Objective O.X: [TODO: Objective Name]

Justification: [TODO: Detailed explanation]

Adequacy: [TODO: Justification of adequacy]

Summary: [TODO: Summary of fulfillment]

32.4.3 Additional OSPs

[TODO: Document the rationale for all additional OSPs]

32.5 Rationale for Assumptions

32.5.1 Assumption A.1: [TODO: Assumption Name]

Assumption Description: [TODO: Brief summary of the assumption from section 0230]

Addressing Security Objectives:

32.5.1.1 Environmental Security Objective OE.X: [TODO: Objective Name]

Justification: [TODO: Explain how this environmental security objective supports or ensures the assumption]

Adequacy: [TODO: Justify why this objective is sufficient to justify the assumption]

Summary: [TODO: Summarize the support of the assumption]

32.5.2 Assumption A.2: [TODO: Assumption Name]

Assumption Description: [TODO: Brief summary]

Addressing Security Objectives:

32.5.2.1 Environmental Security Objective OE.X: [TODO: Objective Name]

Justification: [TODO: Detailed explanation]

Adequacy: [TODO: Justification of adequacy]

Summary: [TODO: Summary of support]

32.5.3 Additional Assumptions

[TODO: Document the rationale for all additional assumptions]

32.6 Completeness Analysis

32.6.1 Coverage Matrix: Security Problems to Security Objectives

Security Problem	Type	Addressing Security Objectives	Status
T.1: [TODO]	Threat	O.1, O.2	Complete
T.2: [TODO]	Threat	O.3	Complete
P.1: [TODO]	OSP	O.4, O.5	Complete
P.2: [TODO]	OSP	O.6	Complete
A.1: [TODO]	Assumption	OE.1	Complete
A.2: [TODO]	Assumption	OE.2, OE.3	Complete

Legend: - **Complete:** All aspects of the security problem are addressed - **Partial:** Some aspects are addressed, additional objectives required - **Incomplete:** Security problem is not sufficiently addressed

32.6.2 Identified Gaps

[TODO: List all security problems that are not completely addressed by security objectives]

Gap 1: [TODO: Description] - **Affected Security Problem:** [TODO] - **Missing Coverage:** [TODO] - **Planned Action:** [TODO: Additional objective or justification why no action is required]

32.6.3 Redundancy Analysis

[TODO: Analyze whether security objectives are redundant or overlap]

Redundancy 1: [TODO: Description] - **Affected Objectives:** [TODO: O.X, O.Y] - **Overlap:** [TODO: Describe the overlap] - **Justification:** [TODO: Explain why both objectives are necessary, or suggest consolidation]

32.7 Adequacy Analysis

32.7.1 Assessment Criteria

[TODO: Define the criteria for adequacy of security objectives]

Criteria: - Security objectives address the root cause of threats - Security objectives are realistically implementable - Security objectives are measurable and verifiable - Security objectives are proportional to the risk

32.7.2 Adequacy Assessment

Security Objective	Addressed Problems	Adequacy	Justification
O.1: [TODO]	T.1, T.2	Adequate	[TODO: Justification]
O.2: [TODO]	T.1, P.1	Adequate	[TODO: Justification]
O.3: [TODO]	T.3	To Review	[TODO: Justification]

Legend: - **Adequate:** Objective is sufficient to address the problem - **To Review:** Further analysis required - **Insufficient:** Objective must be strengthened or supplemented

32.8 Rationale Summary

32.8.1 Completeness

[TODO: Confirm that all security problems are addressed by security objectives]

Status: [TODO: Complete / Incomplete]

Justification: [TODO: Explain the completeness status]

32.8.2 Adequacy

[TODO: Confirm that the security objectives are adequate]

Status: [TODO: Adequate / Needs Improvement]

Justification: [TODO: Explain the adequacy status]

32.8.3 Consistency

[TODO: Confirm that the security objectives are consistent and non-contradictory]

Status: [TODO: Consistent / Inconsistencies Present]

Justification: [TODO: Explain the consistency status]

32.9 References

- **Section 0200:** Security Problem Definition
- **Section 0210:** Threats
- **Section 0220:** Organizational Security Policies
- **Section 0230:** Assumptions
- **Section 0300:** Security Objectives
- **Section 0320:** Security Objectives Coverage Matrix

Next Steps: 1. Document the rationale for each threat 2. Document the rationale for each OSP 3. Document the rationale for each assumption 4. Create the coverage matrix 5. Conduct completeness and adequacy analyses 6. Identify and address gaps 7. Have the rationale reviewed by evaluators

ewpage

Chapter 33

Rationale for Security Requirements

Document-ID: 0620
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and HTML comments with project-specific information.

33.1 Overview

This chapter provides the rationale demonstrating that the defined security requirements (Security Functional Requirements - SFRs and Security Assurance Requirements - SARs) completely and adequately fulfill the security objectives.

33.2 Rationale Methodology

33.2.1 Approach

[TODO: Describe the systematic approach to creating the rationale]

Steps: 1. Mapping of SFRs to TOE security objectives 2. Justification of completeness and adequacy 3. Justification of all SFR operations 4. Verification of SFR dependencies 5. Justification of SAR selection

33.2.2 Completeness Criteria

[TODO: Define when the security requirements are considered complete]

Criteria: - Each TOE security objective is fulfilled by at least one SFR - All SFR dependencies are satisfied - All SFR operations are justified - SARs correspond to the chosen EAL

33.3 Rationale for Security Functional Requirements (SFRs)

33.3.1 Mapping: Security Objectives to SFRs

33.3.1.1 Security Objective O.1: [TODO: Objective Name]

Objective Description: [TODO: Brief summary of the security objective from section 0300]

Fulfilling SFRs:

33.3.1.1.1 SFR 1: [TODO: SFR-Identifier] - [TODO: SFR-Name] SFR Description: [TODO: Brief description of the SFR from section 0400]

Justification: [TODO: Explain in detail how this SFR fulfills the security objective]

Adequacy: [TODO: Justify why this SFR is sufficient to achieve the objective]

Operations:

- **Selection:** [TODO: Describe selected options and justification]
- **Assignment:** [TODO: Describe assigned values and justification]
- **Refinement:** [TODO: Describe refinements and justification]
- **Iteration:** [TODO: Describe iterations and justification]

33.3.1.1.2 SFR 2: [TODO: SFR-Identifier] - [TODO: SFR-Name] (if applicable) SFR Description: [TODO: Brief description]

Justification: [TODO: Detailed explanation]

Adequacy: [TODO: Justification of adequacy]

Operations: [TODO: Document all operations]

Summary for O.1: [TODO: Summarize how the combination of SFRs completely fulfills the security objective]

33.3.1.2 Security Objective O.2: [TODO: Objective Name]

Objective Description: [TODO: Brief summary]

Fulfilling SFRs:

33.3.1.2.1 SFR X: [TODO: SFR-Identifier] - [TODO: SFR-Name] SFR Description: [TODO: Brief description]

Justification: [TODO: Detailed explanation]

Adequacy: [TODO: Justification of adequacy]

Operations: [TODO: Document all operations]

Summary for O.2: [TODO: Summary of fulfillment]

33.3.2 Additional Security Objectives

[TODO: Document the rationale for all additional security objectives]

33.4 SFR Operations Rationale

33.4.1 Selection

SFR	Selection Options	Chosen Option	Justification
[TODO: SFR-ID]	[TODO: Option A, B, C]	[TODO: Option B]	[TODO: Why was this option chosen?]
[TODO]	[TODO]	[TODO]	[TODO]

33.4.2 Assignment

SFR	Parameter	Assigned Value	Justification
[TODO: SFR-ID]	[TODO: Parameter]	[TODO: Value]	[TODO: Why was this value assigned?]
[TODO]	[TODO]	[TODO]	[TODO]

33.4.3 Refinement

SFR	Original Text	Refined Text	Justification
[TODO: SFR-ID]	[TODO: Original]	[TODO: Refined]	[TODO: Why was it refined?]
[TODO]	[TODO]	[TODO]	[TODO]

33.4.4 Iteration

SFR	Iteration	Purpose	Justification
[TODO: SFR-ID]	[TODO: Iteration 1]	[TODO: Purpose]	[TODO: Why was it iterated?]
[TODO]	[TODO]	[TODO]	[TODO]

33.5 SFR Dependencies Rationale

33.5.1 Dependency Analysis

SFR	Dependent SFR	Status	Justification
[TODO: SFR-ID]	[TODO: Dependent SFR]	Satisfied / Not Satisfied	[TODO: Explanation]
[TODO]	[TODO]	[TODO]	[TODO]

Legend: - **Satisfied:** The dependent SFR is included in the ST - **Not Satisfied:** The dependent SFR is missing (justification required)

33.5.2 Unsatisfied Dependencies

33.5.2.1 Dependency 1: [TODO: SFR-ID] → [TODO: Dependent SFR]

Description: [TODO: Describe the dependency]

Reason for Non-Satisfaction: [TODO: Explain why the dependency is not satisfied]

Compensating Measures: [TODO: Describe alternative measures or justify why no compensation is required]

Security Impact: [TODO: Assess the impact on security]

33.6 Rationale for Security Assurance Requirements (SARs)

33.6.1 EAL Selection Rationale

Chosen EAL: [TODO: EAL1 / EAL2 / EAL3 / EAL4 / EAL5 / EAL6 / EAL7]

Justification: [TODO: Explain why this EAL was chosen]

Factors: - **Threat Environment:** [TODO: Describe the threat environment] - **Protection Needs:** [TODO: Describe the protection needs] - **Cost-Benefit Ratio:** [TODO: Assess the ratio] - **Market Requirements:** [TODO: Describe market requirements]

33.6.2 SAR Components Rationale

33.6.2.1 SAR Family: [TODO: Family Name]

SAR Component	EAL Standard	Augmented	Justification
[TODO: SAR-ID]	Yes / No	Yes / No	[TODO: Explanation]
[TODO]	[TODO]	[TODO]	[TODO]

Summary: [TODO: Summarize the SAR selection for this family]

33.6.3 Augmented SARs

SAR	Standard EAL	Chosen Level	Justification
[TODO: SAR-ID]	[TODO: EAL]	[TODO: Higher Level]	[TODO: Why was it augmented?]
[TODO]	[TODO]	[TODO]	[TODO]

33.6.4 Reduced SARs

SAR	Standard EAL	Chosen Level	Justification
[TODO: SAR-ID]	[TODO: EAL]	[TODO: Lower Level]	[TODO: Why was it reduced?]
[TODO]	[TODO]	[TODO]	[TODO]

33.7 Completeness Analysis

33.7.1 Coverage Matrix: Security Objectives to SFRs

Security Objective	Fulfilling SFRs	Status
O.1: [TODO]	[TODO: SFR-IDs]	Complete
O.2: [TODO]	[TODO: SFR-IDs]	Complete
O.3: [TODO]	[TODO: SFR-IDs]	Complete

Legend: - **Complete:** All aspects of the objective are fulfilled by SFRs - **Partial:** Some aspects are fulfilled, additional SFRs required - **Incomplete:** Objective is not sufficiently fulfilled by SFRs

33.7.2 Identified Gaps

[TODO: List all security objectives that are not completely fulfilled by SFRs]

Gap 1: [TODO: Description] - **Affected Security Objective:** [TODO] - **Missing Coverage:** [TODO] - **Planned Action:** [TODO: Additional SFR or justification why no action is required]

33.7.3 Redundancy Analysis

[TODO: Analyze whether SFRs are redundant or overlap]

Redundancy 1: [TODO: Description] - **Affected SFRs:** [TODO: SFR-IDs] - **Overlap:** [TODO: Describe the overlap] - **Justification:** [TODO: Explain why both SFRs are necessary, or suggest consolidation]

33.8 Adequacy Analysis

33.8.1 Assessment Criteria

[TODO: Define the criteria for adequacy of security requirements]

Criteria: - SFRs are technically implementable - SFRs are measurable and testable - SFRs are proportional to the risk - SARs are appropriate for the assurance level

33.8.2 Adequacy Assessment

SFR	Fulfilled Objectives	Adequacy	Justification
[TODO: SFR-ID]	[TODO: Objectives]	Adequate	[TODO: Justification]
[TODO]	[TODO]	[TODO]	[TODO]

Legend: - **Adequate:** SFR is sufficient to fulfill the objectives - **To Review:** Further analysis required - **Insufficient:** SFR must be strengthened or supplemented

33.9 Consistency Analysis

33.9.1 Internal Consistency

[TODO: Verify that the SFRs are internally consistent]

Identified Inconsistencies: [TODO: List all inconsistencies]

Inconsistency 1: [TODO: Description] - **Affected SFRs:** [TODO: SFR-IDs] - **Conflict:** [TODO: Describe the conflict] - **Resolution:** [TODO: Describe the resolution]

33.9.2 Consistency with Security Objectives

[TODO: Verify that the SFRs are consistent with the security objectives]

Identified Inconsistencies: [TODO: List all inconsistencies]

33.10 Rationale Summary

33.10.1 Completeness

[TODO: Confirm that all security objectives are fulfilled by SFRs]

Status: [TODO: Complete / Incomplete]

Justification: [TODO: Explain the completeness status]

33.10.2 Adequacy

[TODO: Confirm that the security requirements are adequate]

Status: [TODO: Adequate / Needs Improvement]

Justification: [TODO: Explain the adequacy status]

33.10.3 Consistency

[TODO: Confirm that the security requirements are consistent]

Status: [TODO: Consistent / Inconsistencies Present]

Justification: [TODO: Explain the consistency status]

33.11 References

- **Section 0300:** Security Objectives
- **Section 0400:** Security Requirements
- **Section 0410:** Evaluation Assurance Level
- **Section 0430:** SFR Dependencies
- **Section 0440:** Coverage Matrix

Next Steps: 1. Document the rationale for each security objective 2. Justify all SFR operations 3. Verify all SFR dependencies 4. Justify the SAR selection 5. Create the coverage matrix 6. Conduct completeness, adequacy, and consistency analyses 7. Identify and address gaps and inconsistencies 8. Have the rationale reviewed by evaluators

ewpage

Chapter 34

Glossary and Term Definitions

Document-ID: 0630
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and HTML comments with project-specific information.

34.1 Overview

This glossary defines all important terms, abbreviations, and acronyms used in the Security Target. It serves as a central reference for terminology and ensures that all terms are used consistently.

34.2 Common Criteria Standard Terms

34.2.1 A

Asset [TODO: Definition or reference to ISO/IEC 15408-1] An asset is an entity that has value to the owner or user and therefore must be protected.

Assumption [TODO: Definition or reference to ISO/IEC 15408-1] An assumption is a statement about the security aspects of the TOE environment that is assumed to be true.

Attack Potential [TODO: Definition or reference to ISO/IEC 18045] Attack potential is a measure of an attacker's ability to conduct a successful attack.

Augmentation [TODO: Definition or reference to ISO/IEC 15408-1] Augmentation is the addition of requirements to an EAL that exceed the standard requirements.

34.2.2 C

Common Criteria (CC) [TODO: Definition] ISO/IEC 15408 - International standard for evaluating the security of IT products and systems.

34.2.3 E

Evaluation Assurance Level (EAL) [TODO: Definition or reference to ISO/IEC 15408-3] An EAL is a package of security assurance requirements (SARs) that represents a specific level of confidence in the security of the TOE.

Evaluation Authority [TODO: Definition] An organization responsible for overseeing and certifying Common Criteria evaluations.

34.2.4 O

Organizational Security Policy (OSP) [TODO: Definition or reference to ISO/IEC 15408-1] An OSP is a security policy imposed by an organization that must be enforced by the TOE.

34.2.5 P

Protection Profile (PP) [TODO: Definition or reference to ISO/IEC 15408-1] A PP is an implementation-independent set of security requirements for a category of TOEs.

34.2.6 S

Security Assurance Requirement (SAR) [TODO: Definition or reference to ISO/IEC 15408-3] A SAR is a requirement that ensures confidence in the correct implementation of security functions.

Security Functional Requirement (SFR) [TODO: Definition or reference to ISO/IEC 15408-2] An SFR is a requirement that describes a security function that the TOE must provide.

Security Objective [TODO: Definition or reference to ISO/IEC 15408-1] A security objective is a statement of the intended response to identified threats and/or OSPs.

Security Target (ST) [TODO: Definition or reference to ISO/IEC 15408-1] An ST is an implementation-specific set of security requirements and specifications for a concrete TOE.

Strength of Function (SOF) [TODO: Definition or reference to ISO/IEC 15408-1] SOF is a measure of the effectiveness of a security function against direct attacks.

34.2.7 T

Target of Evaluation (TOE) [TODO: Definition or reference to ISO/IEC 15408-1] The TOE is the IT product or system being evaluated.

Threat [TODO: Definition or reference to ISO/IEC 15408-1] A threat is a potential violation of security by an attacker.

Threat Agent [TODO: Definition or reference to ISO/IEC 15408-1] A threat agent is an entity that can execute a threat.

TSF (TOE Security Functionality) [TODO: Definition or reference to ISO/IEC 15408-1] The TSF is the totality of all hardware, software, and firmware components of the TOE responsible for enforcing the security policy.

TSP (TOE Security Policy) [TODO: Definition or reference to ISO/IEC 15408-1] The TSP is the set of rules that govern the security of the TOE.

34.3 TOE-Specific Terms

34.3.1 [TODO: Term 1]

Definition: [TODO: Define the term in the context of the TOE]

Usage in ST: [TODO: Describe how the term is used in the ST]

Related Terms: [TODO: List related terms]

34.3.2 [TODO: Term 2]

Definition: [TODO: Definition]

Usage in ST: [TODO: Usage]

Related Terms: [TODO: Related terms]

34.4 Technical Terms

34.4.1 [TODO: Technical Term 1]

Definition: [TODO: Define the technical term]

Context: [TODO: Explain the context in which the term is used]

Example: [TODO: Provide an example of usage]

34.4.2 [TODO: Technical Term 2]

Definition: [TODO: Definition]

Context: [TODO: Context]

Example: [TODO: Example]

34.5 Abbreviations and Acronyms

Abbreviation	Meaning	Explanation
CC	Common Criteria	ISO/IEC 15408
EAL	Evaluation Assurance Level	Evaluation assurance level
IT	Information Technology	Information technology

Abbreviation	Meaning	Explanation
OSP	Organizational Security Policy	Organizational security policy
PP	Protection Profile	Protection profile
SAR	Security Assurance Requirement	Security assurance requirement
SFR	Security Functional Requirement	Security functional requirement
SOF	Strength of Function	Strength of function
ST	Security Target	Security target
TOE	Target of Evaluation	Target of evaluation
TSF	TOE Security Functionality	TOE security functionality
TSP	TOE Security Policy	TOE security policy
[TODO]	[TODO]	[TODO]

34.6 Domain-Specific Terms

34.6.1 [TODO: Domain Term 1]

Definition: [TODO: Define the domain-specific term]

Relevance to TOE: [TODO: Explain the relevance to the TOE]

Standards Reference: [TODO: Reference relevant standards or specifications]

34.6.2 [TODO: Domain Term 2]

Definition: [TODO: Definition]

Relevance to TOE: [TODO: Relevance]

Standards Reference: [TODO: Reference]

34.7 Security Terms

34.7.1 [TODO: Security Term 1]

Definition: [TODO: Define the security term]

Threat Context: [TODO: Explain the context in relation to threats]

Protection Measures: [TODO: Describe relevant protection measures]

34.7.2 [TODO: Security Term 2]

Definition: [TODO: Definition]

Threat Context: [TODO: Context]

Protection Measures: [TODO: Measures]

34.8 Operations on SFRs

34.8.1 Assignment

Definition: Assigning a specific value to a parameter in an SFR.

Notation: [assignment: value]

Example: [assignment: 8 characters] for minimum password length

34.8.2 Iteration

Definition: Using an SFR multiple times with different operations or for different purposes.

Notation: SFR-ID/Iteration (e.g., FDP_ACC.1/User, FDP_ACC.1/Admin)

Example: Separate access control policies for users and administrators

34.8.3 Refinement

Definition: Adding details to an SFR to make it more precise or restrictive.

Notation: Italic text or [refinement: text]

Example: Refinement of "user" to "authenticated user with role X"

34.8.4 Selection

Definition: Selecting one or more options from a predefined list in an SFR.

Notation: [selection: Option A, Option B, Option C]

Example: [selection: symmetric encryption, asymmetric encryption]

34.9 Evaluation Terms

34.9.1 [TODO: Evaluation Term 1]

Definition: [TODO: Define the evaluation term]

Evaluation Context: [TODO: Explain the context in evaluation]

Reference: [TODO: Reference ISO/IEC 18045 or other relevant documents]

34.9.2 [TODO: Evaluation Term 2]

Definition: [TODO: Definition]

Evaluation Context: [TODO: Context]

Reference: [TODO: Reference]

34.10 References and Standards

34.10.1 ISO/IEC Standards

- **ISO/IEC 15408-1:** Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model
- **ISO/IEC 15408-2:** Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components
- **ISO/IEC 15408-3:** Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components
- **ISO/IEC 18045:** Information technology — Security techniques — Methodology for IT security evaluation

34.10.2 Additional Standards

[TODO: List additional relevant standards]

- [TODO: Standard 1]
- [TODO: Standard 2]

34.11 Terminology Consistency

34.11.1 Preferred Terms

Preferred Term	Avoid	Justification
TOE	Product, System	Official CC terminology
User	End-user, Operator	Consistency with English ST version
[TODO]	[TODO]	[TODO]

34.11.2 Capitalization

[TODO: Document conventions for capitalization of terms]

Examples: - TOE (always uppercase) - Security Target (capitalized as proper noun) - [TODO: Additional examples]

34.12 Change History

Version	Date	Change	Author
[TODO: 1.0]	[TODO: Date]	Initial version	[TODO: Name]
[TODO]	[TODO]	[TODO]	[TODO]

Next Steps: 1. Identify all terms used in the ST 2. Define all TOE-specific terms 3. Define all technical and domain-specific terms 4. Create the abbreviations list 5. Verify terminology consistency throughout the ST 6. Update the glossary when changes are made to the ST 7. Have the glossary reviewed by subject matter experts

ewpage

Chapter 35

References and Citations

Document-ID: 0640
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and HTML comments with project-specific information.

35.1 Overview

This chapter contains all references and citations that are cited or used in the Security Target. The references are organized by categories to facilitate navigation.

35.2 Common Criteria Standards

35.2.1 ISO/IEC 15408 (Common Criteria)

[**CC1**] ISO/IEC 15408-1:2022
Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model
International Organization for Standardization, 2022

[**CC2**] ISO/IEC 15408-2:2022
Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components
International Organization for Standardization, 2022

[**CC3**] ISO/IEC 15408-3:2022
Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components
International Organization for Standardization, 2022

35.2.2 Common Methodology for IT Security Evaluation

[CEM] ISO/IEC 18045:2022
Information technology — Security techniques — Methodology for IT security evaluation
International Organization for Standardization, 2022

35.2.3 Common Criteria Portal

[CCPORTAL] Common Criteria Portal
https://www.commoncriteriaportal.org/
[TODO: Access date]

35.3 Protection Profiles

35.3.1 [TODO: PP 1 Name]

[PP1] [TODO: PP Title]
Version [TODO: Version], [TODO: Date]
[TODO: Publisher/Organization]
[TODO: Registration number if available]
[TODO: URL or source]

Relevance: [TODO: Describe the relevance of this PP to the TOE]

35.3.2 [TODO: PP 2 Name] (if applicable)

[PP2] [TODO: PP Title]
Version [TODO: Version], [TODO: Date]
[TODO: Publisher/Organization]
[TODO: Registration number]
[TODO: URL]

Relevance: [TODO: Relevance]

35.4 Technical Standards and Specifications

35.4.1 Cryptography Standards

[FIPS140] FIPS PUB 140-3
Security Requirements for Cryptographic Modules
National Institute of Standards and Technology, 2019
https://csrc.nist.gov/publications/detail/fips/140/3/final

[NIST-SP800-57] NIST Special Publication 800-57 Part 1 Rev. 5
Recommendation for Key Management: Part 1 – General
National Institute of Standards and Technology, 2020
https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

[TODO: Additional Crypto Standards] [TODO: Add additional relevant cryptography standards]

35.4.2 Network and Communication Standards

[**TODO: Standard 1**] [TODO: Complete reference]

[**TODO: Standard 2**] [TODO: Complete reference]

35.4.3 Hardware and Platform Standards

[**TODO: Standard 1**] [TODO: Complete reference]

[**TODO: Standard 2**] [TODO: Complete reference]

35.4.4 Software Standards

[**TODO: Standard 1**] [TODO: Complete reference]

[**TODO: Standard 2**] [TODO: Complete reference]

35.5 Security Standards and Best Practices

35.5.1 ISO/IEC Security Standards

[**ISO27001**] ISO/IEC 27001:2022
Information security, cybersecurity and privacy protection — Information security management systems — Requirements
International Organization for Standardization, 2022

[**ISO27002**] ISO/IEC 27002:2022
Information security, cybersecurity and privacy protection — Information security controls
International Organization for Standardization, 2022

[**TODO: Additional ISO Standards**] [TODO: Add additional relevant ISO standards]

35.5.2 NIST Standards

[**NIST-CSF**] NIST Cybersecurity Framework Version 1.1
Framework for Improving Critical Infrastructure Cybersecurity
National Institute of Standards and Technology, 2018
https://www.nist.gov/cyberframework

[**NIST-SP800-53**] NIST Special Publication 800-53 Rev. 5
Security and Privacy Controls for Information Systems and Organizations
National Institute of Standards and Technology, 2020
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[**TODO: Additional NIST Standards**] [TODO: Add additional relevant NIST standards]

35.5.3 Industry-Specific Standards

[**TODO: Standard 1**] [TODO: Complete reference for industry-specific standards]

[**TODO: Standard 2**] [TODO: Complete reference]

35.6 Product Documentation

35.6.1 TOE Documentation

[TOE-SPEC] [TODO: TOE Specification Title]
Version [TODO: Version], [TODO: Date]
[TODO: Manufacturer]
[TODO: Document number]

[TOE-ARCH] [TODO: TOE Architecture Document]
Version [TODO: Version], [TODO: Date]
[TODO: Manufacturer]
[TODO: Document number]

[TOE-USER] [TODO: User Manual]
Version [TODO: Version], [TODO: Date]
[TODO: Manufacturer]
[TODO: Document number]

[TOE-ADMIN] [TODO: Administrator Manual]
Version [TODO: Version], [TODO: Date]
[TODO: Manufacturer]
[TODO: Document number]

35.6.2 Development Documentation

[DEV-DESIGN] [TODO: Design Document]
Version [TODO: Version], [TODO: Date]
[TODO: Internal document]

[DEV-TEST] [TODO: Test Documentation]
Version [TODO: Version], [TODO: Date]
[TODO: Internal document]

35.7 Evaluation Documentation

35.7.1 Evaluation Reports

[EVAL-PLAN] [TODO: Evaluation Plan]
Version [TODO: Version], [TODO: Date]
[TODO: Evaluation laboratory]

[EVAL-REPORT] [TODO: Evaluation Report] (if already available)
Version [TODO: Version], [TODO: Date]
[TODO: Evaluation laboratory]

35.7.2 Certification Documents

[CERT-SCHEME] [TODO: Certification Scheme]
Version [TODO: Version], [TODO: Date]
[TODO: Certification body]
[TODO: URL]

35.8 Regulatory Requirements

35.8.1 Laws and Regulations

[TODO: Law/Regulation 1] [TODO: Complete reference]

[TODO: Law/Regulation 2] [TODO: Complete reference]

35.8.2 Guidelines and Directives

[TODO: Guideline 1] [TODO: Complete reference]

[TODO: Guideline 2] [TODO: Complete reference]

35.9 Scientific Literature

35.9.1 Books

[TODO: Book 1] [TODO: Author(s)], *[TODO: Title]*, [TODO: Publisher], [TODO: Year], ISBN [TODO: ISBN]

[TODO: Book 2] [TODO: Complete reference]

35.9.2 Articles and Papers

[TODO: Article 1] [TODO: Author(s)], "[TODO: Title]", *[TODO: Journal/Conference]*, [TODO: Year], [TODO: Pages], DOI: [TODO: DOI]

[TODO: Article 2] [TODO: Complete reference]

35.10 Online Resources

35.10.1 Official Websites

[TODO: Website 1] [TODO: Title/Organization]
[TODO: URL]
Accessed: [TODO: Date]

[TODO: Website 2] [TODO: Complete reference]

35.10.2 Technical Documentation

[TODO: Online Doc 1] [TODO: Title]
[TODO: URL]
Accessed: [TODO: Date]

[TODO: Online Doc 2] [TODO: Complete reference]

35.11 Internal Documents

35.11.1 Security Policies

[INT-POL1] [TODO: Internal Security Policy]
Version [TODO: Version], [TODO: Date]
[TODO: Organization]
[TODO: Classification]

35.11.2 Process Documentation

[INT-PROC1] [TODO: Internal Process]
Version [TODO: Version], [TODO: Date]
[TODO: Organization]
[TODO: Classification]

35.12 Reference Index

Abbreviation	Title	Category	Section
[CC1]	ISO/IEC 15408-1:2022	CC Standard	Common Criteria Standards
[CC2]	ISO/IEC 15408-2:2022	CC Standard	Common Criteria Standards
[CC3]	ISO/IEC 15408-3:2022	CC Standard	Common Criteria Standards
[CEM]	ISO/IEC 18045:2022	CC Standard	Common Criteria Standards
[TODO]	[TODO]	[TODO]	[TODO]

35.13 Usage in Security Target

35.13.1 Frequently Cited References

Reference	Usage in ST	Sections
[CC2]	SFR definitions	0400, 0420
[CC3]	SAR definitions	0400, 0410
[PP1]	PP conformance	0600
[TODO]	[TODO]	[TODO]

35.14 Updates and Versioning

35.14.1 Change History

Version	Date	Change	Affected References
[TODO: 1.0]	[TODO: Date]	Initial version	All
[TODO]	[TODO]	[TODO]	[TODO]

35.14.2 Obsolete References

Old Reference	New Reference	Date of Change	Reason
[TODO]	[TODO]	[TODO]	[TODO: New version available]

35.15 Availability of References

35.15.1 Publicly Available Documents

[TODO: List which references are publicly available and where they can be obtained]

35.15.2 Restricted Availability Documents

[TODO: List which references have restricted availability and how they can be requested]

35.15.3 Proprietary Documents

[TODO: List which references are proprietary and under what conditions they are available]

35.16 Contact Information

35.16.1 Evaluation Laboratory

Name: [TODO: Name of evaluation laboratory]
Address: [TODO: Address]
Phone: [TODO: Phone]
Email: [TODO: Email]
Website: [TODO: Website]

35.16.2 Certification Body

Name: [TODO: Name of certification body]
Address: [TODO: Address]
Phone: [TODO: Phone]
Email: [TODO: Email]
Website: [TODO: Website]

35.16.3 TOE Manufacturer

Name: [TODO: Name of manufacturer]
Address: [TODO: Address]
Phone: [TODO: Phone]
Email: [TODO: Email]
Website: [TODO: Website]

Next Steps: 1. Identify all references used in the ST 2. Collect complete bibliographic information 3. Organize references by categories 4. Create the reference index 5. Document usage in the ST 6. Verify currency of all references 7. Ensure all references are available 8. Update the reference list when changes are made to the ST

ewpage

Chapter 36

Evidence and Documentation

Document-ID: 0650
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft / In Review / Approved
Classification: Internal / Confidential / Strictly Confidential
Last Update: {{ meta.date }}

> **Note:** This document is a template. Replace all `[TODO]` placeholders and HTML comments with project-specific information.

36.1 Overview

This chapter documents all evidence and documentation required for the Common Criteria evaluation of the TOE. The evidence is organized by SAR families and corresponds to the chosen Evaluation Assurance Level (EAL).

Chosen EAL: [TODO: EAL1 / EAL2 / EAL3 / EAL4 / EAL5 / EAL6 / EAL7]

36.2 Evidence Overview

36.2.1 Evidence Matrix

SAR Family	SAR Component	Required Evidence	Status	Availability
ADV	ADV_ARC.1	Security Architecture Description	[TODO: Status]	[TODO: Available/In Progress]
ADV	ADV_FSP.1	Functional Specification	[TODO: Status]	[TODO]
AGD	AGD_OPE.1	Operational User Guidance	[TODO: Status]	[TODO]
AGD	AGD_PRE.1	Preparative Procedures	[TODO: Status]	[TODO]

SAR Family	SAR Component	Required Evidence	Status	Availability
ALC	ALC_CMC.1	CM Capabilities	[TODO: Status]	[TODO]
ALC	ALC_CMS.1	CM Scope	[TODO: Status]	[TODO]
ATE	ATE_IND.1	Independent Testing	[TODO: Status]	[TODO]
AVA	AVA_VAN.1	Vulnerability Analysis	[TODO: Status]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Status Legend: - **Complete:** Evidence is complete and ready for evaluation - **In Progress:** Evidence is being created - **Planned:** Creation is planned - **Not Required:** Not required for chosen EAL

36.3 ADV: Development

36.3.1 ADV_ARC: Security Architecture

36.3.1.1 ADV_ARC.1: Security Architecture Description

Required Evidence: [TODO: Describe the required evidence according to ISO/IEC 15408-3]

Documentation: - **Document Title:** [TODO: Title of architecture document] - **Document Number:** [TODO: Number] - **Version:** [TODO: Version] - **Date:** [TODO: Date] - **Location:** [TODO: Path or reference] - **Classification:** [TODO: Classification]

Content: - Description of TOE security architecture - Identification of TSF subsystems - Description of security domains - Evidence of non-bypassability - Evidence of domain separation

Status: [TODO: Complete / In Progress / Planned]

Evaluation Notes: [TODO: Special notes for evaluators]

36.3.2 ADV_FSP: Functional Specification

36.3.2.1 ADV_FSP.1: Basic Functional Specification

Required Evidence: [TODO: Describe the required evidence]

Documentation: - **Document Title:** [TODO: Title of functional specification] - **Document Number:** [TODO: Number] - **Version:** [TODO: Version] - **Date:** [TODO: Date] - **Location:** [TODO: Path] - **Classification:** [TODO: Classification]

Content: - Description of all external TSF interfaces - Description of purposes and use of each interface - Description of parameters for each interface - Description of actions for each interface - Mapping of SFRs to TSF interfaces

Status: [TODO: Complete / In Progress / Planned]

Evaluation Notes: [TODO: Special notes]

36.3.3 Additional ADV Components

[TODO: Add additional ADV components if required (e.g., ADV_FSP.2, ADV_IMP.1, ADV_TDS.1)]

36.4 AGD: Guidance Documents

36.4.1 AGD_OPE: Operational User Guidance

36.4.1.1 AGD_OPE.1: Operational User Guidance

Required Evidence: [TODO: Describe the required evidence]

Documentation: - **Document Title:** [TODO: User Manual] - **Document Number:** [TODO: Number] - **Version:** [TODO: Version] - **Date:** [TODO: Date] - **Location:** [TODO: Path] - **Classification:** [TODO: Public / Confidential]

Content: - Description of security functions - Guidance for secure use - Warnings about insecure states - Description of user roles - Guidance for managing security attributes

Status: [TODO: Complete / In Progress / Planned]

Target Audience: [TODO: End users / Administrators / Both]

36.4.2 AGD_PRE: Preparative Procedures

36.4.2.1 AGD_PRE.1: Preparative Procedures

Required Evidence: [TODO: Describe the required evidence]

Documentation: - **Document Title:** [TODO: Installation and Configuration Manual] - **Document Number:** [TODO: Number] - **Version:** [TODO: Version] - **Date:** [TODO: Date] - **Location:** [TODO: Path] - **Classification:** [TODO: Classification]

Content: - Description of secure installation - Description of secure configuration - Description of security parameters - Guidance for verifying secure configuration

Status: [TODO: Complete / In Progress / Planned]

Target Audience: [TODO: Administrators / Installers]

36.5 ALC: Life-cycle Support

36.5.1 ALC_CMC: CM Capabilities

36.5.1.1 ALC_CMC.1: Labelling of the TOE

Required Evidence: [TODO: Describe the required evidence]

Documentation: - **Document Title:** [TODO: Configuration Management Plan] - **Document Number:** [TODO: Number] - **Version:** [TODO: Version] - **Date:** [TODO: Date] - **Location:** [TODO: Path] - **Classification:** [TODO: Classification]

Content: - Description of CM system - Unique identification of TOE - Description of version control - Description of change control

Status: [TODO: Complete / In Progress / Planned]

TOE Identification: - **TOE Name:** [TODO: Name] - **TOE Version:** [TODO: Version] - **TOE Build:** [TODO: Build number]

36.5.2 ALC_CMS: CM Scope

36.5.2.1 ALC_CMS.1: TOE CM Coverage

Required Evidence: [TODO: Describe the required evidence]

Documentation: - **Document Title:** [TODO: CM Scope Document] - **Document Number:** [TODO: Number] - **Version:** [TODO: Version] - **Date:** [TODO: Date] - **Location:** [TODO: Path] - **Classification:** [TODO: Classification]

Content: - List of all TOE components under CM control - List of all evaluation evidence under CM control - Description of CM procedures

Status: [TODO: Complete / In Progress / Planned]

CM Items: [TODO: List all CM items]

36.5.3 Additional ALC Components

[TODO: Add additional ALC components if required (e.g., ALC_DEL.1, ALC_DVS.1, ALC_LCD.1)]

36.6 ATE: Tests

36.6.1 ATE_IND: Independent Testing

36.6.1.1 ATE_IND.1: Independent Testing - Conformance

Required Evidence: [TODO: Describe the required evidence]

Documentation: - **Document Title:** [TODO: Test Documentation] - **Document Number:** [TODO: Number] - **Version:** [TODO: Version] - **Date:** [TODO: Date] - **Location:** [TODO: Path] - **Classification:** [TODO: Classification]

Content: - TOE for independent testing - Test environment - Test documentation - Test resources

Status: [TODO: Complete / In Progress / Planned]

Test Environment: [TODO: Describe the test environment]

36.6.2 Additional ATE Components

[TODO: Add additional ATE components if required (e.g., ATE_COV.1, ATE_FUN.1)]

36.7 AVA: Vulnerability Assessment

36.7.1 AVA_VAN: Vulnerability Analysis

36.7.1.1 AVA_VAN.1: Vulnerability Survey

Required Evidence: [TODO: Describe the required evidence]

Documentation: - **Document Title:** [TODO: Vulnerability Analysis Report] - **Document Number:** [TODO: Number] - **Version:** [TODO: Version] - **Date:** [TODO: Date] - **Location:** [TODO: Path] - **Classification:** [TODO: Strictly Confidential]

Content: - Analysis of publicly known vulnerabilities - Assessment of applicability to TOE - Evidence of resistance to vulnerabilities

Status: [TODO: Complete / In Progress / Planned]

Vulnerability Sources: [TODO: List vulnerability databases used (e.g., CVE, NVD)]

36.7.2 Additional AVA Components

[TODO: Add additional AVA components if required (e.g., AVA_VAN.2, AVA_VAN.3)]

36.8 Additional Evidence

36.8.1 Security Target (ST)

Documentation: - **Document Title:** Security Target for [TODO: TOE Name] - **Document Number:** [TODO: Number] - **Version:** [TODO: Version] - **Date:** [TODO: Date] - **Location:** [TODO: Path] - **Classification:** [TODO: Classification]

Status: [TODO: Complete / In Progress]

36.8.2 Evaluation Plan

Documentation: - **Document Title:** [TODO: Evaluation Plan] - **Document Number:** [TODO: Number] - **Version:** [TODO: Version] - **Date:** [TODO: Date] - **Location:** [TODO: Path] - **Classification:** [TODO: Classification]

Status: [TODO: Complete / In Progress / Planned]

36.8.3 Additional Documents

[TODO: List additional relevant documents]

36.9 Evidence Delivery

36.9.1 Delivery Plan

Evidence	Delivery Date	Recipient	Transmission Method
[TODO: Evidence 1]	[TODO: Date]	[TODO: Evaluation laboratory]	[TODO: Secure upload / Physical]
[TODO: Evidence 2]	[TODO: Date]	[TODO: Recipient]	[TODO: Method]

36.9.2 Access Control

Evidence	Classification	Authorized Personnel	Access Method
[TODO: Evidence 1]	[TODO: Classification]	[TODO: Roles]	[TODO: Method]
[TODO: Evidence 2]	[TODO]	[TODO]	[TODO]

36.10 Evidence Validation

36.10.1 Completeness Check

Check Date: [TODO: Date]
Checked By: [TODO: Name/Role]

Result: - [ ] All required evidence is present - [ ] All evidence is current - [ ] All evidence is complete - [ ] All evidence meets SAR requirements

Identified Gaps: [TODO: List missing or incomplete evidence]

36.10.2 Quality Check

Check Date: [TODO: Date]
Checked By: [TODO: Name/Role]

Criteria: - [ ] Evidence is clear and understandable - [ ] Evidence is consistent with ST - [ ] Evidence contains all required information - [ ] Evidence is technically correct

Identified Issues: [TODO: List quality issues]

36.11 Evidence Archiving

36.11.1 Archiving Plan

Archive Location: [TODO: Storage location]
Archive Duration: [TODO: Duration]
Responsible: [TODO: Role/Person]

Archived Versions: | Evidence | Version | Archive Date | Location | |———-|———|————|———-| | [TODO] | [TODO] | [TODO] | [TODO] |

36.11.2 Recovery Procedures

[TODO: Describe the procedure for recovering archived evidence]

36.12 Contact Information

36.12.1 Evidence Coordinator

Name: [TODO: Name]
Role: [TODO: Role]
Email: [TODO: Email]
Phone: [TODO: Phone]

36.12.2 Evaluation Laboratory Contact

Name: [TODO: Name]
Organization: [TODO: Evaluation laboratory]
Email: [TODO: Email]
Phone: [TODO: Phone]

Next Steps: 1. Identify all required evidence based on chosen EAL 2. Create a timeline for evidence creation 3. Assign responsibilities for each evidence item 4. Create or collect all required evidence 5. Conduct completeness and quality checks 6. Deliver evidence to evaluation laboratory 7. Archive all evidence according to requirements 8. Update evidence documentation when changes occur

ewpage