Contents

Chapter 1

Metadaten: Common Criteria Security Target

Dokument-ID: 0000
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

1.1 Handbuch-Informationen

Handbuch-Titel: Common Criteria Security Target (ISO/IEC 15408)
Organisation: {{ meta.organization }}
Autor: Andreas Huemmer [andreas.huemmer@adminsend.de]
Erstellungsdatum: {{ meta.date }}
Version: {{ meta.version }}
Geltungsbereich: {{ meta.scope }}

1.2 Zweck

Dieses Security Target (ST) dokumentiert die Sicherheitseigenschaften des Target of Evaluation (TOE) gemäß ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation). Es beschreibt die Sicherheitsfunktionen, Sicherheitsziele und Sicherheitsanforderungen des TOE sowie die Evaluierungsstufe (Evaluation Assurance Level, EAL).

1.3 Zielgruppe

- Evaluatoren und Zertifizierungsstellen
- Produktentwickler und Sicherheitsarchitekten

- Kunden und Beschaffer sicherheitskritischer IT-Produkte
- Auditoren und Compliance-Verantwortliche

1.4 Dokumentenstruktur

Das Security Target folgt der Struktur von ISO/IEC 15408-1:2022 und umfasst:

1. **ST Introduction** - Einführung, TOE-Übersicht, Konformitätsansprüche
2. **TOE Description** - Detaillierte Beschreibung des Evaluierungsgegenstands
3. **Security Problem Definition** - Bedrohungen, organisatorische Sicherheitspolitiken, Annahmen
4. **Security Objectives** - Sicherheitsziele für TOE und Umgebung
5. **Security Requirements** - Funktionale und Vertrauenswürdigkeitsanforderungen (SFR, SAR)
6. **TOE Summary Specification** - Zusammenfassung der Sicherheitsfunktionen
7. **Appendices** - PP-Konformität, Rationale, Glossar

1.5 Hinweise zur Verwendung

- Alle `[TODO]`-Platzhalter müssen durch spezifische Informationen ersetzt werden
- Platzhalter im Format `{{ source.field }}` werden automatisch aus Datenquellen befüllt
- Diagramme können im Unterordner `diagrams/` abgelegt werden
- Das ST muss konsistent mit dem gewählten Protection Profile (PP) sein
- Alle Sicherheitsanforderungen müssen aus ISO/IEC 15408-2 und 15408-3 stammen

---

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
{{ meta.version }}	{{ meta.date }}	Andreas Huemmer [andreas.huemmer@adminsend.de]	Initiale Version

ewpage

Chapter 2

ST Introduction

Dokument-ID: 0010
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

2.1 1. ST Identification

2.1.1 1.1 ST Title

ST Title: [TODO: Vollständiger Titel des 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: Kontaktinformationen]

2.1.3 1.3 TOE Identification

TOE Name: [TODO: Name des Target of Evaluation]
TOE Version: [TODO: Version des TOE]
TOE Developer: [TODO: Hersteller/Entwickler]
TOE Type: [TODO: Produkttyp, z.B. Firewall, Smartcard, Operating System]

2.2 2. ST Overview

2.2.1 2.1 Purpose

Dieses Security Target (ST) beschreibt die Sicherheitseigenschaften von [TODO: TOE Name] gemäß ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation). Das ST dient als Grundlage für die Evaluierung und Zertifizierung des TOE.

2.2.2 2.2 Scope

Das ST umfasst: - Physische und logische Beschreibung des TOE - Definition der Sicherheitsprobleme (Bedrohungen, OSPs, Annahmen) - Sicherheitsziele für TOE und Umgebung - Sicherheitsanforderungen (SFRs und SARs) - Zusammenfassung der Sicherheitsfunktionen - Begründungen (Rationales) für alle Beziehungen

2.2.3 2.3 Intended Readership

Dieses ST richtet sich an: - Evaluatoren und Zertifizierungsstellen - Produktentwickler und Sicherheitsarchitekten - Kunden und Beschaffer - Auditoren und Compliance-Verantwortliche

2.3 3. ST Reference

2.3.1 3.1 ST Identification

ST Reference: [TODO: Eindeutige Referenz, z.B. ST-PRODUCT-v1.0]
ST Registration: [TODO: Registrierungsnummer bei Zertifizierungsstelle]

2.3.2 3.2 TOE Reference

TOE Reference: [TODO: Eindeutige TOE-Referenz]
TOE Platform: [TODO: Hardware/Software-Plattform]
TOE Delivery: [TODO: Lieferform, z.B. Software-Download, Hardware-Gerät]

2.4 4. Document Organization

2.4.1 4.1 ST Structure

Das ST ist wie folgt strukturiert:

1. **ST Introduction** (dieses Dokument) - Einführung und Identifikation
2. **TOE Description** - Detaillierte Beschreibung des TOE
3. **Security Problem Definition** - Bedrohungen, OSPs, Annahmen
4. **Security Objectives** - Sicherheitsziele
5. **Security Requirements** - SFRs und SARs
6. **TOE Summary Specification** - Sicherheitsfunktionen
7. **Appendices** - PP-Konformität, Rationales, Glossar

2.4.2 4.2 Document Conventions

- **SFR**: Security Functional Requirement (Funktionale Sicherheitsanforderung)

- **SAR**: Security Assurance Requirement (Vertrauenswürdigkeitsanforderung)
- **TOE**: Target of Evaluation (Evaluierungsgegenstand)
- **TSF**: TOE Security Functionality (Sicherheitsfunktionalität des TOE)
- **PP**: Protection Profile (Schutzprofil)
- **EAL**: Evaluation Assurance Level (Evaluierungsstufe)

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: Liste relevanter Protection Profiles, falls zutreffend] - PP Name: [TODO] - PP Version: [TODO] - PP Registration: [TODO]

2.5.3 5.3 TOE Documentation

[TODO: Liste der TOE-Dokumentation] - 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: Beschreibung der Änderungen]

Nächste Schritte: 1. Vervollständigen Sie alle [TODO]-Platzhalter 2. Überprüfen Sie die Konsistenz mit anderen ST-Abschnitten 3. Stellen Sie sicher, dass alle Referenzen korrekt sind 4. Lassen Sie das Dokument von relevanten Stakeholdern reviewen

ewpage

Chapter 3

TOE Overview

Dokument-ID: 0020
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

3.1 1. TOE Overview

3.1.1 1.1 TOE Type

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

3.1.2 1.2 TOE Purpose

[TODO: Beschreibe den Hauptzweck und die Funktionalität des TOE]

Der TOE bietet: - [TODO: Hauptfunktion 1] - [TODO: Hauptfunktion 2] - [TODO: Hauptfunktion 3]

3.1.3 1.3 TOE Usage

Intended Use: [TODO: Beschreibe den vorgesehenen Anwendungsfall]
Target Environment: [TODO: z.B. Unternehmensnetzwerk, Behörde, Consumer-Gerät]
User Types: [TODO: z.B. Administratoren, Endbenutzer, Sicherheitsbeauftragte]

3.2 2. TOE Scope

3.2.1 2.1 Physical Scope

Der TOE besteht aus folgenden physischen Komponenten:

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

3.2.2 2.2 Logical Scope

Der TOE bietet folgende Sicherheitsfunktionen:

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

3.2.3 2.3 TOE Boundaries

Im TOE enthalten: - [TODO: Komponente/Funktion enthalten] - [TODO: Komponente/Funktion enthalten]

Nicht im TOE enthalten: - [TODO: Komponente/Funktion ausgeschlossen] - [TODO: Komponente/Funktion ausgeschlossen]

3.3 3. TOE Features

3.3.1 3.1 Major Security Features

[TODO: Beschreibe die wichtigsten Sicherheitsfunktionen]

1. **[TODO: Feature 1]**
   - Beschreibung: [TODO]
   - Sicherheitsnutzen: [TODO]
2. **[TODO: Feature 2]**
   - Beschreibung: [TODO]
   - Sicherheitsnutzen: [TODO]
3. **[TODO: Feature 3]**
   - Beschreibung: [TODO]
   - Sicherheitsnutzen: [TODO]

3.3.2 3.2 Non-Security Features

[TODO: Liste nicht-sicherheitsrelevante Features, die Teil des TOE sind, aber nicht evaluiert werden] - [TODO: Feature 1] - [TODO: Feature 2]

3.4 4. TOE Architecture

3.4.1 4.1 High-Level Architecture

[TODO: Stelle ein High-Level-Architekturdiagramm bereit]

`[TODO: Architekturdiagramm oder Beschreibung einfügen]`

3.4.2 4.2 Components

Hauptkomponenten: 1. [TODO: Komponentenname] - Zweck: [TODO] - Technologie: [TODO] - Schnittstellen: [TODO]

2. [TODO: Komponentenname]
   - Zweck: [TODO]
   - Technologie: [TODO]
   - Schnittstellen: [TODO]

3.4.3 4.3 Data Flow

[TODO: Beschreibe die Hauptdatenflüsse innerhalb des TOE]

`[TODO: Datenflussdiagramm oder Beschreibung einfügen]`

3.5 5. TOE Environment

3.5.1 5.1 Operational Environment

Hardware Platform: [TODO: Erforderliche Hardware]
Operating System: [TODO: Erforderliches OS]
Network: [TODO: Netzwerkanforderungen]
Dependencies: [TODO: Externe Abhängigkeiten]

3.5.2 5.2 Environmental Assumptions

Der TOE nimmt folgendes über seine Umgebung an: - [TODO: Annahme 1] - [TODO: Annahme 2] - [TODO: Annahme 3]

3.5.3 5.3 Environmental Security

Die Umgebung muss bereitstellen: - [TODO: Sicherheitsmaßnahme 1] - [TODO: Sicherheitsmaßnahme 2] - [TODO: Sicherheitsmaßnahme 3]

3.6 6. TOE Interfaces

3.6.1 6.1 User Interfaces

Interface	Type	Users	Description
[TODO: Interface 1]	GUI/CLI/API	[TODO: Benutzertyp]	[TODO: Beschreibung]
[TODO: Interface 2]	GUI/CLI/API	[TODO: Benutzertyp]	[TODO: Beschreibung]

3.6.2 6.2 External Interfaces

Interface	Protocol	Purpose	Security
[TODO: Interface 1]	[TODO: Protokoll]	[TODO: Zweck]	[TODO: Sicherheits-maßnahmen]
[TODO: Interface 2]	[TODO: Protokoll]	[TODO: Zweck]	[TODO: Sicherheits-maßnahmen]

3.6.3 6.3 Administrative Interfaces

[TODO: Beschreibe administrative Schnittstellen] - Konfigurationsschnittstelle: [TODO] - Monitoring-Schnittstelle: [TODO] - Logging-Schnittstelle: [TODO]

3.7 7. TOE Lifecycle

3.7.1 7.1 Development

Development Process: [TODO: Beschreibe Entwicklungsmethodik]
Security in Development: [TODO: Sicherheitsmaßnahmen während der Entwicklung]

3.7.2 7.2 Delivery

Delivery Method: [TODO: z.B. Download, Physische Medien, Vorinstalliert]
Integrity Protection: [TODO: z.B. Digitale Signatur, Prüfsumme]

3.7.3 7.3 Installation

Installation Process: [TODO: Kurze Beschreibung]
Secure Installation: [TODO: Sicherheitsmaßnahmen während der Installation]

3.7.4 7.4 Operation

Operational Modes: [TODO: z.B. Normalmodus, Wartungsmodus]
Secure Operation: [TODO: Sicherheitsmaßnahmen während des Betriebs]

3.7.5 7.5 Maintenance

Maintenance Activities: [TODO: z.B. Updates, Patches, Konfigurationsänderungen]
Secure Maintenance: [TODO: Sicherheitsmaßnahmen während der Wartung]

3.7.6 7.6 Decommissioning

Decommissioning Process: [TODO: Kurze Beschreibung]
Secure Decommissioning: [TODO: z.B. Datenlöschung, Schlüsselvernichtung]

3.8 8. TOE Documentation

3.8.1 8.1 User Documentation

- [TODO: Benutzerhandbuch]
- [TODO: Schnellstartanleitung]

- [TODO: Online-Hilfe]

3.8.2 8.2 Administrator Documentation

- [TODO: Administratorhandbuch]
- [TODO: Installationsanleitung]
- [TODO: Konfigurationshandbuch]
- [TODO: Sicherheitshandbuch]

3.8.3 8.3 Developer Documentation

- [TODO: Architekturdokument]
- [TODO: Design-Spezifikation]
- [TODO: Sicherheitsarchitektur]

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter mit TOE-spezifischen Informationen 2. Erstelle Architektur- und Datenflussdiagramme 3. Überprüfe die Konsistenz mit der detaillierten TOE-Beschreibung 4. Stelle sicher, dass alle Schnittstellen dokumentiert sind

ewpage

Chapter 4

TOE Description Summary

Dokument-ID: 0030
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

4.1 1. TOE Summary

4.1.1 1.1 Product Summary

Product Name: [TODO: Produktname]
Version: [TODO: Version]
Type: [TODO: Produkttyp]

Kurzbeschreibung:
[TODO: 2-3 Sätze, die den TOE zusammenfassen]

4.1.2 1.2 Security Summary

Der TOE bietet Sicherheit durch: - [TODO: Hauptsicherheitsmerkmal 1] - [TODO: Hauptsicherheitsmerkmal 2] - [TODO: Hauptsicherheitsmerkmal 3]

4.2 2. Physical Description

4.2.1 2.1 Hardware Components

[TODO: Falls zutreffend] - [TODO: Hardware-Komponente 1] - [TODO: Hardware-Komponente 2]

4.2.2 2.2 Software Components

[TODO: Falls zutreffend] - [TODO: Software-Komponente 1] - [TODO: Software-Komponente 2]

4.2.3 2.3 Firmware Components

[TODO: Falls zutreffend] - [TODO: Firmware-Komponente 1] - [TODO: Firmware-Komponente 2]

4.3 3. Logical Description

4.3.1 3.1 Security Functions

Der TOE implementiert folgende Sicherheitsfunktionen:

1. **[TODO: Funktion 1]**
   - Zweck: [TODO]
   - Mechanismus: [TODO]
2. **[TODO: Funktion 2]**
   - Zweck: [TODO]
   - Mechanismus: [TODO]
3. **[TODO: Funktion 3]**
   - Zweck: [TODO]
   - Mechanismus: [TODO]

4.3.2 3.2 Security Domains

[TODO: Beschreibe Sicherheitsdomänen, falls zutreffend] - Domain 1: [TODO] - Domain 2: [TODO]

4.4 4. TOE Configuration

4.4.1 4.1 Evaluated Configuration

Configuration: [TODO: Beschreibe die evaluierte Konfiguration]
Options: [TODO: Konfigurationsoptionen]
Modes: [TODO: Betriebsmodi]

4.4.2 4.2 Non-Evaluated Configurations

[TODO: Liste Konfigurationen auf, die nicht Teil der Evaluierung sind] - [TODO: Konfiguration 1] - [TODO: Konfiguration 2]

4.5 5. TOE Capabilities

4.5.1 5.1 Security Capabilities

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

4.5.2 5.2 Performance Characteristics

[TODO: Beschreibe relevante Performance-Charakteristiken] - Throughput: [TODO] - Latency: [TODO] - Capacity: [TODO]

4.6 6. TOE Dependencies

4.6.1 6.1 Hardware Dependencies

[TODO: Liste Hardware-Abhängigkeiten auf] - [TODO: Abhängigkeit 1] - [TODO: Abhängigkeit 2]

4.6.2 6.2 Software Dependencies

[TODO: Liste Software-Abhängigkeiten auf] - [TODO: Abhängigkeit 1] - [TODO: Abhängigkeit 2]

4.6.3 6.3 Environmental Dependencies

[TODO: Liste Umgebungsabhängigkeiten auf] - [TODO: Abhängigkeit 1] - [TODO: Abhängigkeit 2]

4.7 7. TOE Limitations

4.7.1 7.1 Functional Limitations

[TODO: Beschreibe funktionale Einschränkungen] - [TODO: Einschränkung 1] - [TODO: Einschränkung 2]

4.7.2 7.2 Security Limitations

[TODO: Beschreibe Sicherheitseinschränkungen] - [TODO: Einschränkung 1] - [TODO: Einschränkung 2]

4.7.3 7.3 Out of Scope

[TODO: Was ist explizit außerhalb des Scopes] - [TODO: Item 1] - [TODO: Item 2]

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter 2. Stelle Konsistenz mit der detaillierten TOE-Beschreibung sicher 3. Überprüfe, dass alle Komponenten aufgelistet sind

ewpage

Chapter 5

Conformance Claims

Dokument-ID: 0040
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ 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: Wähle eine Option] - [ ] CC Part 2 conformant - [ ] CC Part 2 extended - [ ] CC Part 3 conformant - [ ] CC Part 3 extended

Begründung: [TODO: Begründe die Konformitätsansprüche]

5.2 2. PP Conformance Claim

5.2.1 2.1 PP Identification

[TODO: Falls zutreffend, identifiziere das Protection Profile]

PP Name: [TODO: Name des Protection Profile]
PP Version: [TODO: Version]
PP Registration: [TODO: Registrierungsnummer]
PP Date: [TODO: Datum]

5.2.2 2.2 PP Conformance Type

[TODO: Wähle den Konformitätstyp] - [ ] Strict conformance - [ ] Demonstrable conformance - [ ] No PP conformance

Begründung: [TODO: Begründe den Konformitätstyp]

5.2.3 2.3 PP Deviations

[TODO: Falls zutreffend, dokumentiere Abweichungen vom PP]

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

5.3 3. Package Conformance Claim

5.3.1 3.1 Assurance Package

Package: [TODO: Wähle das 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: Falls zutreffend, liste zusätzliche SARs auf]

Augmentation: [TODO: Ja/Nein]

SAR Component	Rationale
[TODO: SAR 1]	[TODO: Begründung für Hinzufügung]
[TODO: SAR 2]	[TODO: Begründung für Hinzufügung]

5.4 4. Conformance Rationale

5.4.1 4.1 CC Part 2 Conformance Rationale

[TODO: Begründe die Konformität mit CC Part 2]

SFR Selection: - Alle SFRs stammen aus ISO/IEC 15408-2:2022 - [TODO: Weitere Details]

SFR Extensions: [TODO: Falls zutreffend, begründe SFR-Erweiterungen] - [TODO: Erweiterung 1] - [TODO: Erweiterung 2]

5.4.2 4.2 CC Part 3 Conformance Rationale

[TODO: Begründe die Konformität mit CC Part 3]

SAR Selection: - Alle SARs stammen aus ISO/IEC 15408-3:2022 - [TODO: Weitere Details]

SAR Augmentation: [TODO: Falls zutreffend, begründe SAR-Augmentierungen] - [TODO: Augmentierung 1] - [TODO: Augmentierung 2]

5.4.3 4.3 PP Conformance Rationale

[TODO: Falls PP-Konformität beansprucht wird]

Conformance Demonstration: - [TODO: Zeige, wie das ST dem PP entspricht] - [TODO: Dokumentiere alle Abweichungen] - [TODO: Begründe alle Ergänzungen]

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 oder "None"]	[TODO: Details]
Assurance Package	[TODO: EAL Level]	[TODO: Details]
Augmentation	[TODO: Yes/No]	[TODO: Details]

5.5.2 5.2 Conformance Verification

[TODO: Beschreibe, wie die Konformität verifiziert werden kann] - 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: Datum]

5.6.2 6.2 Change Management

[TODO: Beschreibe, wie Änderungen an Konformitätsansprüchen verwaltet werden] - Change process: [TODO] - Impact assessment: [TODO] - Re-evaluation triggers: [TODO]

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter 2. Verifiziere Konformität mit gewählten Standards 3. Dokumentiere alle Abweichungen vollständig 4. Stelle Konsistenz mit anderen ST-Abschnitten sicher

ewpage

Chapter 6

Document Conventions

Dokument-ID: 0050
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

6.1 1. Terminology and Notation

6.1.1 1.1 Common Criteria Terminology

Dieses Security Target verwendet Terminologie aus ISO/IEC 15408:2022:

Term	Definition
TOE	Target of Evaluation - das IT-Produkt oder -System, das evaluiert wird
TSF	TOE Security Functionality - kombinierte Funktionalität aller Hardware, Software und Firmware des TOE, die für die korrekte Durchsetzung der SFRs erforderlich ist
TSP	TOE Security Policy - Regelwerk, das regelt, wie Assets innerhalb des TOE verwaltet, geschützt und verteilt werden
SFR	Security Functional Requirement - Anforderung an die Sicherheitsdurchsetzung durch den TOE
SAR	Security Assurance Requirement - Anforderung zur Sicherstellung der Sicherheit des TOE
PP	Protection Profile - implementierungsunabhängige Aussage über Sicherheitsbedürfnisse für einen TOE-Typ
ST	Security Target - implementierungsabhängige Aussage über Sicherheitsbedürfnisse für einen spezifischen TOE
EAL	Evaluation Assurance Level - Paket von Vertrauenswürdigkeitsanforderungen

6.1.2 1.2 TOE-Specific Terminology

[TODO: Definiere TOE-spezifische Begriffe]

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

6.2 2. Notation Conventions

6.2.1 2.1 SFR Notation

Security Functional Requirements werden mit der Notation aus ISO/IEC 15408-2:2022 identifiziert:

Format: `CLASS.FAMILY.COMPONENT.ELEMENT`

Beispiel: `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 werden mit der Notation aus ISO/IEC 15408-3:2022 identifiziert:

Format: `CLASS.FAMILY.COMPONENT`

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

6.2.3 2.3 Operations on Requirements

Folgende Operationen können auf SFRs und SARs angewendet werden:

Operation	Symbol	Description
Assignment	[assignment:]	Parameter spezifizieren
Selection	[selection:]	Aus einer Liste von Optionen wählen
Refinement	**fett**	Details hinzufügen oder einschränken
Iteration	/iteration	Anforderung mehrfach anwenden

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

6.3 3. Document Structure

6.3.1 3.1 Section Organization

Dieses ST ist gemäß ISO/IEC 15408-1:2022 organisiert:

1. **ST Introduction** - Identifikation und Überblick

2. **TOE Description** - Physische und logische Beschreibung
3. **Security Problem Definition** - Bedrohungen, OSPs, Annahmen
4. **Security Objectives** - Ziele für TOE und Umgebung
5. **Security Requirements** - SFRs und SARs
6. **TOE Summary Specification** - Sicherheitsfunktionen
7. **Appendices** - Unterstützende Informationen

6.3.2 3.2 Cross-References

Querverweise innerhalb dieses ST verwenden folgendes Format: - Abschnittsverweise: “Siehe Abschnitt X.Y” - Tabellenverweise: “Siehe Tabelle X” - Abbildungsverweise: “Siehe Abbildung X”

6.4 4. Formatting Conventions

6.4.1 4.1 Text Formatting

Format	Usage
Fett	Betonung, Verfeinerungen
Kursiv	Definitionen, erste Verwendung von Begriffen
`Monospace`	Code, Befehle, Identifikatoren
[TODO]	Platzhalter, der vervollständigt werden muss

6.4.2 4.2 Lists and Tables

- **Aufzählungslisten**: Verwendet für ungeordnete Elemente
- **Nummerierte Listen**: Verwendet für sequenzielle Schritte oder geordnete Elemente
- **Tabellen**: Verwendet für strukturierte Daten und Zuordnungen

6.4.3 4.3 Diagrams

[TODO: Beschreibe Diagrammkonventionen, falls zutreffend] - Architekturdiagramme: [TODO] - Datenflussdiagramme: [TODO] - Sequenzdiagramme: [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: Liste TOE-spezifische Abkürzungen auf]

Abbreviation	Full Term
[TODO: Abk. 1]	[TODO: Vollständiger Begriff]
[TODO: Abk. 2]	[TODO: Vollständiger Begriff]
[TODO: Abk. 3]	[TODO: Vollständiger Begriff]

6.6 6. References

6.6.1 6.1 Normative References

Folgende Dokumente werden normativ in diesem ST referenziert:

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: Liste informative Referenzen auf]

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

6.7 7. Document Conventions Summary

6.7.1 7.1 Key Conventions

- Alle SFRs stammen aus ISO/IEC 15408-2:2022, sofern nicht als erweitert markiert
- Alle SARs stammen aus ISO/IEC 15408-3:2022, sofern nicht als augmentiert markiert
- Operationen auf Anforderungen sind klar markiert
- Alle [TODO]-Platzhalter müssen vor Finalisierung vervollständigt werden

6.7.2 7.2 Consistency Rules

- Terminologie muss im gesamten ST konsistent sein
- Alle Querverweise müssen gültig sein
- Alle Tabellen und Abbildungen müssen sequenziell nummeriert sein
- Alle Anforderungen müssen eindeutig identifiziert sein

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter 2. Verifiziere Konsistenz der Terminologieverwendung 3. Stelle sicher, dass alle Abkürzungen definiert sind 4. Prüfe, dass alle Referenzen vollständig sind

ewpage

Chapter 7

TOE Physical Scope

Dokument-ID: 0100
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

7.1 1. Physical Components Overview

7.1.1 1.1 TOE Physical Composition

Der TOE besteht aus folgenden physischen Komponenten:

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

7.1.2 1.2 Component Dependencies

[TODO: Beschreibe Abhängigkeiten zwischen physischen Komponenten]

`[TODO: Komponentenabhängigkeitsdiagramm einfügen]`

7.2 2. Hardware Components

7.2.1 2.1 Hardware Inventory

Hardware-Komponenten im TOE:

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

7.2.2 2.2 Hardware Specifications

[TODO: Hardware-Komponente 1] - Prozessor: [TODO: CPU-Spezifikationen] - Speicher: [TODO: RAM-Spezifikationen] - Speichermedien: [TODO: Storage-Spezifikationen] - Netzwerk: [TODO: Netzwerkschnittstellen] - Sicherheitsmodule: [TODO: z.B. TPM, HSM, Secure Element]

[TODO: Hardware-Komponente 2] - [TODO: Spezifikationen]

7.2.3 2.3 Hardware Security Features

[TODO: Beschreibe hardwarebasierte Sicherheitsfunktionen] - Secure Boot: [TODO: Beschreibung] - Hardware-Verschlüsselung: [TODO: Beschreibung] - Tamper-Schutz: [TODO: Beschreibung] - Physische Sicherheitsmerkmale: [TODO: Beschreibung]

7.3 3. Software Components

7.3.1 3.1 Software Inventory

Software-Komponenten im TOE:

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

7.3.2 3.2 Software Modules

[TODO: Software-Modul 1] - Zweck: [TODO: Beschreibung] - Programmiersprache: [TODO: z.B. C, C++, Java, Python] - Größe: [TODO: LOC oder Dateigröße] - Abhängigkeiten: [TODO: Externe Bibliotheken]

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

7.3.3 3.3 Software Configuration

Konfigurationsdateien: - [TODO: Konfigurationsdatei 1]: [TODO: Zweck] - [TODO: Konfigurationsdatei 2]: [TODO: Zweck]

Datenbanken: - [TODO: Datenbank 1]: [TODO: Zweck und Schema]

7.4 4. Firmware Components

7.4.1 4.1 Firmware Inventory

Firmware-Komponenten im TOE:

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

7.4.2 4.2 Firmware Details

[TODO: Firmware-Komponente 1] - Typ: [TODO: z.B. BIOS, UEFI, Embedded Controller] - Größe: [TODO: Größe in KB/MB] - Update-Mechanismus: [TODO: Beschreibung] - Signatur: [TODO: Signiermethode]

7.4.3 4.3 Firmware Security

[TODO: Beschreibe Firmware-Sicherheitsmaßnahmen] - Secure Firmware Update: [TODO] - Firmware-Integritätsprüfung: [TODO] - Rollback-Schutz: [TODO]

7.5 5. Documentation Components

7.5.1 5.1 User Documentation

Im TOE enthaltene Benutzerdokumentation: - [TODO: Benutzerhandbuch]: [TODO: Format, Version] - [TODO: Schnellstartanleitung]: [TODO: Format, Version] - [TODO: Online-Hilfe]: [TODO: Format, Version]

7.5.2 5.2 Administrator Documentation

Im TOE enthaltene Administratordokumentation: - [TODO: Administratorhandbuch]: [TODO: Format, Version] - [TODO: Installationsanleitung]: [TODO: Format, Version] - [TODO: Konfigurationshandbuch]: [TODO: Format, Version] - [TODO: Sicherheitshandbuch]: [TODO: Format, Version]

7.5.3 5.3 Security Documentation

Sicherheitsrelevante Dokumentation: - Security Target (ST): [TODO: Version] - [TODO: Weitere Sicherheitsdokumentation]

7.6 6. Physical Boundaries

7.6.1 6.1 Included Components

Folgende Komponenten sind im TOE enthalten: - [TODO: Komponente 1]: [TODO: Begründung für Einschluss] - [TODO: Komponente 2]: [TODO: Begründung für Einschluss] - [TODO: Komponente 3]: [TODO: Begründung für Einschluss]

7.6.2 6.2 Excluded Components

Folgende Komponenten sind NICHT im TOE enthalten: - [TODO: Komponente 1]: [TODO: Begründung für Ausschluss] - [TODO: Komponente 2]: [TODO: Begründung für Ausschluss] - [TODO: Komponente 3]: [TODO: Begründung für Ausschluss]

7.6.3 6.3 Boundary Rationale

[TODO: Erkläre die Begründung für die physischen Grenzen des TOE]

Die physischen Grenzen wurden wie folgt definiert: - [TODO: Begründung 1] - [TODO: Begründung 2] - [TODO: Begründung 3]

7.7 7. Delivery and Packaging

7.7.1 7.1 Delivery Format

Der TOE wird geliefert als: - [TODO: z.B. Physisches Gerät, Software-Download, Container-Image, etc.]

Liefermedien: - [TODO: z.B. USB-Stick, DVD, Download-Link, etc.]

7.7.2 7.2 Package Contents

Das TOE-Paket enthält: 1. [TODO: Komponente 1] 2. [TODO: Komponente 2] 3. [TODO: Komponente 3] 4. [TODO: Dokumentation] 5. [TODO: Lizenzinformationen]

7.7.3 7.3 Integrity Protection

Integritätsschutz für Lieferung: - Digitale Signatur: [TODO: Signaturalgorithmus und Schlüssel] - Prüfsummen: [TODO: Hash-Algorithmus] - Versiegelung: [TODO: Physische Versiegelung falls zutreffend]

7.8 8. Version Control

7.8.1 8.1 Component Versions

Versionskontrolle für TOE-Komponenten:

Component	Version	Release Date	Changes
[TODO: Komponente 1]	[TODO: Version]	[TODO: Datum]	[TODO: Änderungen]
[TODO: Komponente 2]	[TODO: Version]	[TODO: Datum]	[TODO: Änderungen]

7.8.2 8.2 Version Identification

Versionserkennung: - Methode: [TODO: z.B. About-Dialog, Versionsdatei, CLI-Befehl] - Befehl: [TODO: z.B. `--version`, `/version`, etc.] - Ausgabeformat: [TODO: Beispielausgabe]

7.8.3 8.3 Configuration Management

Konfigurationsmanagement: - CM-System: [TODO: z.B. Git, SVN, etc.] - Repository: [TODO: Repository-Informationen] - Build-System: [TODO: Build-System-Informationen]

7.9 9. Physical Scope Diagram

7.9.1 9.1 Component Diagram

[TODO: Erstelle ein Diagramm, das alle physischen Komponenten und ihre Beziehungen zeigt]

`[TODO: Komponentendiagramm einfügen]`

7.9.2 9.2 Deployment Diagram

[TODO: Erstelle ein Deployment-Diagramm, das zeigt, wie Komponenten bereitgestellt werden]

`[TODO: Deployment-Diagramm einfügen]`

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter mit TOE-spezifischen Informationen 2. Erstelle detaillierte Komponentendiagramme 3. Dokumentiere alle Versionen und Build-Informationen 4. Überprüfe die Konsistenz mit dem logischen Umfang (Template 0110) 5. Stelle sicher, dass alle Lieferkomponenten dokumentiert sind

ewpage

Chapter 8

TOE Logical Scope

Dokument-ID: 0110
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

8.1 1. Logical Components Overview

8.1.1 1.1 TOE Logical Composition

Der TOE besteht aus folgenden logischen Komponenten:

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

8.1.2 1.2 Logical Architecture

[TODO: Beschreibe die logische Architektur des TOE]

`[TODO: Logisches Architekturdiagramm einfügen]`

8.2 2. Security Functions

8.2.1 2.1 Security Function Overview

Der TOE bietet folgende Sicherheitsfunktionen:

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

8.2.2 2.2 Identification and Authentication

Identifikations- und Authentifizierungsfunktionen:

[TODO: Funktion 1] - Zweck: [TODO: z.B. Benutzeridentifikation] - Mechanismus: [TODO: z.B. Username/Password, Biometrie, Token] - Stärke: [TODO: z.B. Multi-Faktor, Single-Faktor] - Unterstützte Methoden: [TODO: Liste der Methoden]

[TODO: Funktion 2] - [TODO: Details]

8.2.3 2.3 Access Control

Zugriffskontrollfunktionen:

[TODO: Funktion 1] - Modell: [TODO: z.B. DAC, MAC, RBAC, ABAC] - Granularität: [TODO: z.B. Datei, Objekt, Feld] - Durchsetzung: [TODO: Beschreibung] - Verwaltung: [TODO: Beschreibung]

[TODO: Funktion 2] - [TODO: Details]

8.2.4 2.4 Audit and Logging

Audit- und Logging-Funktionen:

[TODO: Funktion 1] - Ereignistypen: [TODO: Liste der auditierten Ereignisse] - Audit-Daten: [TODO: Gespeicherte Informationen] - Speicherung: [TODO: Speichermechanismus] - Schutz: [TODO: Integritätsschutz] - Überprüfung: [TODO: Überprüfungsmechanismen]

[TODO: Funktion 2] - [TODO: Details]

8.2.5 2.5 Cryptographic Functions

Kryptografische Funktionen:

[TODO: Funktion 1] - Zweck: [TODO: z.B. Verschlüsselung, Signatur, Hashing] - Algorithmen: [TODO: z.B. AES-256, RSA-2048, SHA-256] - Schlüssellängen: [TODO: Schlüssellängen] - Modi: [TODO: z.B. CBC, GCM, CTR] - Schlüsselverwaltung: [TODO: Beschreibung]

[TODO: Funktion 2] - [TODO: Details]

8.2.6 2.6 Data Protection

Datenschutzfunktionen:

[**TODO: Funktion 1**] - Datentyp: [TODO: z.B. Benutzerdaten, Konfiguration, Credentials] - Schutzmechanismus: [TODO: z.B. Verschlüsselung, Hashing, Obfuscation] - Speicherort: [TODO: z.B. Datenbank, Dateisystem, Memory] - Lebenszyklus: [TODO: Erstellung, Nutzung, Löschung]

[**TODO: Funktion 2**] - [TODO: Details]

8.2.7 2.7 Communication Security

Kommunikationssicherheitsfunktionen:

[**TODO: Funktion 1**] - Protokoll: [TODO: z.B. TLS 1.3, IPsec, SSH] - Verschlüsselung: [TODO: Algorithmen und Modi] - Authentifizierung: [TODO: Mechanismus] - Integritätsschutz: [TODO: Mechanismus]

[**TODO: Funktion 2**] - [TODO: Details]

8.2.8 2.8 Security Management

Sicherheitsmanagementfunktionen:

[**TODO: Funktion 1**] - Verwaltungsbereich: [TODO: z.B. Benutzer, Richtlinien, Konfiguration] - Verwaltungsschnittstelle: [TODO: GUI/CLI/API] - Berechtigungen: [TODO: Erforderliche Rechte] - Audit: [TODO: Auditierung von Verwaltungsaktionen]

[**TODO: Funktion 2**] - [TODO: Details]

8.3 3. Functional Modules

8.3.1 3.1 Core Modules

Kernmodule des TOE:

[**TODO: Modul 1**] - Zweck: [TODO: Beschreibung] - Funktionen: [TODO: Bereitgestellte Funktionen] - Schnittstellen: [TODO: Interne und externe Schnittstellen] - Abhängigkeiten: [TODO: Abhängigkeiten zu anderen Modulen] - Sicherheitsrelevanz: [TODO: Sicherheitsfunktionen]

[**TODO: Modul 2**] - [TODO: Details]

8.3.2 3.2 Security Modules

Sicherheitsmodule:

[**TODO: Sicherheitsmodul 1**] - Zweck: [TODO: Beschreibung] - Sicherheitsfunktionen: [TODO: Implementierte Sicherheitsfunktionen] - Kryptografie: [TODO: Verwendete kryptografische Mechanismen] - Schnittstellen: [TODO: Schnittstellen]

[**TODO: Sicherheitsmodul 2**] - [TODO: Details]

8.3.3 3.3 Support Modules

Unterstützungsmodule:

[TODO: Modul 1] - Zweck: [TODO: Beschreibung] - Funktionen: [TODO: Bereitgestellte Funktionen] - Sicherheitsrelevanz: [TODO: Indirekte Sicherheitsrelevanz]

[TODO: Modul 2] - [TODO: Details]

8.4 4. Functional Capabilities

8.4.1 4.1 User Functions

Benutzerfunktionen:

Function	Description	Security Impact
[TODO: Funktion 1]	[TODO: Beschreibung]	[TODO: Sicherheitsauswirkung]
[TODO: Funktion 2]	[TODO: Beschreibung]	[TODO: Sicherheitsauswirkung]
[TODO: Funktion 3]	[TODO: Beschreibung]	[TODO: Sicherheitsauswirkung]

8.4.2 4.2 Administrative Functions

Administratorfunktionen:

Function	Description	Required Privilege
[TODO: Funktion 1]	[TODO: Beschreibung]	[TODO: Erforderliche Berechtigung]
[TODO: Funktion 2]	[TODO: Beschreibung]	[TODO: Erforderliche Berechtigung]
[TODO: Funktion 3]	[TODO: Beschreibung]	[TODO: Erforderliche Berechtigung]

8.4.3 4.3 System Functions

Systemfunktionen:

Function	Description	Trigger
[TODO: Funktion 1]	[TODO: Beschreibung]	[TODO: Auslöser]
[TODO: Funktion 2]	[TODO: Beschreibung]	[TODO: Auslöser]
[TODO: Funktion 3]	[TODO: Beschreibung]	[TODO: Auslöser]

8.5 5. Logical Boundaries

8.5.1 5.1 Included Functions

Folgende Funktionen sind im TOE enthalten:

Sicherheitsfunktionen: - [TODO: Funktion 1]: [TODO: Begründung für Einschluss] - [TODO: Funktion 2]: [TODO: Begründung für Einschluss]

Nicht-Sicherheitsfunktionen: - [TODO: Funktion 1]: [TODO: Begründung für Einschluss] - [TODO: Funktion 2]: [TODO: Begründung für Einschluss]

8.5.2 5.2 Excluded Functions

Folgende Funktionen sind NICHT im TOE enthalten: - [TODO: Funktion 1]: [TODO: Begründung für Ausschluss] - [TODO: Funktion 2]: [TODO: Begründung für Ausschluss] - [TODO: Funktion 3]: [TODO: Begründung für Ausschluss]

8.5.3 5.3 Boundary Rationale

[TODO: Erkläre die Begründung für die logischen Grenzen des TOE]

Die logischen Grenzen wurden wie folgt definiert: - [TODO: Begründung 1] - [TODO: Begründung 2] - [TODO: Begründung 3]

8.6 6. Security Mechanisms

8.6.1 6.1 Authentication Mechanisms

Authentifizierungsmechanismen:

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

8.6.2 6.2 Authorization Mechanisms

Autorisierungsmechanismen:

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

8.6.3 6.3 Cryptographic Mechanisms

Kryptografische Mechanismen:

Mechanism	Algorithm	Key Length	Purpose
[TODO: Mechanismus 1]	[TODO: Algorithmus]	[TODO: Schlüssellänge]	[TODO: Zweck]
[TODO: Mechanismus 2]	[TODO: Algorithmus]	[TODO: Schlüssellänge]	[TODO: Zweck]

8.6.4 6.4 Integrity Mechanisms

Integritätsmechanismen:

Mechanism	Type	Protected Asset	Verification
[TODO: Mechanismus 1]	Hash/MAC/Signature	[TODO: Geschütztes Asset]	[TODO: Verifikation]
[TODO: Mechanismus 2]	Hash/MAC/Signature	[TODO: Geschütztes Asset]	[TODO: Verifikation]

8.7 7. Data Flow

8.7.1 7.1 Internal Data Flow

[TODO: Beschreibe den internen Datenfluss zwischen logischen Komponenten]

`[TODO: Internes Datenflussdiagramm einfügen]`

8.7.2 7.2 Security-Critical Data Flow

[TODO: Beschreibe sicherheitskritische Datenflüsse]

[TODO: Datenfluss 1] - Quelle: [TODO: Quellkomponente] - Ziel: [TODO: Zielkomponente] - Datentyp: [TODO: z.B. Credentials, Keys, Audit Data] - Schutz: [TODO: Schutzmechanismen]

[TODO: Datenfluss 2] - [TODO: Details]

8.7.3 7.3 Trust Boundaries

[TODO: Definiere Vertrauensgrenzen innerhalb des TOE]

`[TODO: Vertrauensgrenzendiagramm einfügen]`

8.8 8. Functional Architecture

8.8.1 8.1 Layered Architecture

[TODO: Beschreibe die geschichtete Architektur des TOE]

Schicht 1: [TODO: Schichtname] - Zweck: [TODO: Beschreibung] - Komponenten: [TODO: Komponenten in dieser Schicht] - Schnittstellen: [TODO: Schnittstellen]

Schicht 2: [TODO: Schichtname] - [TODO: Details]

8.8.2 8.2 Component Interactions

[TODO: Beschreibe Interaktionen zwischen Komponenten]

`[TODO: Komponenteninteraktionsdiagramm einfügen]`

8.8.3 8.3 Security Enforcement Points

Sicherheitsdurchsetzungspunkte:

Enforcement Point	Location	Enforced Policy	Mechanism
[TODO: Punkt 1]	[TODO: Ort]	[TODO: Richtlinie]	[TODO: Mechanismus]
[TODO: Punkt 2]	[TODO: Ort]	[TODO: Richtlinie]	[TODO: Mechanismus]

8.9 9. Operational Modes

8.9.1 9.1 Normal Operation Mode

Normalbetriebsmodus: - Beschreibung: [TODO: Beschreibung] - Verfügbare Funktionen: [TODO: Funktionen] - Sicherheitsverhalten: [TODO: Sicherheitsverhalten]

8.9.2 9.2 Maintenance Mode

Wartungsmodus: - Beschreibung: [TODO: Beschreibung] - Verfügbare Funktionen: [TODO: Funktionen] - Sicherheitsverhalten: [TODO: Sicherheitsverhalten] - Zugriffskontrolle: [TODO: Zugriffskontrolle]

8.9.3 9.3 Secure State

Sicherer Zustand: - Definition: [TODO: Definition des sicheren Zustands] - Aufrechterhaltung: [TODO: Wie wird der sichere Zustand aufrechterhalten] - Wiederherstellung: [TODO: Wiederherstellung nach Fehler]

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter mit TOE-spezifischen Informationen 2. Erstelle detaillierte funktionale Architekturdiagramme 3. Dokumentiere alle Sicherheitsmechanismen vollständig 4. Überprüfe die Konsistenz mit dem physischen Umfang (Template 0100) 5. Stelle sicher, dass alle Sicherheitsfunktionen dokumentiert sind

ewpage

Chapter 9

TOE Interfaces

Dokument-ID: 0120
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

9.1 1. Interface Overview

9.1.1 1.1 Interface Categories

Der TOE bietet folgende Schnittstellenkategorien:

Category	Count	Description
User Interfaces	[TODO: Anzahl]	Schnittstellen für Endbenutzer
Administrative Interfaces	[TODO: Anzahl]	Schnittstellen für Administratoren
External Interfaces	[TODO: Anzahl]	Schnittstellen zu externen Systemen
Internal Interfaces	[TODO: Anzahl]	Schnittstellen zwischen TOE-Komponenten

9.1.2 1.2 Interface Architecture

[TODO: Beschreibe die Schnittstellenarchitektur]

`[TODO: Schnittstellenarchitekturdiagramm einfügen]`

9.2 2. User Interfaces

9.2.1 2.1 Graphical User Interface (GUI)

[TODO: GUI-Name]

Allgemeine Informationen: - Typ: Web-basiert / Desktop-Anwendung / Mobile App - Technologie: [TODO: z.B. HTML5, React, Qt, etc.] - Zugriff: [TODO: z.B. Browser, Native App] - Authentifizierung: [TODO: Authentifizierungsmethode]

Funktionen: - [TODO: Funktion 1]: [TODO: Beschreibung] - [TODO: Funktion 2]: [TODO: Beschreibung] - [TODO: Funktion 3]: [TODO: Beschreibung]

Sicherheitsmerkmale: - Session-Management: [TODO: Beschreibung] - Input-Validierung: [TODO: Beschreibung] - Output-Encoding: [TODO: Beschreibung] - CSRF-Schutz: [TODO: Beschreibung]

Benutzerrollen: | Role | Access Level | Available Functions | |——|————|————————| | [TODO: Rolle 1] | [TODO: Level] | [TODO: Funktionen] | | [TODO: Rolle 2] | [TODO: Level] | [TODO: Funktionen] |

9.2.2 2.2 Command Line Interface (CLI)

[TODO: CLI-Name]

Allgemeine Informationen: - Zugriff: [TODO: z.B. SSH, Lokale Konsole] - Shell: [TODO: z.B. Bash, PowerShell, Custom Shell] - Authentifizierung: [TODO: Authentifizierungsmethode]

Verfügbare Befehle: | Command | Syntax | Description | Required Privilege | |———|———|———————-|————————-| | [TODO: Befehl 1] | [TODO: Syntax] | [TODO: Beschreibung] | [TODO: Berechtigung] | | [TODO: Befehl 2] | [TODO: Syntax] | [TODO: Beschreibung] | [TODO: Berechtigung] | | [TODO: Befehl 3] | [TODO: Syntax] | [TODO: Beschreibung] | [TODO: Berechtigung] |

Sicherheitsmerkmale: - Befehlsvalidierung: [TODO: Beschreibung] - Audit-Logging: [TODO: Beschreibung] - Privilegientrennung: [TODO: Beschreibung]

9.2.3 2.3 Application Programming Interface (API)

[TODO: API-Name]

Allgemeine Informationen: - Typ: REST / SOAP / GraphQL / gRPC - Protokoll: HTTPS / HTTP / Custom - Authentifizierung: [TODO: z.B. OAuth 2.0, API Keys, JWT] - Autorisierung: [TODO: Autorisierungsmechanismus]

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

Sicherheitsmerkmale: - TLS-Verschlüsselung: [TODO: Version und Cipher Suites] - Rate Limiting: [TODO: Beschreibung] - Input-Validierung: [TODO: Beschreibung] - API-Versionierung: [TODO: Beschreibung]

API-Dokumentation: - Format: [TODO: z.B. OpenAPI/Swagger, WSDL] - Zugriff: [TODO: URL oder Speicherort]

9.3 3. Administrative Interfaces

9.3.1 3.1 Configuration Interface

[TODO: Konfigurationsschnittstelle]

Allgemeine Informationen: - Typ: GUI / CLI / API / Konfigurationsdatei - Zugriff: [TODO: Zugriffsmethode] - Authentifizierung: [TODO: Authentifizierungsmethode] - Autorisierung: [TODO: Erforderliche Berechtigung]

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

Sicherheitsmerkmale: - Konfigurationsvalidierung: [TODO: Beschreibung] - Änderungsaudit: [TODO: Beschreibung] - Rollback-Mechanismus: [TODO: Beschreibung]

9.3.2 3.2 Monitoring Interface

[TODO: Monitoring-Schnittstelle]

Allgemeine Informationen: - Typ: GUI / CLI / API - Protokoll: [TODO: z.B. SNMP, REST, Proprietary] - Authentifizierung: [TODO: Authentifizierungsmethode]

Überwachte Metriken: | Metric | Type | Unit | Threshold | Alert | |———|——|——|————|——-| | [TODO: Metrik 1] | Performance/Security/Availability | [TODO: Einheit] | [TODO: Schwellwert] | [TODO: Alarm] | | [TODO: Metrik 2] | Performance/Security/Availability | [TODO: Einheit] | [TODO: Schwellwert] | [TODO: Alarm] |

Sicherheitsmerkmale: - Zugriffskontrolle: [TODO: Beschreibung] - Datenintegrität: [TODO: Beschreibung]

9.3.3 3.3 Logging Interface

[TODO: Logging-Schnittstelle]

Allgemeine Informationen: - Typ: Syslog / File-based / Database / SIEM Integration - Protokoll: [TODO: z.B. Syslog, REST] - Format: [TODO: z.B. JSON, CEF, Plain Text]

Log-Kategorien: | Category | Events | Severity Levels | Retention | |———-|——|——————|————| | [TODO: Kategorie 1] | [TODO: Ereignisse] | [TODO: Levels] | [TODO: Aufbewahrung] | | [TODO: Kategorie 2] | [TODO: Ereignisse] | [TODO: Levels] | [TODO: Aufbewahrung] |

Sicherheitsmerkmale: - Log-Integrität: [TODO: Beschreibung] - Verschlüsselung: [TODO: Beschreibung] - Zugriffskontrolle: [TODO: Beschreibung]

9.3.4 3.4 Backup and Restore Interface

[TODO: Backup/Restore-Schnittstelle]

Allgemeine Informationen: - Typ: CLI / API / GUI - Authentifizierung: [TODO: Authentifizierungsmethode] - Autorisierung: [TODO: Erforderliche Berechtigung]

Funktionen: - Backup-Erstellung: [TODO: Beschreibung] - Backup-Wiederherstellung: [TODO: Beschreibung] - Backup-Verifikation: [TODO: Beschreibung]

Sicherheitsmerkmale: - Backup-Verschlüsselung: [TODO: Algorithmus] - Integritätsschutz: [TODO: Mechanismus] - Zugriffskontrolle: [TODO: Beschreibung]

9.4 4. External Interfaces

9.4.1 4.1 Network Interfaces

[TODO: Netzwerkschnittstelle 1]

Allgemeine Informationen: - Typ: Ethernet / Wi-Fi / Serial / etc. - Protokoll: [TODO: z.B. TCP/IP, UDP] - Port: [TODO: Port-Nummer] - Richtung: Inbound / Outbound / Bidirectional

Kommunikationspartner: | Partner | Purpose | Protocol | Security | |———|———|———-|———-| | [TODO: System 1] | [TODO: Zweck] | [TODO: Protokoll] | [TODO: Sicherheit] | | [TODO: System 2] | [TODO: Zweck] | [TODO: Protokoll] | [TODO: Sicherheit] |

Sicherheitsmerkmale: - Verschlüsselung: [TODO: z.B. TLS 1.3] - Authentifizierung: [TODO: Mechanismus] - Firewall-Regeln: [TODO: Beschreibung]

9.4.2 4.2 Database Interfaces

[TODO: Datenbankschnittstelle]

Allgemeine Informationen: - Datenbank-Typ: [TODO: z.B. PostgreSQL, MySQL, Oracle] - Verbindungsprotokoll: [TODO: z.B. JDBC, ODBC, Native] - Authentifizierung: [TODO: Authentifizierungsmethode]

Datenbankoperationen: | Operation | Tables | Purpose | Frequency | |————|———|———|———-| | [TODO: Operation 1] | [TODO: Tabellen] | [TODO: Zweck] | [TODO: Häufigkeit] | | [TODO: Operation 2] | [TODO: Tabellen] | [TODO: Zweck] | [TODO: Häufigkeit] |

Sicherheitsmerkmale: - Verbindungsverschlüsselung: [TODO: Beschreibung] - SQL-Injection-Schutz: [TODO: Beschreibung] - Zugriffskontrolle: [TODO: Beschreibung]

9.4.3 4.3 Directory Service Interfaces

[TODO: Directory-Service-Schnittstelle]

Allgemeine Informationen: - Typ: LDAP / Active Directory / Azure AD / etc. - Protokoll: [TODO: z.B. LDAPS, Kerberos] - Zweck: [TODO: z.B. Authentifizierung, Autorisierung]

Operationen: - Authentifizierung: [TODO: Beschreibung] - Attributabfrage: [TODO: Beschreibung] - Gruppenmitgliedschaft: [TODO: Beschreibung]

Sicherheitsmerkmale: - Verschlüsselung: [TODO: Beschreibung] - Zertifikatsvalidierung: [TODO: Beschreibung]

9.4.4 4.4 External System Interfaces

[TODO: Externes System 1]

Allgemeine Informationen: - System: [TODO: Systemname] - Zweck: [TODO: Integrationszweck] - Protokoll: [TODO: Kommunikationsprotokoll] - Datenformat: [TODO: z.B. JSON, XML, Binary]

Datenaustausch: | Data Type | Direction | Format | Frequency | Security | |————|————|————|————|————-| | [TODO: Datentyp 1] | In/Out/Both | [TODO: Format] | [TODO: Häufigkeit] | [TODO: Sicherheit] | | [TODO: Datentyp 2] | In/Out/Both | [TODO: Format] | [TODO: Häufigkeit] | [TODO: Sicherheit] |

Sicherheitsmerkmale: - Authentifizierung: [TODO: Mechanismus] - Verschlüsselung: [TODO: Mechanismus] - Datenvalidierung: [TODO: Beschreibung]

9.5 5. Internal Interfaces

9.5.1 5.1 Inter-Component Interfaces

[TODO: Interne Schnittstelle 1]

Allgemeine Informationen: - Quelle: [TODO: Quellkomponente] - Ziel: [TODO: Zielkomponente] - Typ: Function Call / IPC / Message Queue / etc. - Protokoll: [TODO: Internes Protokoll]

Datenaustausch: | Data Type | Purpose | Format | Security | |————|————|————|————-| | [TODO: Datentyp 1] | [TODO: Zweck] | [TODO: Format] | [TODO: Sicherheit] | | [TODO: Datentyp 2] | [TODO: Zweck] | [TODO: Format] | [TODO: Sicherheit] |

Sicherheitsmerkmale: - Zugriffskontrolle: [TODO: Beschreibung] - Datenvalidierung: [TODO: Beschreibung]

9.5.2 5.2 Module Interfaces

[TODO: Modulschnittstelle 1]

Allgemeine Informationen: - Modul: [TODO: Modulname] - Typ: API / Library / Service - Programmiersprache: [TODO: Sprache]

Bereitgestellte Funktionen: | Function | Parameters | Return Type | Description | |————-|————|————-|————-| | [TODO: Funktion 1] | [TODO: Parameter] | [TODO: Rückgabetyp] | [TODO: Beschreibung] | | [TODO: Funktion 2] | [TODO: Parameter] | [TODO: Rückgabetyp] | [TODO: Beschreibung] |

Sicherheitsmerkmale: - Input-Validierung: [TODO: Beschreibung] - Error-Handling: [TODO: Beschreibung]

9.6 6. Interface Security

9.6.1 6.1 Authentication Mechanisms

Schnittstellenauthentifizierung:

Interface	Authentication Method	Credential Type	Multi-Factor
[TODO: Schnittstelle 1]	[TODO: Methode]	[TODO: Credential-Typ]	Yes/No
[TODO: Schnittstelle 2]	[TODO: Methode]	[TODO: Credential-Typ]	Yes/No

9.6.2 6.2 Authorization Mechanisms

Schnittstellenautorisierung:

Interface	Authorization Model	Enforcement Point	Policy
[TODO: Schnittstelle 1]	[TODO: Modell]	[TODO: Punkt]	[TODO: Richtlinie]
[TODO: Schnittstelle 2]	[TODO: Modell]	[TODO: Punkt]	[TODO: Richtlinie]

9.6.3 6.3 Encryption and Integrity

Verschlüsselung und Integrität:

Interface	Encryption	Algorithm	Integrity Protection
[TODO: Schnittstelle 1]	Yes/No	[TODO: Algorithmus]	[TODO: Mechanismus]
[TODO: Schnittstelle 2]	Yes/No	[TODO: Algorithmus]	[TODO: Mechanismus]

9.6.4 6.4 Input Validation

Eingabevalidierung:

Interface	Validation Type	Sanitization	Error Handling
[TODO: Schnittstelle 1]	[TODO: Typ]	[TODO: Sanitization]	[TODO: Error-Handling]
[TODO: Schnittstelle 2]	[TODO: Typ]	[TODO: Sanitization]	[TODO: Error-Handling]

9.7 7. Interface Protocols

9.7.1 7.1 Communication Protocols

Verwendete Kommunikationsprotokolle:

Protocol	Version	Purpose	Security Features
[TODO: Protokoll 1]	[TODO: Version]	[TODO: Zweck]	[TODO: Sicherheitsmerkmale]
[TODO: Protokoll 2]	[TODO: Version]	[TODO: Zweck]	[TODO: Sicherheitsmerkmale]

9.7.2 7.2 Data Formats

Verwendete Datenformate:

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

9.7.3 7.3 Error Handling

Fehlerbehandlung an Schnittstellen:

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

9.8 8. Interface Documentation

9.8.1 8.1 User Interface Documentation

- [TODO: GUI-Benutzerhandbuch]: [TODO: Speicherort]
- [TODO: CLI-Referenz]: [TODO: Speicherort]
- [TODO: API-Dokumentation]: [TODO: Speicherort]

9.8.2 8.2 Administrator Interface Documentation

- [TODO: Konfigurationshandbuch]: [TODO: Speicherort]
- [TODO: Monitoring-Handbuch]: [TODO: Speicherort]
- [TODO: Logging-Handbuch]: [TODO: Speicherort]

9.8.3 8.3 Developer Interface Documentation

- [TODO: API-Spezifikation]: [TODO: Speicherort]
- [TODO: Integrationshandbuch]: [TODO: Speicherort]
- [TODO: Protokolldokumentation]: [TODO: Speicherort]

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter mit TOE-spezifischen Informationen 2. Erstelle detaillierte Schnittstellendiagramme 3. Dokumentiere alle Sicherheitsmechanismen für jede Schnittstelle 4. Überprüfe die Konsistenz mit der TOE-Architektur (Template 0130) 5. Stelle sicher, dass alle Schnittstellen vollständig dokumentiert sind

ewpage

Chapter 10

TOE Architecture

Dokument-ID: 0130
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

10.1 1. Architecture Overview

10.1.1 1.1 High-Level Architecture

[TODO: Beschreibe die High-Level-Architektur des TOE]

Der TOE folgt einer [TODO: z.B. geschichteten, modularen, serviceorientierten] Architektur mit folgenden Hauptkomponenten:

`[TODO: High-Level-Architekturdiagramm einfügen]`

10.1.2 1.2 Architecture Style

Architekturstil: [TODO: z.B. Layered, Microservices, Client-Server, Event-Driven]

Begründung: [TODO: Erkläre, warum dieser Architekturstil gewählt wurde]

10.1.3 1.3 Architecture Principles

Leitende Architekturprinzipien: 1. [TODO: Prinzip 1, z.B. Separation of Concerns] 2. [TODO: Prinzip 2, z.B. Least Privilege] 3. [TODO: Prinzip 3, z.B. Defense in Depth] 4. [TODO: Prinzip 4, z.B. Fail Secure] 5. [TODO: Prinzip 5, z.B. Simplicity]

10.2 2. Layered Architecture

10.2.1 2.1 Architecture Layers

Der TOE ist in folgende Schichten organisiert:

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

10.2.2 2.2 Layer Interactions

[TODO: Beschreibe, wie Schichten miteinander interagieren]

Interaktionsregeln: - [TODO: Regel 1, z.B. Schichten dürfen nur mit benachbarten Schichten kommunizieren] - [TODO: Regel 2, z.B. Keine Umgehung von Schichten] - [TODO: Regel 3]

`[TODO: Schichteninteraktionsdiagramm einfügen]`

10.2.3 2.3 Layer Details

10.2.3.1 Layer: [TODO: Schichtname 1]

Zweck: [TODO: Beschreibung]

Komponenten: - [TODO: Komponente 1]: [TODO: Beschreibung] - [TODO: Komponente 2]: [TODO: Beschreibung]

Schnittstellen: - Nach oben: [TODO: Bereitgestellte Schnittstellen] - Nach unten: [TODO: Verwendete Schnittstellen]

Sicherheitsverantwortlichkeiten: - [TODO: Sicherheitsverantwortlichkeit 1] - [TODO: Sicherheitsverantwortlichkeit 2]

10.2.3.2 Layer: [TODO: Schichtname 2]

[TODO: Details wie oben]

10.3 3. Component Architecture

10.3.1 3.1 Component Overview

Hauptkomponenten des TOE:

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

10.3.2 3.2 Component Relationships

[TODO: Beschreibe Beziehungen zwischen Komponenten]

`[TODO: Komponentenbeziehungsdiagramm einfügen]`

10.3.3 3.3 Component Details

10.3.3.1 Component: [TODO: Komponentenname 1]

Allgemeine Informationen: - ID: [TODO: COMP-001] - Typ: [TODO: Core/Security/Support] - Schicht: [TODO: Schicht] - Technologie: [TODO: z.B. Java, C++, Python]

Zweck: [TODO: Beschreibe den Zweck dieser Komponente]

Verantwortlichkeiten: - [TODO: Verantwortlichkeit 1] - [TODO: Verantwortlichkeit 2] - [TODO: Verantwortlichkeit 3]

Bereitgestellte Schnittstellen: | Interface | Type | Consumers | |————|——|————| | [TODO: Interface 1] | [TODO: Typ] | [TODO: Konsumenten] | | [TODO: Interface 2] | [TODO: Typ] | [TODO: Konsumenten] |

Verwendete Schnittstellen: | Interface | Provider | Purpose | |————|———-|———| | [TODO: Interface 1] | [TODO: Anbieter] | [TODO: Zweck] | | [TODO: Interface 2] | [TODO: Anbieter] | [TODO: Zweck] |

Abhängigkeiten: - [TODO: Abhängigkeit 1] - [TODO: Abhängigkeit 2]

Sicherheitsrelevanz: [TODO: Beschreibe die Sicherheitsrelevanz dieser Komponente]

10.3.3.2 Component: [TODO: Komponentenname 2]

[TODO: Details wie oben]

10.4 4. Security Architecture

10.4.1 4.1 Security Architecture Overview

[TODO: Beschreibe die Sicherheitsarchitektur des TOE]

`[TODO: Sicherheitsarchitekturdiagramm einfügen]`

10.4.2 4.2 Trust Boundaries

Vertrauensgrenzen im TOE:

Boundary	Description	Protection Mechanism
[TODO: Grenze 1]	[TODO: Beschreibung]	[TODO: Schutzmechanismus]
[TODO: Grenze 2]	[TODO: Beschreibung]	[TODO: Schutzmechanismus]
[TODO: Grenze 3]	[TODO: Beschreibung]	[TODO: Schutzmechanismus]

`[TODO: Vertrauensgrenzendiagramm einfügen]`

10.4.3 4.3 Security Zones

Sicherheitszonen:

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

10.4.4 4.4 Security Enforcement Points

Sicherheitsdurchsetzungspunkte:

Enforcement Point	Location	Enforced Policies	Mechanism
[TODO: Punkt 1]	[TODO: Ort]	[TODO: Richtlinien]	[TODO: Mechanismus]
[TODO: Punkt 2]	[TODO: Ort]	[TODO: Richtlinien]	[TODO: Mechanismus]

10.4.5 4.5 Security Functions Mapping

Zuordnung von Sicherheitsfunktionen zu Komponenten:

Security Function	Implementing Component	Layer	Mechanism
[TODO: Funktion 1]	[TODO: Komponente]	[TODO: Schicht]	[TODO: Mechanismus]
[TODO: Funktion 2]	[TODO: Komponente]	[TODO: Schicht]	[TODO: Mechanismus]

10.5 5. Data Architecture

10.5.1 5.1 Data Flow Architecture

[TODO: Beschreibe die Datenflussarchitektur]

`[TODO: Datenflussarchitekturdiagramm einfügen]`

10.5.2 5.2 Data Storage Architecture

Datenspeicherarchitektur:

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

10.5.3 5.3 Data Protection Architecture

Datenschutzarchitektur:

Data Type	Classification	Protection Mechanism	Location
[TODO: Datentyp 1]	Public/Internal/Confidential/Secret	[TODO: Schutzmechanismus]	[TODO: Ort]
[TODO: Datentyp 2]	Public/Internal/Confidential/Secret	[TODO: Schutzmechanismus]	[TODO: Ort]

10.5.4 5.4 Data Flow Paths

Kritische Datenflusspfade:

[TODO: Datenflusspfad 1] - Quelle: [TODO: Quelle] - Ziel: [TODO: Ziel] - Durchlaufene Komponenten: [TODO: Komponenten] - Sicherheitsmaßnahmen: [TODO: Maßnahmen]

[TODO: Datenflusspfad 2] - [TODO: Details]

10.6 6. Deployment Architecture

10.6.1 6.1 Deployment Overview

[TODO: Beschreibe die Deployment-Architektur]

`[TODO: Deployment-Diagramm einfügen]`

10.6.2 6.2 Deployment Scenarios

Unterstützte Deployment-Szenarien:

Szenario 1: [TODO: Szenarioname] - Beschreibung: [TODO: Beschreibung] - Komponenten: [TODO: Deployierte Komponenten] - Infrastruktur: [TODO: Erforderliche Infrastruktur] - Sicherheitsaspekte: [TODO: Sicherheitsaspekte]

Szenario 2: [TODO: Szenarioname] - [TODO: Details]

10.6.3 6.3 Physical Deployment

Physische Deployment-Topologie:

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

10.6.4 6.4 Network Architecture

Netzwerkarchitektur:

`[TODO: Netzwerkarchitekturdiagramm einfügen]`

Netzwerksegmente: | Segment | Purpose | Components | Security | |———|———|————|———-| | [TODO: Segment 1] | [TODO: Zweck] | [TODO: Komponenten] | [TODO: Sicherheit] | | [TODO: Segment 2] | [TODO: Zweck] | [TODO: Komponenten] | [TODO: Sicherheit] |

10.7 7. Runtime Architecture

10.7.1 7.1 Process Architecture

Prozessarchitektur:

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

10.7.2 7.2 Thread Architecture

Thread-Modell: [TODO: Beschreibe das Threading-Modell des TOE]

10.7.3 7.3 Memory Architecture

Speicherarchitektur: - Heap-Management: [TODO: Beschreibung] - Stack-Management: [TODO: Beschreibung] - Speicherschutz: [TODO: Mechanismen]

10.7.4 7.4 Execution Flow

Ausführungsfluss:

`[TODO: Ausführungsflussdiagramm einfügen]`

10.8 8. Integration Architecture

10.8.1 8.1 External System Integration

Integration mit externen Systemen:

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

10.8.2 8.2 Integration Patterns

Verwendete Integrationsmuster: - [TODO: Muster 1, z.B. Request-Response] - [TODO: Muster 2, z.B. Publish-Subscribe] - [TODO: Muster 3, z.B. Message Queue]

10.8.3 8.3 Integration Security

Sicherheit bei Integration: - Authentifizierung: [TODO: Mechanismus] - Autorisierung: [TODO: Mechanismus] - Verschlüsselung: [TODO: Mechanismus] - Datenvalidierung: [TODO: Mechanismus]

10.9 9. Scalability and Performance Architecture

10.9.1 9.1 Scalability Design

Skalierbarkeitsdesign: - Horizontale Skalierung: [TODO: Beschreibung] - Vertikale Skalierung: [TODO: Beschreibung] - Lastverteilung: [TODO: Mechanismus]

10.9.2 9.2 Performance Considerations

Performance-Überlegungen: - Caching-Strategie: [TODO: Beschreibung] - Datenbankoptimierung: [TODO: Beschreibung] - Netzwerkoptimierung: [TODO: Beschreibung]

10.9.3 9.3 Resource Management

Ressourcenverwaltung: - CPU-Verwaltung: [TODO: Beschreibung] - Speicherverwaltung: [TODO: Beschreibung] - I/O-Verwaltung: [TODO: Beschreibung]

10.10 10. Resilience Architecture

10.10.1 10.1 Fault Tolerance

Fehlertoleranz: - Redundanz: [TODO: Beschreibung] - Failover: [TODO: Mechanismus] - Recovery: [TODO: Mechanismus]

10.10.2 10.2 Error Handling

Fehlerbehandlung: - Fehlererkennungsstrategie: [TODO: Beschreibung] - Fehlerbehandlungsstrategie: [TODO: Beschreibung] - Fehlerprotokollierung: [TODO: Beschreibung]

10.10.3 10.3 Availability Design

Verfügbarkeitsdesign: - Ziel-Verfügbarkeit: [TODO: z.B. 99.9%] - Hochverfügbarkeitsmechanismen: [TODO: Beschreibung] - Wartungsfenster: [TODO: Beschreibung]

10.11 11. Architecture Decisions

10.11.1 11.1 Key Architecture Decisions

Wichtige Architekturentscheidungen:

Entscheidung 1: [TODO: Entscheidungstitel] - Kontext: [TODO: Kontext] - Entscheidung: [TODO: Getroffene Entscheidung] - Alternativen: [TODO: Betrachtete Alternativen] - Begründung: [TODO: Begründung] - Konsequenzen: [TODO: Konsequenzen]

Entscheidung 2: [TODO: Entscheidungstitel] - [TODO: Details]

10.11.2 11.2 Trade-offs

Architektur-Trade-offs: - [TODO: Trade-off 1, z.B. Performance vs. Security] - [TODO: Trade-off 2, z.B. Complexity vs. Maintainability] - [TODO: Trade-off 3]

10.11.3 11.3 Constraints

Architektur-Constraints: - Technische Constraints: [TODO: Liste] - Organisatorische Constraints: [TODO: Liste] - Regulatorische Constraints: [TODO: Liste]

10.12 12. Architecture Documentation

10.12.1 12.1 Architecture Views

Verfügbare Architekturansichten: - Logische Ansicht: [TODO: Speicherort] - Prozessansicht: [TODO: Speicherort] - Entwicklungsansicht: [TODO: Speicherort] - Physische Ansicht: [TODO: Speicherort] - Szenarioansicht: [TODO: Speicherort]

10.12.2 12.2 Architecture Models

Architekturmodelle: - UML-Modelle: [TODO: Speicherort] - C4-Modelle: [TODO: Speicherort] - Datenmodelle: [TODO: Speicherort]

10.12.3 12.3 Architecture Standards

Verwendete Architekturstandards: - [TODO: Standard 1] - [TODO: Standard 2] - [TODO: Standard 3]

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter mit TOE-spezifischen Informationen 2. Erstelle alle erforderlichen Architekturdiagramme 3. Dokumentiere alle Architekturentscheidungen vollständig 4. Überprüfe die Konsistenz mit anderen TOE-Beschreibungsdokumenten 5. Stelle sicher, dass die Sicherheitsarchitektur vollständig dokumentiert ist

ewpage

Chapter 11

TOE Lifecycle

Dokument-ID: 0140
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

11.1 1. Lifecycle Overview

11.1.1 1.1 Lifecycle Phases

Der TOE-Lebenszyklus umfasst folgende Phasen:

Phase	Duration	Responsible	Security Focus
[TODO: Phase 1]	[TODO: Dauer]	[TODO: Verantwortlich]	[TODO: Sicherheitsfokus]
[TODO: Phase 2]	[TODO: Dauer]	[TODO: Verantwortlich]	[TODO: Sicherheitsfokus]
[TODO: Phase 3]	[TODO: Dauer]	[TODO: Verantwortlich]	[TODO: Sicherheitsfokus]
[TODO: Phase 4]	[TODO: Dauer]	[TODO: Verantwortlich]	[TODO: Sicherheitsfokus]

11.1.2 1.2 Lifecycle Diagram

[TODO: Erstelle ein Diagramm, das alle Lebenszyklusphasen und Übergänge zeigt]

`[TODO: Lebenszyklusdiagramm einfügen]`

11.1.3 1.3 Lifecycle Roles

Rollen im TOE-Lebenszyklus:

Role	Responsibilities	Phases
[TODO: Rolle 1]	[TODO: Verantwortlichkeiten]	[TODO: Phasen]
[TODO: Rolle 2]	[TODO: Verantwortlichkeiten]	[TODO: Phasen]
[TODO: Rolle 3]	[TODO: Verantwortlichkeiten]	[TODO: Phasen]

11.2 2. Development Phase

11.2.1 2.1 Development Process

Entwicklungsprozess: - Methodik: [TODO: z.B. Agile, Waterfall, DevSecOps] - Entwicklungsumgebung: [TODO: Beschreibung] - Versionskontrolle: [TODO: z.B. Git, SVN] - Build-System: [TODO: z.B. Maven, Gradle, Make]

11.2.2 2.2 Security in Development

Sicherheitsmaßnahmen während der Entwicklung:

Secure Coding Practices: - Coding-Standards: [TODO: z.B. CERT, MISRA] - Code-Reviews: [TODO: Prozess] - Static Analysis: [TODO: Tools und Prozess] - Security Training: [TODO: Schulungsprogramm]

Security Testing: - Unit Testing: [TODO: Beschreibung] - Integration Testing: [TODO: Beschreibung] - Security Testing: [TODO: z.B. SAST, DAST, Penetration Testing] - Vulnerability Scanning: [TODO: Tools und Prozess]

11.2.3 2.3 Configuration Management

Konfigurationsmanagement: - CM-System: [TODO: System] - Baseline-Management: [TODO: Prozess] - Change Control: [TODO: Prozess] - Release Management: [TODO: Prozess]

11.2.4 2.4 Development Documentation

Entwicklungsdokumentation: - Requirements Specification: [TODO: Speicherort] - Design Documentation: [TODO: Speicherort] - Implementation Documentation: [TODO: Speicherort] - Test Documentation: [TODO: Speicherort]

11.2.5 2.5 Development Environment Security

Sicherheit der Entwicklungsumgebung: - Access Control: [TODO: Zugriffskontrollmechanismen] - Network Segmentation: [TODO: Netzwerksegmentierung] - Audit Logging: [TODO: Audit-Protokollierung] - Backup: [TODO: Backup-Strategie]

11.3 3. Build and Integration Phase

11.3.1 3.1 Build Process

Build-Prozess: - Build-System: [TODO: System] - Build-Automatisierung: [TODO: CI/CD-Pipeline] - Build-Umgebung: [TODO: Beschreibung] - Build-Verifikation: [TODO: Verifikationsmechanismen]

11.3.2 3.2 Build Security

Build-Sicherheit: - Build-Integrität: [TODO: Integritätsschutz] - Dependency Management: [TODO: Verwaltung von Abhängigkeiten] - Supply Chain Security: [TODO: Sicherheitsmaßnahmen] - Build Reproducibility: [TODO: Reproduzierbarkeit]

11.3.3 3.3 Integration Testing

Integrationstests: - Test-Strategie: [TODO: Strategie] - Test-Umgebung: [TODO: Umgebung] - Test-Automatisierung: [TODO: Automatisierung] - Test-Dokumentation: [TODO: Dokumentation]

11.3.4 3.4 Quality Assurance

Qualitätssicherung: - QA-Prozess: [TODO: Prozess] - Code Coverage: [TODO: Ziel-Coverage] - Performance Testing: [TODO: Performance-Tests] - Security Validation: [TODO: Sicherheitsvalidierung]

11.4 4. Delivery Phase

11.4.1 4.1 Delivery Process

Lieferprozess: - Delivery Method: [TODO: z.B. Download, Physical Media, Pre-installed] - Packaging: [TODO: Verpackung] - Distribution Channels: [TODO: Vertriebskanäle] - Delivery Timeline: [TODO: Zeitplan]

11.4.2 4.2 Delivery Security

Liefersicherheit:

Integrity Protection: - Digital Signature: [TODO: Signaturalgorithmus und Schlüssel] - Checksums: [TODO: Hash-Algorithmus] - Tamper-Evident Packaging: [TODO: Manipulationssichere Verpackung]

Authenticity Verification: - Certificate Chain: [TODO: Zertifikatskette] - Verification Process: [TODO: Verifikationsprozess] - Public Key Distribution: [TODO: Verteilung öffentlicher Schlüssel]

11.4.3 4.3 Delivery Documentation

Lieferdokumentation: - Release Notes: [TODO: Speicherort] - Installation Guide: [TODO: Speicherort] - User Documentation: [TODO: Speicherort] - Security Guide: [TODO: Speicherort]

11.4.4 4.4 Delivery Verification

Lieferverifikation: - Verification Steps: [TODO: Verifikationsschritte] - Verification Tools: [TODO: Tools] - Verification Documentation: [TODO: Dokumentation]

11.5 5. Installation Phase

11.5.1 5.1 Installation Process

Installationsprozess: - Installation Method: [TODO: z.B. Automated, Manual, Hybrid] - Installation Steps: [TODO: Schritte] - Installation Time: [TODO: Geschätzte Zeit] - Prerequisites: [TODO: Voraussetzungen]

11.5.2 5.2 Secure Installation

Sichere Installation:

Pre-Installation: - System Requirements Verification: [TODO: Verifikation] - Security Prerequisites: [TODO: Sicherheitsvoraussetzungen] - Backup Existing System: [TODO: Backup-Prozess]

During Installation: - Integrity Verification: [TODO: Integritätsprüfung] - Secure Configuration: [TODO: Sichere Konfiguration] - Credential Setup: [TODO: Credential-Einrichtung] - Security Hardening: [TODO: Härtungsmaßnahmen]

Post-Installation: - Installation Verification: [TODO: Verifikation] - Security Testing: [TODO: Sicherheitstests] - Documentation: [TODO: Dokumentation]

11.5.3 5.3 Initial Configuration

Initiale Konfiguration: - Configuration Parameters: [TODO: Parameter] - Security Settings: [TODO: Sicherheitseinstellungen] - Network Configuration: [TODO: Netzwerkkonfiguration] - User Setup: [TODO: Benutzereinrichtung]

11.5.4 5.4 Installation Validation

Installationsvalidierung: - Functional Testing: [TODO: Funktionstests] - Security Validation: [TODO: Sicherheitsvalidierung] - Performance Baseline: [TODO: Performance-Baseline] - Documentation: [TODO: Dokumentation]

11.6 6. Operation Phase

11.6.1 6.1 Operational Procedures

Betriebsverfahren: - Startup Procedures: [TODO: Startverfahren] - Shutdown Procedures: [TODO: Herunterfahrverfahren] - Backup Procedures: [TODO: Backup-Verfahren] - Monitoring Procedures: [TODO: Überwachungsverfahren]

11.6.2 6.2 Secure Operation

Sicherer Betrieb:

Access Control: - User Management: [TODO: Benutzerverwaltung] - Privilege Management: [TODO: Berechtigungsverwaltung] - Authentication: [TODO: Authentifizierung] - Authorization: [TODO: Autorisierung]

Monitoring and Logging: - Security Monitoring: [TODO: Sicherheitsüberwachung] - Audit Logging: [TODO: Audit-Protokollierung] - Log Review: [TODO: Log-Überprüfung] - Incident Detection: [TODO: Vorfallserkennung]

Configuration Management: - Configuration Baseline: [TODO: Konfigurations-Baseline] - Change Management: [TODO: Änderungsmanagement] - Configuration Audits: [TODO: Konfigurationsaudits]

11.6.3 6.3 Operational Modes

Betriebsmodi:

Normal Operation Mode: - Description: [TODO: Beschreibung] - Available Functions: [TODO: Verfügbare Funktionen] - Security Behavior: [TODO: Sicherheitsverhalten]

Maintenance Mode: - Description: [TODO: Beschreibung] - Access Control: [TODO: Zugriffskontrolle] - Security Restrictions: [TODO: Sicherheitseinschränkungen]

Emergency Mode: - Description: [TODO: Beschreibung] - Activation Criteria: [TODO: Aktivierungskriterien] - Security Measures: [TODO: Sicherheitsmaßnahmen]

11.6.4 6.4 Operational Documentation

Betriebsdokumentation: - Operations Manual: [TODO: Speicherort] - Security Operations Guide: [TODO: Speicherort] - Troubleshooting Guide: [TODO: Speicherort] - Incident Response Plan: [TODO: Speicherort]

11.7 7. Maintenance Phase

11.7.1 7.1 Maintenance Types

Wartungstypen:

Corrective Maintenance: - Bug Fixes: [TODO: Prozess] - Security Patches: [TODO: Prozess] - Emergency Updates: [TODO: Prozess]

Preventive Maintenance: - Regular Updates: [TODO: Zeitplan] - Security Hardening: [TODO: Maßnahmen] - Performance Optimization: [TODO: Maßnahmen]

Adaptive Maintenance: - Feature Updates: [TODO: Prozess] - Configuration Changes: [TODO: Prozess] - Integration Updates: [TODO: Prozess]

11.7.2 7.2 Secure Maintenance

Sichere Wartung:

Update Process: - Update Verification: [TODO: Verifikation] - Backup Before Update: [TODO: Backup-Prozess] - Update Testing: [TODO: Testprozess] - Rollback Capability: [TODO: Rollback-Mechanismus]

Maintenance Access: - Access Control: [TODO: Zugriffskontrolle] - Authentication: [TODO: Authentifizierung] - Audit Logging: [TODO: Audit-Protokollierung] - Session Management: [TODO: Sitzungsverwaltung]

11.7.3 7.3 Patch Management

Patch-Management: - Patch Assessment: [TODO: Bewertungsprozess] - Patch Testing: [TODO: Testprozess] - Patch Deployment: [TODO: Deployment-Prozess] - Patch Verification: [TODO: Verifikation]

11.7.4 7.4 Maintenance Documentation

Wartungsdokumentation: - Maintenance Log: [TODO: Speicherort] - Change Records: [TODO: Speicherort] - Test Results: [TODO: Speicherort] - Incident Reports: [TODO: Speicherort]

11.8 8. Monitoring and Incident Response

11.8.1 8.1 Continuous Monitoring

Kontinuierliche Überwachung: - Monitoring Scope: [TODO: Überwachungsumfang] - Monitoring Tools: [TODO: Tools] - Monitoring Frequency: [TODO: Häufigkeit] - Alert Thresholds: [TODO: Alarmschwellen]

11.8.2 8.2 Incident Response

Vorfallreaktion: - Incident Detection: [TODO: Erkennungsmechanismen] - Incident Classification: [TODO: Klassifizierung] - Incident Response Process: [TODO: Reaktionsprozess] - Incident Documentation: [TODO: Dokumentation]

11.8.3 8.3 Security Events

Sicherheitsereignisse:

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

11.8.4 8.4 Forensics and Investigation

Forensik und Untersuchung: - Evidence Collection: [TODO: Beweissammlung] - Evidence Preservation: [TODO: Beweissicherung] - Investigation Process: [TODO: Untersuchungsprozess] - Reporting: [TODO: Berichterstattung]

11.9 9. Decommissioning Phase

11.9.1 9.1 Decommissioning Process

Außerbetriebnahmeprozess: - Decommissioning Planning: [TODO: Planung] - Decommissioning Steps: [TODO: Schritte] - Decommissioning Timeline: [TODO: Zeitplan] - Decommissioning Verification: [TODO: Verifikation]

11.9.2 9.2 Secure Decommissioning

Sichere Außerbetriebnahme:

Data Sanitization: - Data Identification: [TODO: Datenidentifikation] - Sanitization Method: [TODO: z.B. Overwriting, Degaussing, Physical Destruction] - Sanitization Verification: [TODO: Verifikation] - Sanitization Documentation: [TODO: Dokumentation]

Key Destruction: - Key Identification: [TODO: Schlüsselidentifikation] - Destruction Method: [TODO: Vernichtungsmethode] - Destruction Verification: [TODO: Verifikation] - Destruction Documentation: [TODO: Dokumentation]

Configuration Removal: - Configuration Backup: [TODO: Konfigurations-Backup] - Configuration Removal: [TODO: Entfernung] - Verification: [TODO: Verifikation]

11.9.3 9.3 Asset Disposal

Asset-Entsorgung: - Hardware Disposal: [TODO: Hardware-Entsorgung] - Software Removal: [TODO: Software-Entfernung] - Documentation Disposal: [TODO: Dokumentationsentsorgung] - Certificate Revocation: [TODO: Zertifikatswiderruf]

11.9.4 9.4 Decommissioning Documentation

Außerbetriebnahme-Dokumentation: - Decommissioning Plan: [TODO: Speicherort] - Sanitization Records: [TODO: Speicherort] - Disposal Records: [TODO: Speicherort] - Completion Certificate: [TODO: Speicherort]

11.10 10. Lifecycle Security Controls

11.10.1 10.1 Security Controls by Phase

Sicherheitskontrollen nach Phase:

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

11.10.2 10.2 Continuous Security

Kontinuierliche Sicherheit: - Security Assessments: [TODO: Bewertungen] - Vulnerability Management: [TODO: Schwachstellenmanagement] - Compliance Monitoring: [TODO: Compliance-Überwachung] - Security Updates: [TODO: Sicherheitsupdates]

11.10.3 10.3 Lifecycle Audits

Lebenszyklus-Audits: - Audit Frequency: [TODO: Häufigkeit] - Audit Scope: [TODO: Umfang] - Audit Process: [TODO: Prozess] - Audit Documentation: [TODO: Dokumentation]

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter mit TOE-spezifischen Informationen 2. Erstelle detaillierte Prozessdiagramme für jede Lebenszyklusphase 3. Dokumentiere alle Sicherheitsmaßnahmen vollständig 4. Überprüfe die Konsistenz mit anderen TOE-Beschreibungsdokumenten 5. Stelle sicher, dass alle Phasen und Übergänge dokumentiert sind

ewpage

Chapter 12

Security Problem Definition

Dokument-ID: 0200
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

12.1 1. Security Problem Overview

12.1.1 1.1 Purpose

Dieses Dokument definiert das Sicherheitsproblem, das der TOE lösen soll. Es beschreibt: - **Threats (Bedrohungen)**: Potenzielle Angriffe und Sicherheitsverletzungen - **Organizational Security Policies (OSPs)**: Sicherheitsrichtlinien, die eingehalten werden müssen - **Assumptions (Annahmen)**: Erwartungen an die Betriebsumgebung

12.1.2 1.2 Security Problem Context

Anwendungskontext: [TODO: Beschreibe den Kontext, in dem der TOE eingesetzt wird]

Sicherheitsrelevante Faktoren: - [TODO: Faktor 1] - [TODO: Faktor 2] - [TODO: Faktor 3]

12.1.3 1.3 Security Problem Scope

Im Scope: - [TODO: Was wird durch die Sicherheitsproblem-Definition abgedeckt]

Außerhalb des Scope: - [TODO: Was wird nicht abgedeckt]

12.2 2. Assets

12.2.1 2.1 Asset Identification

Schützenswerte Assets:

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

12.2.2 2.2 Asset Classification

Daten-Assets: - [TODO: Daten-Asset 1]: [TODO: Klassifizierung und Schutzbedarf] - [TODO: Daten-Asset 2]: [TODO: Klassifizierung und Schutzbedarf]

Service-Assets: - [TODO: Service-Asset 1]: [TODO: Verfügbarkeitsanforderungen] - [TODO: Service-Asset 2]: [TODO: Verfügbarkeitsanforderungen]

Funktions-Assets: - [TODO: Funktions-Asset 1]: [TODO: Integritätsanforderungen] - [TODO: Funktions-Asset 2]: [TODO: Integritätsanforderungen]

12.2.3 2.3 Asset Dependencies

[TODO: Beschreibe Abhängigkeiten zwischen Assets]

`[TODO: Asset-Abhängigkeitsdiagramm einfügen]`

12.3 3. Threat Agents

12.3.1 3.1 Threat Agent Profiles

Identifizierte Bedrohungsagenten:

Agent ID	Agent Type	Motivation	Capability	Resources	Description
[TODO: TA.001]	[TODO: z.B. Insider, External Attacker]	[TODO: Motivation]	High/Medium/Low	High/Medium/Low	[TODO: Beschreibung]
[TODO: TA.002]	[TODO: Typ]	[TODO: Motivation]	High/Medium/Low	High/Medium/Low	[TODO: Beschreibung]

12.3.2 3.2 Threat Agent Capabilities

[TODO: Bedrohungsagent 1] - **Fähigkeiten**: [TODO: z.B. Netzwerkzugriff, physischer Zugriff, Insider-Wissen] - **Ressourcen**: [TODO: z.B. Zeit, Budget, Werkzeuge] - **Motivation**: [TODO: z.B. finanzieller Gewinn, Sabotage, Spionage] - **Angriffsvektoren**: [TODO: Mögliche Angriffswege]

[TODO: Bedrohungsagent 2] - [TODO: Details]

12.3.3 3.3 Attack Potential

Bewertung des Angriffspotenzials:

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

Identifizierte Bedrohungen:

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

12.4.2 4.2 Threat Details

12.4.2.1 T.001: [TODO: Bedrohungsname]

Beschreibung: [TODO: Detaillierte Beschreibung der Bedrohung]

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

Bedrohungsagent: - [TODO: TA.001]

Angriffsszenario: 1. [TODO: Schritt 1] 2. [TODO: Schritt 2] 3. [TODO: Schritt 3]

Auswirkungen: - Vertraulichkeit: [TODO: High/Medium/Low/None] - Integrität: [TODO: High/Medium/Low/None] - Verfügbarkeit: [TODO: High/Medium/Low/None]

Wahrscheinlichkeit: [TODO: High/Medium/Low]

Risikobewertung: [TODO: High/Medium/Low]

12.4.2.2 T.002: [TODO: Bedrohungsname]

[TODO: Wiederhole die Struktur für jede Bedrohung]

12.4.3 4.3 Threat Scenarios

Angriffsszenario 1: [TODO: Szenarioname] [TODO: Beschreibe ein vollständiges Angriffsszenario]

Angriffsszenario 2: [TODO: Szenarioname] [TODO: Beschreibe ein weiteres Angriffsszenario]

12.5 5. Organizational Security Policies

12.5.1 5.1 OSP Catalog

Organisatorische Sicherheitsrichtlinien:

OSP ID	OSP Name	Category	Mandatory	Description
[TODO: P.001]	[TODO: Richtlinienname]	[TODO: z.B. Access Control, Audit, Crypto]	Yes/No	[TODO: Beschreibung]
[TODO: P.002]	[TODO: Richtlinienname]	[TODO: Kategorie]	Yes/No	[TODO: Beschreibung]

12.5.2 5.2 OSP Details

12.5.2.1 P.001: [TODO: Richtlinienname]

Beschreibung: [TODO: Detaillierte Beschreibung der Richtlinie]

Zweck: [TODO: Warum ist diese Richtlinie erforderlich?]

Anforderungen: - [TODO: Anforderung 1] - [TODO: Anforderung 2] - [TODO: Anforderung 3]

Anwendungsbereich: [TODO: Wo gilt diese Richtlinie?]

Compliance-Anforderungen: [TODO: Externe Standards oder Vorschriften, die diese Richtlinie erfüllt]

12.5.2.2 P.002: [TODO: Richtlinienname]

[TODO: Wiederhole die Struktur für jede OSP]

12.5.3 5.3 Policy Compliance Matrix

Zuordnung von Richtlinien zu externen 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

Annahmen über die Betriebsumgebung:

Assumption ID	Assumption Name	Category	Criticality	Description
[TODO: A.001]	[TODO: Annahmename]	[TODO: z.B. Physical, Personnel, Connectivity]	High/Medium/Low	[TODO: Beschreibung]
[TODO: A.002]	[TODO: Annahmename]	[TODO: Kategorie]	High/Medium/Low	[TODO: Beschreibung]

12.6.2 6.2 Assumption Details

12.6.2.1 A.001: [TODO: Annahmename]

Beschreibung: [TODO: Detaillierte Beschreibung der Annahme]

Begründung: [TODO: Warum ist diese Annahme gerechtfertigt?]

Auswirkungen: [TODO: Was passiert, wenn diese Annahme nicht erfüllt ist?]

Verantwortlichkeit: [TODO: Wer ist für die Erfüllung dieser Annahme verantwortlich?]

Verifikation: [TODO: Wie kann überprüft werden, dass diese Annahme erfüllt ist?]

12.6.2.2 A.002: [TODO: Annahmename]

[TODO: Wiederhole die Struktur für jede Annahme]

12.6.3 6.3 Environmental Assumptions

Physische Umgebung: - [TODO: Annahme über physische Sicherheit] - [TODO: Annahme über Umgebungsbedingungen]

Personal: - [TODO: Annahme über Benutzerverhalten] - [TODO: Annahme über Administratorkompetenzen]

Konnektivität: - [TODO: Annahme über Netzwerksicherheit] - [TODO: Annahme über Kommunikationskanäle]

12.7 7. Security Problem Summary

12.7.1 7.1 Threat Summary

Zusammenfassung der Bedrohungen: - Anzahl identifizierter Bedrohungen: [TODO: Anzahl] - Bedrohungen mit hohem Risiko: [TODO: Anzahl] - Bedrohungen mit mittlerem Risiko: [TODO: Anzahl] - Bedrohungen mit niedrigem Risiko: [TODO: Anzahl]

12.7.2 7.2 OSP Summary

Zusammenfassung der Richtlinien: - Anzahl organisatorischer Sicherheitsrichtlinien: [TODO: Anzahl] - Verpflichtende Richtlinien: [TODO: Anzahl] - Optionale Richtlinien: [TODO: Anzahl]

12.7.3 7.3 Assumption Summary

Zusammenfassung der Annahmen: - Anzahl der Annahmen: [TODO: Anzahl] - Kritische Annahmen: [TODO: Anzahl] - Annahmen mit mittlerer Kritikalität: [TODO: Anzahl] - Annahmen mit niedriger Kritikalität: [TODO: Anzahl]

12.7.4 7.4 Coverage Analysis

Abdeckungsanalyse: [TODO: Analysiere, ob alle Assets durch Bedrohungen, OSPs oder Annahmen abgedeckt sind]

12.8 8. Traceability

12.8.1 8.1 Asset-to-Threat Mapping

Zuordnung von Assets zu Bedrohungen:

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

Zuordnung von Bedrohungen zu Agenten:

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

Vollständige Rückverfolgbarkeit:

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]

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter mit TOE-spezifischen Informationen 2. Führe eine vollständige Bedrohungsanalyse durch 3. Dokumentiere alle relevanten OSPs 4. Identifiziere und validiere alle Annahmen 5. Erstelle Bedrohungsmodell und Angriffsszenarien 6. Überprüfe die Konsistenz mit Security Objectives (Template 0300)

ewpage

Chapter 13

Threats (Bedrohungen)

Dokument-ID: 0210
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

13.1 1. Threat Overview

13.1.1 1.1 Threat Identification Methodology

Methodik zur Bedrohungsidentifikation: [TODO: Beschreibe die verwendete Methodik, z.B. STRIDE, PASTA, Attack Trees]

Verwendete Frameworks: - [TODO: z.B. MITRE ATT&CK] - [TODO: z.B. OWASP Top 10] - [TODO: z.B. CWE Top 25]

13.1.2 1.2 Threat Categories

Bedrohungskategorien: - **Confidentiality Threats**: Bedrohungen der Vertraulichkeit - **Integrity Threats**: Bedrohungen der Integrität - **Availability Threats**: Bedrohungen der Verfügbarkeit - **Authentication Threats**: Bedrohungen der Authentifizierung - **Authorization Threats**: Bedrohungen der Autorisierung - **Non-Repudiation Threats**: Bedrohungen der Nicht-Abstreitbarkeit

13.1.3 1.3 Threat Scope

Im Scope: [TODO: Welche Bedrohungen werden betrachtet?]

Außerhalb des Scope: [TODO: Welche Bedrohungen werden nicht betrachtet und warum?]

13.2 2. Confidentiality Threats

13.2.1 T.UNAUTHORIZED_ACCESS

Bedrohungs-ID: T.UNAUTHORIZED_ACCESS
Kategorie: Confidentiality
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Ein Angreifer könnte unbefugten Zugriff auf vertrauliche Daten erlangen]

Betroffene Assets: - [TODO: A.001 - Benutzerdaten] - [TODO: A.002 - Konfigurationsdaten]

Bedrohungsagent: - [TODO: TA.001 - Externer Angreifer] - [TODO: TA.002 - Böswilliger Insider]

Angriffsszenario: 1. [TODO: Angreifer identifiziert Schwachstelle in Zugriffskontrolle] 2. [TODO: Angreifer umgeht Authentifizierung] 3. [TODO: Angreifer greift auf vertrauliche Daten zu] 4. [TODO: Angreifer exfiltriert Daten]

Voraussetzungen: - [TODO: Netzwerkzugriff auf TOE] - [TODO: Kenntnis der Systemarchitektur]

Auswirkungen: - **Vertraulichkeit:** High - Vollständiger Verlust der Datenkontrolle - **Integrität:** None - **Verfügbarkeit:** None

Wahrscheinlichkeit: [TODO: High/Medium/Low]
Risikobewertung: [TODO: High/Medium/Low]

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

13.2.2 T.EAVESDROPPING

Bedrohungs-ID: T.EAVESDROPPING
Kategorie: Confidentiality
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Ein Angreifer könnte Kommunikation abhören und vertrauliche Informationen erlangen]

Betroffene Assets: - [TODO: A.003 - Kommunikationsdaten]

Bedrohungsagent: - [TODO: TA.003 - Network Attacker]

Angriffsszenario: 1. [TODO: Angreifer positioniert sich im Netzwerkpfad] 2. [TODO: Angreifer fängt unverschlüsselte Kommunikation ab] 3. [TODO: Angreifer analysiert abgefangene Daten]

Voraussetzungen: - [TODO: Zugriff auf Netzwerkinfrastruktur] - [TODO: Unverschlüsselte Kommunikation]

Auswirkungen: - **Vertraulichkeit:** High - **Integrität:** None - **Verfügbarkeit:** None

Wahrscheinlichkeit: [TODO: High/Medium/Low]
Risikobewertung: [TODO: High/Medium/Low]

13.2.3 T.DATA_LEAKAGE

Bedrohungs-ID: T.DATA_LEAKAGE
Kategorie: Confidentiality
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Vertrauliche Daten könnten durch Fehler oder Schwachstellen unbeabsichtigt offengelegt werden]

[TODO: Füge weitere Confidentiality Threats hinzu]

13.3 3. Integrity Threats

13.3.1 T.DATA_MANIPULATION

Bedrohungs-ID: T.DATA_MANIPULATION
Kategorie: Integrity
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Ein Angreifer könnte Daten unbefugt ändern oder manipulieren]

Betroffene Assets: - [TODO: A.004 - Transaktionsdaten] - [TODO: A.005 - Konfigurationsdaten]

Bedrohungsagent: - [TODO: TA.001 - Externer Angreifer] - [TODO: TA.002 - Böswilliger Insider]

Angriffsszenario: 1. [TODO: Angreifer erlangt Schreibzugriff] 2. [TODO: Angreifer modifiziert kritische Daten] 3. [TODO: Modifikation bleibt unentdeckt] 4. [TODO: System verarbeitet manipulierte Daten]

Voraussetzungen: - [TODO: Schreibzugriff auf Daten] - [TODO: Fehlende Integritätsprüfungen]

Auswirkungen: - **Vertraulichkeit:** None - **Integrität:** High - Datenintegrität kompromittiert - **Verfügbarkeit:** None

Wahrscheinlichkeit: [TODO: High/Medium/Low]
Risikobewertung: [TODO: High/Medium/Low]

13.3.2 T.CODE_INJECTION

Bedrohungs-ID: T.CODE_INJECTION
Kategorie: Integrity
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Ein Angreifer könnte schädlichen Code in das System einschleusen]

[TODO: Füge weitere Integrity Threats hinzu]

13.4 4. Availability Threats

13.4.1 T.DENIAL_OF_SERVICE

Bedrohungs-ID: T.DENIAL_OF_SERVICE
Kategorie: Availability

Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Ein Angreifer könnte die Verfügbarkeit des TOE durch Überlastung beeinträchtigen]

Betroffene Assets: - [TODO: A.006 - Service-Verfügbarkeit]

Bedrohungsagent: - [TODO: TA.003 - Network Attacker]

Angriffsszenario: 1. [TODO: Angreifer sendet große Anzahl von Anfragen] 2. [TODO: System-Ressourcen werden erschöpft] 3. [TODO: Legitime Anfragen können nicht mehr verarbeitet werden]

Voraussetzungen: - [TODO: Netzwerkzugriff] - [TODO: Fehlende Rate-Limiting]

Auswirkungen: - **Vertraulichkeit:** None - **Integrität:** None - **Verfügbarkeit:** High - Service nicht verfügbar

Wahrscheinlichkeit: [TODO: High/Medium/Low]
Risikobewertung: [TODO: High/Medium/Low]

13.4.2 T.RESOURCE_EXHAUSTION

Bedrohungs-ID: T.RESOURCE_EXHAUSTION
Kategorie: Availability
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Ein Angreifer könnte System-Ressourcen erschöpfen]

[TODO: Füge weitere Availability Threats hinzu]

13.5 5. Authentication Threats

13.5.1 T.AUTHENTICATION_BYPASS

Bedrohungs-ID: T.AUTHENTICATION_BYPASS
Kategorie: Authentication
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Ein Angreifer könnte Authentifizierungsmechanismen umgehen]

Betroffene Assets: - [TODO: A.007 - Authentifizierungssystem]

Bedrohungsagent: - [TODO: TA.001 - Externer Angreifer]

Angriffsszenario: 1. [TODO: Angreifer identifiziert Schwachstelle in Authentifizierung] 2. [TODO: Angreifer umgeht Authentifizierungsprüfung] 3. [TODO: Angreifer erlangt unbefugten Zugriff]

Voraussetzungen: - [TODO: Zugriff auf Authentifizierungsschnittstelle] - [TODO: Schwachstelle in Authentifizierungslogik]

Auswirkungen: - **Vertraulichkeit:** High - **Integrität:** High - **Verfügbarkeit:** Medium

Wahrscheinlichkeit: [TODO: High/Medium/Low]
Risikobewertung: [TODO: High/Medium/Low]

13.5.2 T.CREDENTIAL_THEFT

Bedrohungs-ID: T.CREDENTIAL_THEFT
Kategorie: Authentication
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Ein Angreifer könnte Authentifizierungsdaten stehlen]

[TODO: Füge weitere Authentication Threats hinzu]

13.6 6. Authorization Threats

13.6.1 T.PRIVILEGE_ESCALATION

Bedrohungs-ID: T.PRIVILEGE_ESCALATION
Kategorie: Authorization
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Ein Angreifer könnte seine Berechtigungen unbefugt erweitern]

Betroffene Assets: - [TODO: A.008 - Autorisierungssystem]

Bedrohungsagent: - [TODO: TA.002 - Böswilliger Insider]

Angriffsszenario: 1. [TODO: Angreifer mit niedrigen Rechten identifiziert Schwachstelle] 2. [TODO: Angreifer nutzt Schwachstelle zur Rechteausweitung] 3. [TODO: Angreifer erlangt administrative Rechte]

Voraussetzungen: - [TODO: Gültiges Benutzerkonto] - [TODO: Schwachstelle in Autorisierungsprüfung]

Auswirkungen: - **Vertraulichkeit:** High - **Integrität:** High - **Verfügbarkeit:** High

Wahrscheinlichkeit: [TODO: High/Medium/Low]
Risikobewertung: [TODO: High/Medium/Low]

13.6.2 T.UNAUTHORIZED_FUNCTION_ACCESS

Bedrohungs-ID: T.UNAUTHORIZED_FUNCTION_ACCESS
Kategorie: Authorization
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Ein Angreifer könnte auf Funktionen zugreifen, für die er nicht autorisiert ist]

[TODO: Füge weitere Authorization Threats hinzu]

13.7 7. Non-Repudiation Threats

13.7.1 T.REPUDIATION

Bedrohungs-ID: T.REPUDIATION
Kategorie: Non-Repudiation
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Ein Benutzer könnte durchgeführte Aktionen abstreiten]

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

Bedrohungsagent: - [TODO: TA.002 - Böswilliger Insider]

Angriffsszenario: 1. [TODO: Benutzer führt kritische Aktion durch] 2. [TODO: Benutzer manipuliert oder löscht Audit-Logs] 3. [TODO: Benutzer streitet Aktion ab]

Voraussetzungen: - [TODO: Zugriff auf Audit-System] - [TODO: Fehlende Log-Integrität]

Auswirkungen: - **Vertraulichkeit:** None - **Integrität:** High - **Verfügbarkeit:** None

Wahrscheinlichkeit: [TODO: High/Medium/Low]
Risikobewertung: [TODO: High/Medium/Low]

13.7.2 T.LOG_TAMPERING

Bedrohungs-ID: T.LOG_TAMPERING
Kategorie: Non-Repudiation
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Ein Angreifer könnte Audit-Logs manipulieren oder löschen]

[TODO: Füge weitere Non-Repudiation Threats hinzu]

13.8 8. Threat Summary

13.8.1 8.1 Threat Statistics

Bedrohungsstatistik: - Gesamtanzahl Bedrohungen: [TODO: Anzahl] - Confidentiality Threats: [TODO: Anzahl] - Integrity Threats: [TODO: Anzahl] - Availability Threats: [TODO: Anzahl] - Authentication Threats: [TODO: Anzahl] - Authorization Threats: [TODO: Anzahl] - Non-Repudiation Threats: [TODO: Anzahl]

13.8.2 8.2 Risk Distribution

Risikoverteilung: - High Risk: [TODO: Anzahl] ([TODO: %]) - Medium Risk: [TODO: Anzahl] ([TODO: %]) - Low Risk: [TODO: Anzahl] ([TODO: %])

13.8.3 8.3 Threat Priority Matrix

Priorisierungsmatrix:

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 Tree für kritische Bedrohungen:

[TODO: Erstelle Attack Trees für die wichtigsten Bedrohungen]

`[TODO: Attack Tree Diagramm einfügen]`

13.9.2 9.2 Threat Relationships

Beziehungen zwischen Bedrohungen:

[TODO: Beschreibe, wie Bedrohungen zusammenhängen oder sich gegenseitig ermöglichen]

`[TODO: Bedrohungsbeziehungsdiagramm einfügen]`

13.9.3 9.3 Attack Chains

Angriffsketten:

Chain 1: [TODO: Name] 1. [TODO: T.001] → [TODO: T.003] → [TODO: T.005] 2. [TODO: Beschreibung der Angriffskette]

Chain 2: [TODO: Name] 1. [TODO: T.002] → [TODO: T.004] 2. [TODO: Beschreibung der Angriffskette]

13.10 10. Traceability

13.10.1 10.1 Threat-to-Asset Mapping

Zuordnung Bedrohungen zu 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

Zuordnung Bedrohungen zu Agenten:

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

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter mit TOE-spezifischen Bedrohungen 2. Führe vollständige Bedrohungsanalyse durch 3. Erstelle Attack Trees für kritische Bedrohungen 4. Bewerte Risiken für alle Bedrohungen 5. Dokumentiere Angriffsketten 6. Überprüfe Konsistenz mit Assets (Template 0200) und Security Objectives (Template 0300)

ewpage

Chapter 14

Organizational Security Policies (OSPs)

Dokument-ID: 0220
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

14.1 1. OSP Overview

14.1.1 1.1 Purpose

Organisatorische Sicherheitsrichtlinien (OSPs) definieren Sicherheitsregeln und -praktiken, die: - Von der Organisation vorgegeben werden - Vom TOE durchgesetzt oder unterstützt werden müssen - Unabhängig von spezifischen Bedrohungen gelten - Compliance-Anforderungen erfüllen

14.1.2 1.2 OSP Categories

Richtlinienkategorien: - **Access Control Policies**: Zugriffskontrollrichtlinien - **Audit Policies**: Audit- und Protokollierungsrichtlinien - **Cryptographic Policies**: Kryptografierichtlinien - **Data Protection Policies**: Datenschutzrichtlinien - **Authentication Policies**: Authentifizierungsrichtlinien - **Configuration Policies**: Konfigurationsrichtlinien - **Operational Policies**: Betriebsrichtlinien

14.1.3 1.3 Policy Scope

Im Scope: [TODO: Welche Richtlinien werden vom TOE durchgesetzt?]

Außerhalb des Scope: [TODO: Welche Richtlinien werden nicht vom TOE durchgesetzt?]

14.2 2. Access Control Policies

14.2.1 P.ACCESS_CONTROL

Richtlinien-ID: P.ACCESS_CONTROL
Kategorie: Access Control
Verpflichtend: [TODO: Yes/No]
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Der TOE muss Zugriffskontrollmechanismen implementieren, die sicherstellen, dass nur autorisierte Benutzer auf geschützte Ressourcen zugreifen können]

Zweck: [TODO: Schutz vor unbefugtem Zugriff auf sensible Daten und Funktionen]

Anforderungen: - [TODO: Implementierung von Role-Based Access Control (RBAC)] - [TODO: Durchsetzung des Least-Privilege-Prinzips] - [TODO: Regelmäßige Überprüfung von Zugriffsrechten] - [TODO: Dokumentation aller Zugriffsentscheidungen]

Anwendungsbereich: [TODO: Alle Benutzer und Administratoren des TOE]

Durchsetzung: - **TOE-Verantwortlichkeit:** [TODO: Zugriffskontrollmechanismen implementieren] - **Umgebungsverantwortlichkeit:** [TODO: Benutzerrollen definieren und zuweisen]

Compliance-Anforderungen: - ISO 27001: A.9.1, A.9.2, A.9.4 - NIST 800-53: AC-2, AC-3, AC-6 - [TODO: Weitere Standards]

Verifikation: [TODO: Wie wird die Einhaltung dieser Richtlinie überprüft?]

14.2.2 P.NEED_TO_KNOW

Richtlinien-ID: P.NEED_TO_KNOW
Kategorie: Access Control
Verpflichtend: [TODO: Yes/No]
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Zugriff auf Informationen darf nur gewährt werden, wenn ein berechtigtes Interesse besteht]

[TODO: Füge weitere Access Control Policies hinzu]

14.3 3. Audit Policies

14.3.1 P.AUDIT_LOGGING

Richtlinien-ID: P.AUDIT_LOGGING
Kategorie: Audit
Verpflichtend: [TODO: Yes/No]
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Der TOE muss alle sicherheitsrelevanten Ereignisse protokollieren und Audit-Logs vor unbefugter Änderung schützen]

Zweck: [TODO: Nachvollziehbarkeit von Aktionen und Unterstützung forensischer Analysen]

Anforderungen: - [TODO: Protokollierung aller Authentifizierungsversuche] - [TODO: Protokollierung aller Zugriffe auf sensible Daten] - [TODO: Protokollierung aller administrativen Aktionen] - [TODO: Schutz der Audit-Logs vor Manipulation] - [TODO: Regelmäßige Überprüfung der Audit-Logs] - [TODO: Aufbewahrung der Logs für [TODO: Zeitraum]]

Anwendungsbereich: [TODO: Alle Benutzer und Systemkomponenten]

Durchsetzung: - **TOE-Verantwortlichkeit:** [TODO: Audit-Mechanismen implementieren] - **Umgebungsverantwortlichkeit:** [TODO: Log-Speicher bereitstellen und überwachen]

Compliance-Anforderungen: - ISO 27001: A.12.4 - NIST 800-53: AU-2, AU-3, AU-9 - [TODO: Weitere Standards]

Verifikation: [TODO: Wie wird die Einhaltung dieser Richtlinie überprüft?]

14.3.2 P.AUDIT_REVIEW

Richtlinien-ID: P.AUDIT_REVIEW
Kategorie: Audit
Verpflichtend: [TODO: Yes/No]
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Audit-Logs müssen regelmäßig überprüft werden, um Sicherheitsvorfälle zu erkennen]

[TODO: Füge weitere Audit Policies hinzu]

14.4 4. Cryptographic Policies

14.4.1 P.CRYPTOGRAPHY

Richtlinien-ID: P.CRYPTOGRAPHY
Kategorie: Cryptographic
Verpflichtend: [TODO: Yes/No]
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Der TOE muss kryptografische Mechanismen verwenden, um Vertraulichkeit und Integrität zu gewährleisten]

Zweck: [TODO: Schutz sensibler Daten durch Verschlüsselung]

Anforderungen: - [TODO: Verwendung von zugelassenen kryptografischen Algorithmen] - [TODO: Mindestschlüssellängen: AES-256, RSA-2048, etc.] - [TODO: Sichere Schlüsselverwaltung und -speicherung] - [TODO: Regelmäßige Schlüsselrotation] - [TODO: Verwendung von TLS 1.2 oder höher für Kommunikation] - [TODO: Verwendung von FIPS 140-2 validierten Kryptomodulen]

Anwendungsbereich: [TODO: Alle verschlüsselten Daten und Kommunikationskanäle]

Durchsetzung: - **TOE-Verantwortlichkeit:** [TODO: Kryptografische Funktionen implementieren] - **Umgebungsverantwortlichkeit:** [TODO: Kryptografische Schlüssel verwalten]

Compliance-Anforderungen: - ISO 27001: A.10.1 - NIST 800-53: SC-12, SC-13 - FIPS 140-2 - [TODO: Weitere Standards]

Verifikation: [TODO: Wie wird die Einhaltung dieser Richtlinie überprüft?]

14.4.2 P.KEY_MANAGEMENT

Richtlinien-ID: P.KEY_MANAGEMENT
Kategorie: Cryptographic
Verpflichtend: [TODO: Yes/No]
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Kryptografische Schlüssel müssen sicher generiert, gespeichert und verwaltet werden]

[TODO: Füge weitere Cryptographic Policies hinzu]

14.5 5. Data Protection Policies

14.5.1 P.DATA_CLASSIFICATION

Richtlinien-ID: P.DATA_CLASSIFICATION
Kategorie: Data Protection
Verpflichtend: [TODO: Yes/No]
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Alle Daten müssen klassifiziert und entsprechend ihrer Klassifizierung geschützt werden]

Zweck: [TODO: Angemessener Schutz von Daten basierend auf ihrer Sensitivität]

Anforderungen: - [TODO: Klassifizierungsschema: Public, Internal, Confidential, Restricted] - [TODO: Kennzeichnung aller Daten mit Klassifizierung] - [TODO: Schutzmaßnahmen entsprechend Klassifizierung] - [TODO: Regelmäßige Überprüfung der Klassifizierung]

Anwendungsbereich: [TODO: Alle im TOE verarbeiteten Daten]

Durchsetzung: - **TOE-Verantwortlichkeit:** [TODO: Klassifizierungsbasierte Zugriffskontrolle] - **Umgebungsverantwortlichkeit:** [TODO: Datenklassifizierung durchführen]

Compliance-Anforderungen: - ISO 27001: A.8.2 - GDPR: Article 32 - [TODO: Weitere Standards]

Verifikation: [TODO: Wie wird die Einhaltung dieser Richtlinie überprüft?]

14.5.2 P.DATA_RETENTION

Richtlinien-ID: P.DATA_RETENTION
Kategorie: Data Protection
Verpflichtend: [TODO: Yes/No]
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Daten müssen gemäß Aufbewahrungsrichtlinien gespeichert und gelöscht werden]

[TODO: Füge weitere Data Protection Policies hinzu]

14.6 6. Authentication Policies

14.6.1 P.STRONG_AUTHENTICATION

Richtlinien-ID: P.STRONG_AUTHENTICATION
Kategorie: Authentication
Verpflichtend: [TODO: Yes/No]
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Der TOE muss starke Authentifizierungsmechanismen implementieren]

Zweck: [TODO: Sicherstellung der Benutzeridentität]

Anforderungen: - [TODO: Multi-Faktor-Authentifizierung (MFA) für privilegierte Konten] - [TODO: Passwortrichtlinien: Mindestlänge, Komplexität, Ablauf] - [TODO: Account-Lockout nach fehlgeschlagenen Anmeldeversuchen] - [TODO: Sichere Speicherung von Authentifizierungsdaten (Hashing)] - [TODO: Session-Timeout nach Inaktivität]

Anwendungsbereich: [TODO: Alle Benutzer des TOE]

Durchsetzung: - **TOE-Verantwortlichkeit:** [TODO: Authentifizierungsmechanismen implementieren] - **Umgebungsverantwortlichkeit:** [TODO: Benutzer schulen und überwachen]

Compliance-Anforderungen: - ISO 27001: A.9.4 - NIST 800-53: IA-2, IA-5 - [TODO: Weitere Standards]

Verifikation: [TODO: Wie wird die Einhaltung dieser Richtlinie überprüft?]

14.6.2 P.PASSWORD_POLICY

Richtlinien-ID: P.PASSWORD_POLICY
Kategorie: Authentication
Verpflichtend: [TODO: Yes/No]
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Passwörter müssen bestimmte Komplexitäts- und Sicherheitsanforderungen erfüllen]

[TODO: Füge weitere Authentication Policies hinzu]

14.7 7. Configuration Policies

14.7.1 P.SECURE_CONFIGURATION

Richtlinien-ID: P.SECURE_CONFIGURATION
Kategorie: Configuration
Verpflichtend: [TODO: Yes/No]
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Der TOE muss in einer sicheren Konfiguration betrieben werden]

Zweck: [TODO: Minimierung der Angriffsfläche durch sichere Konfiguration]

Anforderungen: - [TODO: Deaktivierung nicht benötigter Dienste und Funktionen] - [TODO: Verwendung sicherer Standardeinstellungen] - [TODO: Regelmäßige Überprüfung der Konfiguration] - [TODO: Dokumentation aller Konfigurationsänderungen] - [TODO: Change-Management-Prozess für Konfigurationsänderungen]

Anwendungsbereich: [TODO: Alle TOE-Komponenten]

Durchsetzung: - **TOE-Verantwortlichkeit:** [TODO: Sichere Standardkonfiguration bereitstellen] - **Umgebungsverantwortlichkeit:** [TODO: Konfiguration überwachen und verwalten]

Compliance-Anforderungen: - ISO 27001: A.12.6 - NIST 800-53: CM-6, CM-7 - CIS Controls - [TODO: Weitere Standards]

Verifikation: [TODO: Wie wird die Einhaltung dieser Richtlinie überprüft?]

14.7.2 P.CONFIGURATION_MANAGEMENT

Richtlinien-ID: P.CONFIGURATION_MANAGEMENT
Kategorie: Configuration
Verpflichtend: [TODO: Yes/No]
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Konfigurationsänderungen müssen kontrolliert und dokumentiert werden]

[TODO: Füge weitere Configuration Policies hinzu]

14.8 8. Operational Policies

14.8.1 P.SECURITY_UPDATES

Richtlinien-ID: P.SECURITY_UPDATES
Kategorie: Operational
Verpflichtend: [TODO: Yes/No]
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Sicherheitsupdates müssen zeitnah installiert werden]

Zweck: [TODO: Schutz vor bekannten Schwachstellen]

Anforderungen: - [TODO: Regelmäßige Überprüfung auf verfügbare Updates] - [TODO: Bewertung und Priorisierung von Updates] - [TODO: Zeitnahe Installation kritischer Sicherheitsupdates] - [TODO: Testing von Updates vor Produktivinstallation] - [TODO: Dokumentation aller installierten Updates]

Anwendungsbereich: [TODO: Alle TOE-Komponenten]

Durchsetzung: - **TOE-Verantwortlichkeit:** [TODO: Update-Mechanismus bereitstellen] - **Umgebungsverantwortlichkeit:** [TODO: Updates installieren und verwalten]

Compliance-Anforderungen: - ISO 27001: A.12.6.1 - NIST 800-53: SI-2 - [TODO: Weitere Standards]

Verifikation: [TODO: Wie wird die Einhaltung dieser Richtlinie überprüft?]

14.8.2 P.BACKUP_RECOVERY

Richtlinien-ID: P.BACKUP_RECOVERY
Kategorie: Operational
Verpflichtend: [TODO: Yes/No]
Priorität: [TODO: High/Medium/Low]

Beschreibung: [TODO: Regelmäßige Backups müssen erstellt und getestet werden]

[TODO: Füge weitere Operational Policies hinzu]

14.9 9. Policy Compliance Matrix

14.9.1 9.1 Standards Mapping

Zuordnung zu externen 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

Regulatorische Anforderungen:

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

Branchenstandards:

Standard	Applicable OSPs	Compliance Status
[TODO: ISO 27001]	[TODO: Alle OSPs]	[TODO: Compliant/Partial/Non-Compliant]
[TODO: NIST 800-53]	[TODO: P.001-P.010]	[TODO: Compliant/Partial/Non-Compliant]

Standard	Applicable OSPs	Compliance Status
[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

Richtlinienstatistik: - Gesamtanzahl OSPs: [TODO: Anzahl] - Verpflichtende Richtlinien: [TODO: Anzahl] - Optionale Richtlinien: [TODO: Anzahl] - Access Control Policies: [TODO: Anzahl] - Audit Policies: [TODO: Anzahl] - Cryptographic Policies: [TODO: Anzahl] - Data Protection Policies: [TODO: Anzahl] - Authentication Policies: [TODO: Anzahl] - Configuration Policies: [TODO: Anzahl] - Operational Policies: [TODO: Anzahl]

14.10.2 10.2 Enforcement Responsibility

Durchsetzungsverantwortlichkeit:

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

14.10.3 10.3 Priority Distribution

Prioritätsverteilung: - High Priority: [TODO: Anzahl] ([TODO: %]) - Medium Priority: [TODO: Anzahl] ([TODO: %]) - Low Priority: [TODO: Anzahl] ([TODO: %])

14.11 11. Traceability

14.11.1 11.1 OSP-to-Threat Mapping

Zuordnung OSPs zu Bedrohungen:

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

14.11.2 11.2 OSP-to-Asset Mapping

Zuordnung OSPs zu 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]

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter mit organisationsspezifischen Richtlinien 2. Dokumentiere alle relevanten OSPs 3. Ordne OSPs zu externen Standards zu 4. Definiere Durchsetzungsmechanismen 5. Erstelle Compliance-Matrix 6. Überprüfe Konsistenz mit Threats (Template 0210) und Security Objectives (Template 0300)

ewpage

Chapter 15

Assumptions (Annahmen)

Dokument-ID: 0230
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

15.1 1. Assumptions Overview

15.1.1 1.1 Purpose

Annahmen definieren Erwartungen an die Betriebsumgebung des TOE: - **Physische Umgebung**: Annahmen über physische Sicherheit und Infrastruktur - **Personal**: Annahmen über Benutzer, Administratoren und deren Verhalten - **Konnektivität**: Annahmen über Netzwerk und Kommunikationsinfrastruktur - **Technische Umgebung**: Annahmen über IT-Infrastruktur und Plattformen

15.1.2 1.2 Assumption Categories

Annahmenkategorien: - **Physical Assumptions**: Physische Sicherheitsannahmen - **Personnel Assumptions**: Personalannahmen - **Connectivity Assumptions**: Konnektivitätsannahmen - **Platform Assumptions**: Plattformannahmen - **Operational Assumptions**: Betriebsannahmen

15.1.3 1.3 Assumption Scope

Im Scope: [TODO: Welche Aspekte der Umgebung werden durch Annahmen abgedeckt?]

Außerhalb des Scope: [TODO: Welche Aspekte werden nicht durch Annahmen abgedeckt?]

15.2 2. Physical Assumptions

15.2.1 A.PHYSICAL_SECURITY

Annahme-ID: A.PHYSICAL_SECURITY
Kategorie: Physical
Kritikalität: [TODO: High/Medium/Low]
Verpflichtend: [TODO: Yes/No]

Beschreibung: [TODO: Der TOE wird in einer physisch gesicherten Umgebung betrieben, die vor unbefugtem physischen Zugriff geschützt ist]

Begründung: [TODO: Physische Sicherheit ist erforderlich, um Hardware-Manipulation und direkten Zugriff auf das System zu verhindern]

Anforderungen: - [TODO: Zutrittskontrolle zu Serverräumen] - [TODO: Videoüberwachung kritischer Bereiche] - [TODO: Alarmanlage bei unbefugtem Zutritt] - [TODO: Sichere Aufbewahrung von Backup-Medien] - [TODO: Besucherprotokoll und Begleitpflicht]

Auswirkungen bei Nichterfüllung: [TODO: Beschreibe die Sicherheitsrisiken, wenn diese Annahme nicht erfüllt ist] - Risiko: [TODO: z.B. Hardware-Manipulation, Diebstahl] - Betroffene Assets: [TODO: A.001, A.002] - Betroffene Bedrohungen: [TODO: T.001, T.003]

Verantwortlichkeit: - **Primär:** [TODO: Facility Management] - **Sekundär:** [TODO: Security Team]

Verifikation: [TODO: Wie wird überprüft, dass diese Annahme erfüllt ist?] - Methode: [TODO: z.B. Physische Inspektion, Audit] - Frequenz: [TODO: z.B. Jährlich, Quartalsweise] - Dokumentation: [TODO: z.B. Audit-Bericht, Checkliste]

15.2.2 A.ENVIRONMENTAL_PROTECTION

Annahme-ID: A.ENVIRONMENTAL_PROTECTION
Kategorie: Physical
Kritikalität: [TODO: High/Medium/Low]
Verpflichtend: [TODO: Yes/No]

Beschreibung: [TODO: Der TOE wird in einer Umgebung betrieben, die vor Umwelteinflüssen geschützt ist]

Begründung: [TODO: Schutz vor Feuer, Wasser, Temperatur, Feuchtigkeit ist erforderlich für Verfügbarkeit]

Anforderungen: - [TODO: Klimatisierung und Temperaturkontrolle] - [TODO: Brandmeldeanlage und Löschsystem] - [TODO: Wasserschutz und Leckageerkennung] - [TODO: Unterbrechungsfreie Stromversorgung (USV)] - [TODO: Notstromversorgung]

[TODO: Füge weitere Physical Assumptions hinzu]

15.3 3. Personnel Assumptions

15.3.1 A.TRUSTED_ADMIN

Annahme-ID: A.TRUSTED_ADMIN
Kategorie: Personnel
Kritikalität: [TODO: High/Medium/Low]
Verpflichtend: [TODO: Yes/No]

Beschreibung: [TODO: Administratoren sind vertrauenswürdig, kompetent und handeln nicht böswillig]

Begründung: [TODO: Administratoren haben privilegierten Zugriff und können Sicherheitsmechanismen umgehen]

Anforderungen: - [TODO: Hintergrundüberprüfung vor Einstellung] - [TODO: Unterzeichnung von Vertraulichkeitsvereinbarungen] - [TODO: Regelmäßige Sicherheitsschulungen] - [TODO: Vier-Augen-Prinzip für kritische Operationen] - [TODO: Überwachung administrativer Aktivitäten] - [TODO: Regelmäßige Überprüfung von Administratorrechten]

Auswirkungen bei Nichterfüllung: [TODO: Beschreibe die Sicherheitsrisiken] - Risiko: [TODO: z.B. Insider-Bedrohung, Sabotage, Datendiebstahl] - Betroffene Assets: [TODO: Alle Assets] - Betroffene Bedrohungen: [TODO: T.002, T.004, T.006]

Verantwortlichkeit: - **Primär:** [TODO: HR Department] - **Sekundär:** [TODO: Security Team, IT Management]

Verifikation: [TODO: Wie wird überprüft, dass diese Annahme erfüllt ist?] - Methode: [TODO: z.B. Background Checks, Audit-Log-Review] - Frequenz: [TODO: z.B. Bei Einstellung, Jährlich] - Dokumentation: [TODO: z.B. HR-Akte, Schulungsnachweise]

15.3.2 A.USER_TRAINING

Annahme-ID: A.USER_TRAINING
Kategorie: Personnel
Kritikalität: [TODO: High/Medium/Low]
Verpflichtend: [TODO: Yes/No]

Beschreibung: [TODO: Benutzer sind geschult und befolgen Sicherheitsrichtlinien]

Begründung: [TODO: Benutzer müssen Sicherheitsmechanismen verstehen und korrekt verwenden]

Anforderungen: - [TODO: Sicherheitsschulung vor Systemzugang] - [TODO: Regelmäßige Auffrischungsschulungen] - [TODO: Phishing-Awareness-Training] - [TODO: Schulung zu Passwortrichtlinien] - [TODO: Schulung zu Datenklassifizierung] - [TODO: Incident-Reporting-Schulung]

[TODO: Füge weitere Personnel Assumptions hinzu]

15.4 4. Connectivity Assumptions

15.4.1 A.NETWORK_SECURITY

Annahme-ID: A.NETWORK_SECURITY
Kategorie: Connectivity
Kritikalität: [TODO: High/Medium/Low]
Verpflichtend: [TODO: Yes/No]

Beschreibung: [TODO: Das Netzwerk, in dem der TOE betrieben wird, ist durch Firewalls und andere Sicherheitsmechanismen geschützt]

Begründung: [TODO: Netzwerksicherheit ist erforderlich, um externe Angriffe abzuwehren]

Anforderungen: - [TODO: Firewall zwischen TOE und Internet] - [TODO: Netzwerksegmentierung] - [TODO: Intrusion Detection/Prevention System (IDS/IPS)] - [TODO: Regelmäßige Netzwerk-Scans] - [TODO: VPN für Remote-Zugriff] - [TODO: DDoS-Schutz]

Auswirkungen bei Nichterfüllung: [TODO: Beschreibe die Sicherheitsrisiken] - Risiko: [TODO: z.B. Netzwerkangriffe, Datenabfluss] - Betroffene Assets: [TODO: A.003, A.004] - Betroffene Bedrohungen: [TODO: T.005, T.007]

Verantwortlichkeit: - **Primär:** [TODO: Network Team] - **Sekundär:** [TODO: Security Team]

Verifikation: [TODO: Wie wird überprüft, dass diese Annahme erfüllt ist?] - Methode: [TODO: z.B. Netzwerk-Audit, Penetration Test] - Frequenz: [TODO: z.B. Quartalsweise] - Dokumentation: [TODO: z.B. Netzwerkdiagramm, Firewall-Regeln]

15.4.2 A.SECURE_COMMUNICATION

Annahme-ID: A.SECURE_COMMUNICATION
Kategorie: Connectivity
Kritikalität: [TODO: High/Medium/Low]
Verpflichtend: [TODO: Yes/No]

Beschreibung: [TODO: Kommunikationskanäle zwischen TOE und externen Systemen sind verschlüsselt]

Begründung: [TODO: Verschlüsselung schützt vor Abhören und Man-in-the-Middle-Angriffen]

Anforderungen: - [TODO: TLS 1.2 oder höher für alle Verbindungen] - [TODO: Zertifikatsvalidierung] - [TODO: Sichere Cipher Suites] - [TODO: Regelmäßige Zertifikatserneuerung]

[TODO: Füge weitere Connectivity Assumptions hinzu]

15.5 5. Platform Assumptions

15.5.1 A.TRUSTED_PLATFORM

Annahme-ID: A.TRUSTED_PLATFORM
Kategorie: Platform

Kritikalität: [TODO: High/Medium/Low]
Verpflichtend: [TODO: Yes/No]

Beschreibung: [TODO: Die Plattform, auf der der TOE läuft, ist vertrauenswürdig und sicher konfiguriert]

Begründung: [TODO: TOE-Sicherheit hängt von der Sicherheit der zugrunde liegenden Plattform ab]

Anforderungen: - [TODO: Aktuelles und gepatchtes Betriebssystem] - [TODO: Hardening gemäß Best Practices (z.B. CIS Benchmarks)] - [TODO: Deaktivierung nicht benötigter Dienste] - [TODO: Host-basierte Firewall] - [TODO: Antivirus/Endpoint Protection] - [TODO: Regelmäßige Schwachstellenscans]

Auswirkungen bei Nichterfüllung: [TODO: Beschreibe die Sicherheitsrisiken] - Risiko: [TODO: z.B. Kompromittierung der Plattform, Privilege Escalation] - Betroffene Assets: [TODO: Alle Assets] - Betroffene Bedrohungen: [TODO: T.008, T.009]

Verantwortlichkeit: - **Primär:** [TODO: System Administration] - **Sekundär:** [TODO: Security Team]

Verifikation: [TODO: Wie wird überprüft, dass diese Annahme erfüllt ist?] - Methode: [TODO: z.B. Configuration Audit, Vulnerability Scan] - Frequenz: [TODO: z.B. Monatlich] - Dokumentation: [TODO: z.B. Scan-Berichte, Konfigurationsdokumentation]

15.5.2 A.PLATFORM_AVAILABILITY

Annahme-ID: A.PLATFORM_AVAILABILITY
Kategorie: Platform
Kritikalität: [TODO: High/Medium/Low]
Verpflichtend: [TODO: Yes/No]

Beschreibung: [TODO: Die Plattform bietet ausreichende Ressourcen und Verfügbarkeit für den TOE-Betrieb]

Begründung: [TODO: TOE benötigt ausreichende Ressourcen für ordnungsgemäßen Betrieb]

Anforderungen: - [TODO: Ausreichende CPU-Kapazität] - [TODO: Ausreichender Arbeitsspeicher] - [TODO: Ausreichender Speicherplatz] - [TODO: Hochverfügbarkeitsarchitektur (falls erforderlich)] - [TODO: Regelmäßige Kapazitätsplanung]

[TODO: Füge weitere Platform Assumptions hinzu]

15.6 6. Operational Assumptions

15.6.1 A.SECURITY_MONITORING

Annahme-ID: A.SECURITY_MONITORING
Kategorie: Operational
Kritikalität: [TODO: High/Medium/Low]
Verpflichtend: [TODO: Yes/No]

Beschreibung: [TODO: Sicherheitsereignisse werden kontinuierlich überwacht und analysiert]

Begründung: [TODO: Frühzeitige Erkennung von Sicherheitsvorfällen ist kritisch]

Anforderungen: - [TODO: 24/7 Security Operations Center (SOC)] - [TODO: SIEM-System für Log-Aggregation und -Analyse] - [TODO: Automatische Alerting bei kritischen Ereignissen] - [TODO: Definierte Incident-Response-Prozesse] - [TODO: Regelmäßige Überprüfung von Sicherheitsereignissen]

Auswirkungen bei Nichterfüllung: [TODO: Beschreibe die Sicherheitsrisiken] - Risiko: [TODO: z.B. Verspätete Erkennung von Angriffen] - Betroffene Assets: [TODO: Alle Assets] - Betroffene Bedrohungen: [TODO: Alle Bedrohungen]

Verantwortlichkeit: - **Primär:** [TODO: Security Operations Team] - **Sekundär:** [TODO: IT Operations]

Verifikation: [TODO: Wie wird überprüft, dass diese Annahme erfüllt ist?] - Methode: [TODO: z.B. SOC-Audit, Incident-Response-Test] - Frequenz: [TODO: z.B. Quartalsweise] - Dokumentation: [TODO: z.B. SOC-Berichte, Incident-Logs]

15.6.2 A.BACKUP_RECOVERY

Annahme-ID: A.BACKUP_RECOVERY
Kategorie: Operational
Kritikalität: [TODO: High/Medium/Low]
Verpflichtend: [TODO: Yes/No]

Beschreibung: [TODO: Regelmäßige Backups werden erstellt und Wiederherstellungsprozesse sind getestet]

Begründung: [TODO: Backups sind erforderlich für Disaster Recovery und Business Continuity]

Anforderungen: - [TODO: Tägliche inkrementelle Backups] - [TODO: Wöchentliche vollständige Backups] - [TODO: Offsite-Speicherung von Backups] - [TODO: Verschlüsselung von Backup-Daten] - [TODO: Regelmäßige Wiederherstellungstests] - [TODO: Dokumentierte Recovery-Prozeduren]

[TODO: Füge weitere Operational Assumptions hinzu]

15.7 7. Assumption Summary

15.7.1 7.1 Assumption Statistics

Annahmenstatistik: - Gesamtanzahl Annahmen: [TODO: Anzahl] - Physical Assumptions: [TODO: Anzahl] - Personnel Assumptions: [TODO: Anzahl] - Connectivity Assumptions: [TODO: Anzahl] - Platform Assumptions: [TODO: Anzahl] - Operational Assumptions: [TODO: Anzahl]

15.7.2 7.2 Criticality Distribution

Kritikalitätsverteilung: - High Criticality: [TODO: Anzahl] ([TODO: %]) - Medium Criticality: [TODO: Anzahl] ([TODO: %]) - Low Criticality: [TODO: Anzahl] ([TODO: %])

15.7.3 7.3 Mandatory vs. Optional

Verpflichtende vs. Optionale Annahmen: - Mandatory: [TODO: Anzahl] ([TODO: %]) - Optional: [TODO: Anzahl] ([TODO: %])

15.8 8. Assumption Validation

15.8.1 8.1 Validation Methods

Validierungsmethoden:

Assumption ID	Validation Method	Frequency	Responsible Party
[TODO: A.001]	[TODO: Methode]	[TODO: Frequenz]	[TODO: Verantwortlich]
[TODO: A.002]	[TODO: Methode]	[TODO: Frequenz]	[TODO: Verantwortlich]

15.8.2 8.2 Validation Schedule

Validierungsplan: - [TODO: Monatlich]: [TODO: A.001, A.003] - [TODO: Quartalsweise]: [TODO: A.002, A.004, A.005] - [TODO: Jährlich]: [TODO: A.006, A.007]

15.8.3 8.3 Validation Documentation

Validierungsdokumentation: [TODO: Beschreibe, wie Validierungsergebnisse dokumentiert werden]

15.9 9. Responsibility Matrix

15.9.1 9.1 Primary Responsibilities

Primäre Verantwortlichkeiten:

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

Geteilte Verantwortlichkeiten: [TODO: Beschreibe Annahmen mit geteilten Verantwortlichkeiten]

15.10 10. Traceability

15.10.1 10.1 Assumption-to-Threat Mapping

Zuordnung Annahmen zu Bedrohungen:

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

15.10.2 10.2 Assumption-to-Asset Mapping

Zuordnung Annahmen zu 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

Zuordnung Annahmen zu 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]

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter mit umgebungsspezifischen Annahmen 2. Dokumentiere alle relevanten Annahmen 3. Definiere Validierungsmethoden 4. Weise Verantwortlichkeiten zu 5. Erstelle Validierungsplan 6. Überprüfe Konsistenz mit Threats (Template 0210), OSPs (Template 0220) und Security Objectives (Template 0300)

ewpage

Chapter 16

Threat Agents and Assets

Dokument-ID: 0240
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

16.1 1. Overview

16.1.1 1.1 Purpose

Dieses Dokument definiert: - **Threat Agents**: Potenzielle Angreifer mit ihren Fähigkeiten und Motivationen - **Assets**: Schützenswerte Ressourcen, Daten und Funktionen

16.1.2 1.2 Scope

Im Scope: [TODO: Was wird in diesem Dokument abgedeckt?]

Außerhalb des Scope: [TODO: Was wird nicht abgedeckt?]

16.2 2. Assets

16.2.1 2.1 Asset Identification

16.2.1.1 2.1.1 Asset Categories

Asset-Kategorien: - **Data Assets**: Daten und Informationen - **Service Assets**: Dienste und Funktionen - **System Assets**: Systemkomponenten und Infrastruktur - **Credential Assets**: Authentifizierungs- und Autorisierungsdaten - **Configuration Assets**: Konfigurationsdaten und -einstellungen

16.2.1.2 2.1.2 Asset Inventory

Asset-Inventar:

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

16.2.2 2.2 Data Assets

16.2.2.1 A.USER_DATA

Asset-ID: A.USER_DATA
Kategorie: Data
Typ: [TODO: Personal Data / Business Data / Technical Data]

Beschreibung: [TODO: Benutzerdaten einschließlich persönlicher Informationen, Präferenzen und Profildaten]

Eigenschaften: - **Vertraulichkeit:** [TODO: High/Medium/Low] - **Integrität:** [TODO: High/Medium/Low] - **Verfügbarkeit:** [TODO: High/Medium/Low] - **Datenvolumen:** [TODO: z.B. 1 TB] - **Datenformat:** [TODO: z.B. JSON, XML, Database]

Schutzbedarf: - **Vertraulichkeit:** [TODO: Begründung für Schutzbedarf] - **Integrität:** [TODO: Begründung für Schutzbedarf] - **Verfügbarkeit:** [TODO: Begründung für Schutzbedarf]

Regulatorische Anforderungen: - [TODO: GDPR Article 32 - Security of processing] - [TODO: HIPAA §164.312 - Technical safeguards] - [TODO: Weitere Anforderungen]

Wert: - **Geschäftswert:** [TODO: High/Medium/Low] - **Monetärer Wert:** [TODO: Schätzung] - **Reputationswert:** [TODO: High/Medium/Low]

Lebenszyklus: - **Erstellung:** [TODO: Wie werden Daten erstellt?] - **Speicherung:** [TODO: Wo werden Daten gespeichert?] - **Verarbeitung:** [TODO: Wie werden Daten verarbeitet?] - **Übertragung:** [TODO: Wie werden Daten übertragen?] - **Archivierung:** [TODO: Wie werden Daten archiviert?] - **Löschung:** [TODO: Wie werden Daten gelöscht?]

16.2.2.2 A.AUTHENTICATION_DATA

Asset-ID: A.AUTHENTICATION_DATA
Kategorie: Credential
Typ: [TODO: Passwords / Tokens / Certificates]

Beschreibung: [TODO: Authentifizierungsdaten wie Passwörter, Tokens, Zertifikate]

[TODO: Füge weitere Data Assets hinzu]

16.2.3 2.3 Service Assets

16.2.3.1 A.AUTHENTICATION_SERVICE

Asset-ID: A.AUTHENTICATION_SERVICE
Kategorie: Service
Typ: [TODO: Authentication / Authorization / Identity Management]

Beschreibung: [TODO: Authentifizierungsdienst, der Benutzeridentitäten verifiziert]

Eigenschaften: - **Verfügbarkeit:** [TODO: 99.9% SLA] - **Performance:** [TODO: $<$ 100ms Response Time] - **Kapazität:** [TODO: 1000 req/sec]

Schutzbedarf: - **Verfügbarkeit:** [TODO: High - Kritisch für Systemzugang] - **Integrität:** [TODO: High - Falsche Authentifizierung gefährdet Sicherheit] - **Vertraulichkeit:** [TODO: Medium - Metadaten können sensibel sein]

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

Wert: - **Geschäftswert:** [TODO: High - Grundlegende Sicherheitsfunktion] - **Kritikalität:** [TODO: High - System nicht nutzbar ohne Authentifizierung]

16.2.3.2 A.DATA_PROCESSING_SERVICE

Asset-ID: A.DATA_PROCESSING_SERVICE
Kategorie: Service
Typ: [TODO: Processing / Computation / Transformation]

Beschreibung: [TODO: Dienst zur Verarbeitung von Geschäftsdaten]

[TODO: Füge weitere Service Assets hinzu]

16.2.4 2.4 System Assets

16.2.4.1 A.TOE_PLATFORM

Asset-ID: A.TOE_PLATFORM
Kategorie: System
Typ: [TODO: Hardware / Software / Firmware]

Beschreibung: [TODO: Die Plattform, auf der der TOE läuft]

Komponenten: - [TODO: Betriebssystem] - [TODO: Hardware-Plattform] - [TODO: Virtualisierungsschicht] - [TODO: Container-Runtime]

Schutzbedarf: - **Verfügbarkeit:** [TODO: High] - **Integrität:** [TODO: High] - **Vertraulichkeit:** [TODO: Medium]

Kritikalität: [TODO: High - Kompromittierung der Plattform gefährdet alle Assets]

16.2.4.2 A.CRYPTOGRAPHIC_KEYS

Asset-ID: A.CRYPTOGRAPHIC_KEYS
Kategorie: System
Typ: [TODO: Encryption Keys / Signing Keys / Certificates]

Beschreibung: [TODO: Kryptografische Schlüssel für Verschlüsselung und Signatur]

[TODO: Füge weitere System Assets hinzu]

16.2.5 2.5 Asset Classification

16.2.5.1 2.5.1 Classification Scheme

Klassifizierungsschema:

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-Wert-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-Abhängigkeiten:

[TODO: Erstelle ein Diagramm, das Asset-Abhängigkeiten zeigt]

`[TODO: Asset-Abhängigkeitsdiagramm einfügen]`

16.2.6.2 2.6.2 Dependency Matrix

Abhängigkeitsmatrix:

Asset	Depends On	Impact if Unavailable
[TODO: A.001]	[TODO: A.003, A.005]	[TODO: Service nicht verfügbar]
[TODO: A.002]	[TODO: A.004]	[TODO: Datenverarbeitung nicht möglich]

16.3 3. Threat Agents

16.3.1 3.1 Threat Agent Identification

16.3.1.1 3.1.1 Agent Categories

Agenten-Kategorien: - **External Attackers**: Externe Angreifer ohne legitimen Zugang - **Insiders**: Mitarbeiter mit legitimem Zugang - **Privileged Insiders**: Administratoren mit privilegiertem Zugang - **Nation-State Actors**: Staatlich unterstützte Angreifer - **Organized Crime**: Organisierte Kriminalität - **Hacktivists**: Ideologisch motivierte Angreifer - **Script Kiddies**: Unerfahrene Angreifer mit vorgefertigten Tools

16.3.1.2 3.1.2 Agent Inventory

Agenten-Inventar:

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

16.3.2 3.2 Threat Agent Profiles

16.3.2.1 TA.EXTERNAL_ATTACKER

Agenten-ID: TA.EXTERNAL_ATTACKER
Typ: External Attacker
Skill Level: [TODO: Expert / Proficient / Layman]

Beschreibung: [TODO: Externer Angreifer ohne legitimen Zugang zum System, der versucht, über Netzwerk oder andere externe Schnittstellen einzudringen]

Motivation: - **Primär:** [TODO: z.B. Finanzieller Gewinn, Datendiebstahl] - **Sekundär:** [TODO: z.B. Reputation, Herausforderung]

Fähigkeiten: - **Technische Expertise:** [TODO: High - Kenntnisse in Netzwerksicherheit, Exploitation] - **Werkzeuge:** [TODO: Metasploit, Burp Suite, Custom Scripts] - **Kenntnisse:** [TODO:

Öffentlich verfügbare Informationen, OSINT] - **Zugang:** [TODO: Netzwerkzugang, keine physischen Zugang]

Ressourcen: - **Zeit:** [TODO: Wochen bis Monate] - **Budget:** [TODO: $10,000 - $100,000] - **Team:** [TODO: 1-5 Personen] - **Infrastruktur:** [TODO: Cloud-Ressourcen, Botnets]

Angriffsvektoren: - [TODO: Netzwerkangriffe (SQL Injection, XSS, etc.)] - [TODO: Social Engineering (Phishing)] - [TODO: Exploitation bekannter Schwachstellen] - [TODO: Brute-Force-Angriffe] - [TODO: DDoS-Angriffe]

Angriffspotenzial: [TODO: High - Basierend auf CCRA Attack Potential Methodology]

Beispielszenarien: 1. [TODO: Szenario 1] 2. [TODO: Szenario 2]

16.3.2.2 TA.MALICIOUS_INSIDER

Agenten-ID: TA.MALICIOUS_INSIDER
Typ: Insider
Skill Level: [TODO: Expert / Proficient / Layman]

Beschreibung: [TODO: Böswilliger Mitarbeiter mit legitimem Zugang zum System]

Motivation: - **Primär:** [TODO: z.B. Rache, finanzieller Gewinn] - **Sekundär:** [TODO: z.B. Ideologie, Erpressung]

Fähigkeiten: - **Technische Expertise:** [TODO: Medium - Grundlegende IT-Kenntnisse] - **Werkzeuge:** [TODO: Standard-Benutzertools, USB-Sticks] - **Kenntnisse:** [TODO: Insider-Wissen über Systeme und Prozesse] - **Zugang:** [TODO: Legitimer Benutzerzugang, physischer Zugang]

Ressourcen: - **Zeit:** [TODO: Tage bis Wochen] - **Budget:** [TODO: Minimal] - **Team:** [TODO: Einzelperson] - **Infrastruktur:** [TODO: Unternehmensressourcen]

Angriffsvektoren: - [TODO: Datenexfiltration über USB oder E-Mail] - [TODO: Sabotage von Systemen oder Daten] - [TODO: Missbrauch von Zugriffsrechten] - [TODO: Weitergabe von Credentials an Externe]

Angriffspotenzial: [TODO: Medium-High - Insider-Zugang kompensiert niedrigere technische Fähigkeiten]

16.3.2.3 TA.PRIVILEGED_ADMIN

Agenten-ID: TA.PRIVILEGED_ADMIN
Typ: Privileged Insider
Skill Level: [TODO: Expert]

Beschreibung: [TODO: Böswilliger Administrator mit privilegiertem Zugang]

Motivation: - **Primär:** [TODO: z.B. Finanzieller Gewinn, Erpressung] - **Sekundär:** [TODO: z.B. Rache, Ideologie]

Fähigkeiten: - **Technische Expertise:** [TODO: High - Tiefes Systemverständnis] - **Werkzeuge:** [TODO: Administrative Tools, Root-Zugang] - **Kenntnisse:** [TODO: Vollständiges Insider-Wissen, Zugang zu Dokumentation] - **Zugang:** [TODO: Privilegierter Zugang, physischer Zugang]

Ressourcen: - **Zeit:** [TODO: Stunden bis Tage] - **Budget:** [TODO: Minimal] - **Team:** [TODO: Einzelperson] - **Infrastruktur:** [TODO: Vollständiger Zugang zu Unternehmensressourcen]

Angriffsvektoren: - [TODO: Direkte Datenmanipulation] - [TODO: Deaktivierung von Sicherheitsmechanismen] - [TODO: Erstellung von Backdoors] - [TODO: Manipulation von Audit-Logs] - [TODO: Privilege Escalation für andere Accounts]

Angriffspotenzial: [TODO: Very High - Privilegierter Zugang ermöglicht nahezu alle Angriffe]

16.3.2.4 TA.NATION_STATE

Agenten-ID: TA.NATION_STATE
Typ: Nation-State Actor
Skill Level: [TODO: Expert]

Beschreibung: [TODO: Staatlich unterstützter Angreifer mit umfangreichen Ressourcen]

[TODO: Füge weitere Threat Agents hinzu]

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

Angriffspotenzial-Bewertungen:

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

Fähigkeiten-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

Welche Agenten bedrohen welche 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

Hochrisiko-Kombinationen:

Asset	Agent	Risk Level	Rationale
[TODO: A.001]	[TODO: TA.003]	[TODO: Critical]	[TODO: Hochwertige Daten + Hochqualifizierter Angreifer]
[TODO: A.002]	[TODO: TA.002]	[TODO: High]	[TODO: Kritischer Service + Insider-Zugang]

16.5 5. Summary

16.5.1 5.1 Asset Summary

Asset-Zusammenfassung: - Gesamtanzahl Assets: [TODO: Anzahl] - Critical Assets: [TODO: Anzahl] - High-Value Assets: [TODO: Anzahl] - Medium-Value Assets: [TODO: Anzahl] - Low-Value Assets: [TODO: Anzahl]

16.5.2 5.2 Threat Agent Summary

Agenten-Zusammenfassung: - Gesamtanzahl Agenten: [TODO: Anzahl] - External Attackers: [TODO: Anzahl] - Insiders: [TODO: Anzahl] - Privileged Insiders: [TODO: Anzahl] - Nation-State Actors: [TODO: Anzahl] - Other: [TODO: Anzahl]

16.5.3 5.3 Risk Overview

Risikoübersicht: - Critical Risk Combinations: [TODO: Anzahl] - High Risk Combinations: [TODO: Anzahl] - Medium Risk Combinations: [TODO: Anzahl] - Low Risk Combinations: [TODO: Anzahl]

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter mit TOE-spezifischen Assets und Agenten 2. Führe vollständige Asset-Identifikation durch 3. Dokumentiere alle relevanten Bedrohungsagenten 4. Bewerte Angriffspotenzial für alle Agenten 5. Erstelle Asset-Abhängigkeitsdiagramme 6. Überprüfe Konsistenz mit Threats (Template 0210) und Security Objectives (Template 0300)

ewpage

Chapter 17

Sicherheitsziele (Security Objectives)

Dokument-ID: 0300
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und passe die Inhalte an dein spezifisches TOE (Target of Evaluation) an.

17.1 1. Einleitung

Dieses Dokument definiert die Sicherheitsziele für das TOE **{{ meta.toe_name }}** und dessen Betriebsumgebung. Die Sicherheitsziele leiten sich aus der Sicherheitsproblem-Definition ab und beschreiben die beabsichtigten Sicherheitseigenschaften, die zur Bewältigung der identifizierten Bedrohungen, zur Einhaltung der organisatorischen Sicherheitsrichtlinien und zur Erfüllung der Annahmen erforderlich sind.

17.1.1 1.1 Zweck

Die Sicherheitsziele dienen als Brücke zwischen: - Der Sicherheitsproblem-Definition (Bedrohungen, OSPs, Annahmen) - Den Sicherheitsanforderungen (SFRs und SARs)

Sie beschreiben **was** erreicht werden soll, nicht **wie** es implementiert wird.

17.1.2 1.2 Struktur

Die Sicherheitsziele sind in zwei Kategorien unterteilt: - **Sicherheitsziele für das TOE (O.xxx)**: Ziele, die durch das TOE selbst erreicht werden - **Sicherheitsziele für die Umgebung (OE.xxx)**: Ziele, die durch die Betriebsumgebung erfüllt werden müssen

17.2 2. Sicherheitsziele für das TOE

17.2.1 2.1 Zugriffskontrolle und Authentifizierung

17.2.1.1 O.ACCESS_CONTROL

Beschreibung: Das TOE muss den Zugriff auf geschützte Ressourcen basierend auf Benutzeridentität und Berechtigungen kontrollieren.

Rationale: Dieses Ziel adressiert die Bedrohungen T.UNAUTHORIZED_ACCESS und T.PRIVILEGE_ESCALATION sowie die organisatorische Sicherheitsrichtlinie P.ACCESS_CONTROL.

[**TODO: Passe die Beschreibung an dein spezifisches TOE an**]

17.2.1.2 O.IDENTIFICATION_AUTHENTICATION

Beschreibung: Das TOE muss alle Benutzer eindeutig identifizieren und authentifizieren, bevor Zugriff auf geschützte Funktionen gewährt wird.

Rationale: Dieses Ziel adressiert die Bedrohung T.MASQUERADE und unterstützt O.ACCESS_CONTROL.

[**TODO: Ergänze weitere Authentifizierungsziele falls erforderlich**]

17.2.2 2.2 Audit und Nachvollziehbarkeit

17.2.2.1 O.AUDIT_GENERATION

Beschreibung: Das TOE muss sicherheitsrelevante Ereignisse aufzeichnen, einschließlich Benutzeraktionen, Sicherheitsverletzungen und Systemereignisse.

Rationale: Dieses Ziel adressiert die Bedrohung T.AUDIT_COMPROMISE und die organisatorische Sicherheitsrichtlinie P.ACCOUNTABILITY.

[**TODO: Definiere spezifische Audit-Anforderungen**]

17.2.2.2 O.AUDIT_PROTECTION

Beschreibung: Das TOE muss Audit-Aufzeichnungen vor unbefugter Änderung und Löschung schützen.

Rationale: Dieses Ziel adressiert die Bedrohung T.AUDIT_COMPROMISE und stellt die Integrität der Audit-Daten sicher.

[**TODO: Beschreibe Schutzmechanismen für Audit-Daten**]

17.2.3 2.3 Datenschutz und Vertraulichkeit

17.2.3.1 O.DATA_CONFIDENTIALITY

Beschreibung: Das TOE muss sensible Benutzerdaten vor unbefugter Offenlegung schützen.

Rationale: Dieses Ziel adressiert die Bedrohungen T.DATA_DISCLOSURE und T.EAVESDROPPING sowie die organisatorische Sicherheitsrichtlinie P.CONFIDENTIALITY.

[**TODO: Definiere welche Daten geschützt werden müssen**]

17.2.3.2 O.CRYPTOGRAPHIC_OPERATIONS

Beschreibung: Das TOE muss kryptografische Operationen zur Verschlüsselung und Integritätssicherung von Daten durchführen.

Rationale: Dieses Ziel unterstützt O.DATA_CONFIDENTIALITY und O.DATA_INTEGRITY durch Bereitstellung kryptografischer Mechanismen.

[**TODO: Spezifiziere erforderliche kryptografische Funktionen**]

17.2.4 2.4 Datenintegrität

17.2.4.1 O.DATA_INTEGRITY

Beschreibung: Das TOE muss die Integrität von Benutzerdaten und Systemdaten gegen unbefugte Änderung schützen.

Rationale: Dieses Ziel adressiert die Bedrohungen T.DATA_MODIFICATION und T.DATA_CORRUPTION sowie die organisatorische Sicherheitsrichtlinie P.INTEGRITY.

[**TODO: Beschreibe Integritätsschutzmechanismen**]

17.2.5 2.5 Sicherheitsmanagement

17.2.5.1 O.SECURITY_MANAGEMENT

Beschreibung: Das TOE muss autorisierten Administratoren die Verwaltung von Sicherheitsfunktionen und -richtlinien ermöglichen.

Rationale: Dieses Ziel adressiert die organisatorische Sicherheitsrichtlinie P.MANAGEMENT und ermöglicht die Konfiguration und Wartung des TOE.

[**TODO: Definiere Verwaltungsfunktionen**]

17.2.5.2 O.SECURE_STATE

Beschreibung: Das TOE muss in einem sicheren Zustand starten und bei Fehlern in einen sicheren Zustand übergehen.

Rationale: Dieses Ziel adressiert die Bedrohung T.MALFUNCTION und stellt sicher, dass das TOE auch bei Fehlern sicher bleibt.

[**TODO: Beschreibe sichere Zustände und Fehlerbehandlung**]

17.2.6 2.6 Selbstschutz

17.2.6.1 O.TSF_PROTECTION

Beschreibung: Das TOE muss seine eigenen Sicherheitsfunktionen (TSF) vor Manipulation und Umgehung schützen.

Rationale: Dieses Ziel adressiert die Bedrohungen T.TSF_COMPROMISE und T.TSF_BYPASS und stellt die Integrität der Sicherheitsfunktionen sicher.

[**TODO: Beschreibe TSF-Schutzmechanismen**]

17.2.7 2.7 Weitere TOE-Sicherheitsziele

[TODO: Ergänze weitere spezifische Sicherheitsziele für dein TOE]

17.2.7.1 O.[CUSTOM_OBJECTIVE_1]

Beschreibung: [TODO: Beschreibung]

Rationale: [TODO: Begründung und Bezug zu Bedrohungen/OSPs]

17.2.7.2 O.[CUSTOM_OBJECTIVE_2]

Beschreibung: [TODO: Beschreibung]

Rationale: [TODO: Begründung und Bezug zu Bedrohungen/OSPs]

17.3 3. Sicherheitsziele für die Umgebung

17.3.1 3.1 Physische Sicherheit

17.3.1.1 OE.PHYSICAL_PROTECTION

Beschreibung: Die Betriebsumgebung muss das TOE vor physischem Zugriff durch unbefugte Personen schützen.

Rationale: Dieses Ziel erfüllt die Annahme A.PHYSICAL_SECURITY und adressiert die Bedrohung T.PHYSICAL_ATTACK.

[TODO: Definiere erforderliche physische Schutzmaßnahmen]

17.3.2 3.2 Personal und Vertrauen

17.3.2.1 OE.TRUSTED_ADMIN

Beschreibung: Die Betriebsumgebung muss sicherstellen, dass Administratoren vertrauenswürdig, geschult und kompetent sind.

Rationale: Dieses Ziel erfüllt die Annahme A.TRUSTED_ADMIN und reduziert das Risiko von Insider-Bedrohungen.

[TODO: Beschreibe Anforderungen an Administratoren]

17.3.2.2 OE.USER_TRAINING

Beschreibung: Die Betriebsumgebung muss sicherstellen, dass Benutzer in der sicheren Verwendung des TOE geschult sind.

Rationale: Dieses Ziel erfüllt die Annahme A.USER_TRAINING und reduziert das Risiko von Benutzerfehlern.

[TODO: Definiere Schulungsanforderungen]

17.3.3 3.3 Netzwerk und Konnektivität

17.3.3.1 OE.NETWORK_PROTECTION

Beschreibung: Die Betriebsumgebung muss das TOE vor Netzwerkangriffen durch Firewalls, Intrusion Detection und andere Schutzmechanismen schützen.

Rationale: Dieses Ziel erfüllt die Annahme A.NETWORK_SECURITY und adressiert Bedrohungen aus dem Netzwerk.

[**TODO: Spezifiziere erforderliche Netzwerkschutzmaßnahmen**]

17.3.4 3.4 Externe Systeme und Dienste

17.3.4.1 OE.EXTERNAL_SYSTEMS

Beschreibung: Die Betriebsumgebung muss sicherstellen, dass externe Systeme, mit denen das TOE interagiert, vertrauenswürdig und sicher sind.

Rationale: Dieses Ziel erfüllt die Annahme A.EXTERNAL_SYSTEMS und reduziert Risiken durch Drittanbieter-Komponenten.

[**TODO: Definiere Anforderungen an externe Systeme**]

17.3.5 3.5 Zeitdienste

17.3.5.1 OE.TIME_STAMPS

Beschreibung: Die Betriebsumgebung muss zuverlässige Zeitstempel für Audit-Aufzeichnungen und Sicherheitsereignisse bereitstellen.

Rationale: Dieses Ziel erfüllt die Annahme A.TIME_SOURCE und unterstützt O.AUDIT_GENERATION.

[**TODO: Beschreibe Anforderungen an Zeitquellen**]

17.3.6 3.6 Weitere Umgebungsziele

[**TODO: Ergänze weitere spezifische Sicherheitsziele für die Umgebung**]

17.3.6.1 OE.[CUSTOM_ENV_OBJECTIVE_1]

Beschreibung: [TODO: Beschreibung]

Rationale: [TODO: Begründung und Bezug zu Annahmen]

17.3.6.2 OE.[CUSTOM_ENV_OBJECTIVE_2]

Beschreibung: [TODO: Beschreibung]

Rationale: [TODO: Begründung und Bezug zu Annahmen]

17.4 4. Zusammenfassung der Sicherheitsziele

17.4.1 4.1 TOE-Sicherheitsziele (Übersicht)

Ziel-ID	Kurzbeschreibung	Kategorie
O.ACCESS_CONTROL	Zugriffskontrolle auf Ressourcen	Zugriffskontrolle
O.IDENTIFICATION_AUTHENTICATION	Benutzeridentifikation und -authentifizierung	Zugriffskontrolle
O.AUDIT_GENERATION	Aufzeichnung sicherheitsrelevanter Ereignisse	Audit
O.AUDIT_PROTECTION	Schutz von Audit-Aufzeichnungen	Audit
O.DATA_CONFIDENTIALITY	Schutz sensibler Daten vor Offenlegung	Datenschutz
O.CRYPTOGRAPHIC_OPERATIONS	Kryptografische Operationen	Datenschutz
O.DATA_INTEGRITY	Schutz der Datenintegrität	Integrität
O.SECURITY_MANAGEMENT	Verwaltung von Sicherheitsfunktionen	Management
O.SECURE_STATE	Sicherer Zustand bei Start und Fehlern	Selbstschutz
O.TSF_PROTECTION	Schutz der Sicherheitsfunktionen	Selbstschutz
[**TODO: Weitere Ziele**]		

17.4.2 4.2 Umgebungsziele (Übersicht)

Ziel-ID	Kurzbeschreibung	Kategorie
OE.PHYSICAL_PROTECTION	Physischer Schutz des TOE	Physische Sicherheit
OE.TRUSTED_ADMIN	Vertrauenswürdige Administratoren	Personal
OE.USER_TRAINING	Benutzerschulung	Personal
OE.NETWORK_PROTECTION	Netzwerkschutz	Netzwerk
OE.EXTERNAL_SYSTEMS	Sichere externe Systeme	Integration
OE.TIME_STAMPS	Zuverlässige Zeitstempel	Infrastruktur
[**TODO: Weitere Ziele**]		

17.5 5. Nächste Schritte

Nach der Definition der Sicherheitsziele: 1. Erstelle die Rationale (Begründung) für die Sicherheitsziele (siehe Template 0310) 2. Erstelle die Coverage Matrix (siehe Template 0320) 3. Leite die Sicherheitsanforderungen (SFRs und SARs) aus den Zielen ab

17.6 6. Referenzen

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

Dokumenthistorie:

Version	Datum	Autor	Änderungen
{{ meta.version }}	{{ meta.date }}	{{ meta.owner }}	Initiale Version

ewpage

Chapter 18

Rationale für Sicherheitsziele (Security Objectives Rationale)

Dokument-ID: 0310
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und passe die Inhalte an dein spezifisches TOE (Target of Evaluation) an.

18.1 1. Einleitung

Dieses Dokument liefert die Rationale (Begründung) für die Sicherheitsziele des TOE **{{ meta.toe_name }}** und dessen Betriebsumgebung. Die Rationale demonstriert, dass die definierten Sicherheitsziele ausreichend und angemessen sind, um:

- Alle identifizierten Bedrohungen zu bewältigen
- Alle organisatorischen Sicherheitsrichtlinien (OSPs) umzusetzen
- Alle Annahmen über die Betriebsumgebung zu erfüllen

18.1.1 1.1 Zweck

Die Rationale dient als Nachweis für: - **Vollständigkeit**: Alle Elemente der Sicherheitsproblem-Definition sind durch Ziele abgedeckt - **Angemessenheit**: Jedes Ziel ist geeignet, die zugeordneten Bedrohungen/OSPs/Annahmen zu adressieren - **Rückverfolgbarkeit**: Klare Verbindung zwischen Sicherheitsproblemen und Zielen

18.1.2 1.2 Methodik

Für jedes Sicherheitsziel wird dokumentiert: 1. Welche Bedrohungen, OSPs oder Annahmen es adressiert 2. Wie es diese Sicherheitsprobleme bewältigt 3. Warum es angemessen und ausreichend

ist

18.2 2. Rationale für TOE-Sicherheitsziele

18.2.1 2.1 O.ACCESS_CONTROL

Adressierte Bedrohungen: - T.UNAUTHORIZED_ACCESS: Unbefugter Zugriff auf geschützte Ressourcen - T.PRIVILEGE_ESCALATION: Erlangung höherer Berechtigungen

Adressierte OSPs: - P.ACCESS_CONTROL: Zugriff muss basierend auf Berechtigungen kontrolliert werden

Rationale: Das Ziel O.ACCESS_CONTROL bewältigt die Bedrohungen T.UNAUTHORIZED_ACCESS und T.PRIVILEGE_ESCALATION, indem es sicherstellt, dass das TOE den Zugriff auf geschützte Ressourcen basierend auf Benutzeridentität und zugewiesenen Berechtigungen kontrolliert. Nur authentifizierte Benutzer mit entsprechenden Berechtigungen können auf Ressourcen zugreifen. Dies setzt die organisatorische Sicherheitsrichtlinie P.ACCESS_CONTROL um, die eine rollenbasierte Zugriffskontrolle vorschreibt.

[**TODO: Passe die Rationale an dein spezifisches TOE an**]

18.2.2 2.2 O.IDENTIFICATION_AUTHENTICATION

Adressierte Bedrohungen: - T.MASQUERADE: Vortäuschen einer falschen Identität

Rationale: Das Ziel O.IDENTIFICATION_AUTHENTICATION bewältigt die Bedrohung T.MASQUERADE, indem es sicherstellt, dass alle Benutzer eindeutig identifiziert und authentifiziert werden, bevor Zugriff auf geschützte Funktionen gewährt wird. Dies verhindert, dass Angreifer sich als legitime Benutzer ausgeben können. Das Ziel unterstützt auch O.ACCESS_CONTROL, da eine zuverlässige Identifikation Voraussetzung für eine wirksame Zugriffskontrolle ist.

[**TODO: Ergänze weitere Details zur Authentifizierung**]

18.2.3 2.3 O.AUDIT_GENERATION

Adressierte Bedrohungen: - T.AUDIT_COMPROMISE: Manipulation oder Löschung von Audit-Daten

Adressierte OSPs: - P.ACCOUNTABILITY: Benutzeraktionen müssen nachvollziehbar sein

Rationale: Das Ziel O.AUDIT_GENERATION bewältigt die Bedrohung T.AUDIT_COMPROMISE teilweise, indem es sicherstellt, dass sicherheitsrelevante Ereignisse aufgezeichnet werden. Die Aufzeichnung ermöglicht die Nachvollziehbarkeit von Benutzeraktionen und Sicherheitsereignissen, was die organisatorische Sicherheitsrichtlinie P.ACCOUNTABILITY umsetzt. In Kombination mit O.AUDIT_PROTECTION wird ein vollständiger Schutz der Audit-Daten erreicht.

[**TODO: Definiere welche Ereignisse aufgezeichnet werden**]

18.2.4 2.4 O.AUDIT_PROTECTION

Adressierte Bedrohungen: - T.AUDIT_COMPROMISE: Manipulation oder Löschung von Audit-Daten

Rationale: Das Ziel O.AUDIT_PROTECTION bewältigt die Bedrohung T.AUDIT_COMPROMISE, indem es sicherstellt, dass Audit-Aufzeichnungen vor unbefugter Änderung und Löschung geschützt sind. Dies gewährleistet die Integrität und Verfügbarkeit der Audit-Daten, die für forensische Analysen und Compliance-Nachweise erforderlich sind. Das Ziel ergänzt O.AUDIT_GENERATION und stellt einen vollständigen Audit-Schutz sicher.

[**TODO: Beschreibe Schutzmechanismen**]

18.2.5 2.5 O.DATA_CONFIDENTIALITY

Adressierte Bedrohungen: - T.DATA_DISCLOSURE: Unbefugte Offenlegung sensibler Daten - T.EAVESDROPPING: Abhören von Datenübertragungen

Adressierte OSPs: - P.CONFIDENTIALITY: Sensible Daten müssen vertraulich behandelt werden

Rationale: Das Ziel O.DATA_CONFIDENTIALITY bewältigt die Bedrohungen T.DATA_DISCLOSURE und T.EAVESDROPPING, indem es sicherstellt, dass sensible Benutzerdaten vor unbefugter Offenlegung geschützt werden. Dies wird durch Zugriffskontrolle, Verschlüsselung und sichere Datenübertragung erreicht. Das Ziel setzt die organisatorische Sicherheitsrichtlinie P.CONFIDENTIALITY um, die den Schutz vertraulicher Informationen vorschreibt.

[**TODO: Spezifiziere geschützte Datentypen**]

18.2.6 2.6 O.CRYPTOGRAPHIC_OPERATIONS

Adressierte Bedrohungen: - T.DATA_DISCLOSURE: Unbefugte Offenlegung sensibler Daten - T.DATA_MODIFICATION: Unbefugte Änderung von Daten

Rationale: Das Ziel O.CRYPTOGRAPHIC_OPERATIONS unterstützt O.DATA_CONFIDENTIALITY und O.DATA_INTEGRITY, indem es kryptografische Mechanismen zur Verschlüsselung und Integritätssicherung von Daten bereitstellt. Kryptografische Operationen schützen Daten sowohl im Ruhezustand als auch während der Übertragung vor Offenlegung und Manipulation.

[**TODO: Definiere erforderliche kryptografische Algorithmen**]

18.2.7 2.7 O.DATA_INTEGRITY

Adressierte Bedrohungen: - T.DATA_MODIFICATION: Unbefugte Änderung von Daten - T.DATA_CORRUPTION: Beschädigung von Daten

Adressierte OSPs: - P.INTEGRITY: Datenintegrität muss gewährleistet sein

Rationale: Das Ziel O.DATA_INTEGRITY bewältigt die Bedrohungen T.DATA_MODIFICATION und T.DATA_CORRUPTION, indem es sicherstellt, dass Benutzerdaten und Systemdaten vor unbefugter Änderung geschützt sind. Dies wird durch Integritätsprüfungen, Zugriffskontrolle und kryptografische Mechanismen erreicht. Das Ziel setzt die organisatorische Sicherheitsrichtlinie P.INTEGRITY um.

[**TODO: Beschreibe Integritätsschutzmechanismen**]

18.2.8 2.8 O.SECURITY_MANAGEMENT

Adressierte OSPs: - P.MANAGEMENT: Sicherheitsfunktionen müssen verwaltbar sein

Rationale: Das Ziel O.SECURITY_MANAGEMENT setzt die organisatorische Sicherheitsrichtlinie P.MANAGEMENT um, indem es autorisierten Administratoren die Verwaltung von Sicherheitsfunktionen und -richtlinien ermöglicht. Dies umfasst die Konfiguration von Zugriffskontrollrichtlinien, Audit-Einstellungen und anderen Sicherheitsparametern. Eine wirksame Verwaltung ist Voraussetzung für die Aufrechterhaltung der Sicherheit über den gesamten Lebenszyklus des TOE.

[**TODO: Definiere Verwaltungsfunktionen**]

18.2.9 2.9 O.SECURE_STATE

Adressierte Bedrohungen: - T.MALFUNCTION: Fehlfunktion des TOE

Rationale: Das Ziel O.SECURE_STATE bewältigt die Bedrohung T.MALFUNCTION, indem es sicherstellt, dass das TOE in einem sicheren Zustand startet und bei Fehlern in einen sicheren Zustand übergeht. Dies verhindert, dass Fehlfunktionen zu Sicherheitsverletzungen führen. Das TOE muss auch bei unerwarteten Ereignissen seine Sicherheitseigenschaften aufrechterhalten.

[**TODO: Beschreibe sichere Zustände**]

18.2.10 2.10 O.TSF_PROTECTION

Adressierte Bedrohungen: - T.TSF_COMPROMISE: Manipulation der Sicherheitsfunktionen - T.TSF_BYPASS: Umgehung der Sicherheitsfunktionen

Rationale: Das Ziel O.TSF_PROTECTION bewältigt die Bedrohungen T.TSF_COMPROMISE und T.TSF_BYPASS, indem es sicherstellt, dass die Sicherheitsfunktionen (TSF) des TOE vor Manipulation und Umgehung geschützt sind. Dies ist fundamental für die Wirksamkeit aller anderen Sicherheitsziele, da kompromittierte Sicherheitsfunktionen alle Schutzmechanismen unwirksam machen würden.

[**TODO: Beschreibe TSF-Schutzmechanismen**]

18.2.11 2.11 Weitere TOE-Sicherheitsziele

[**TODO: Ergänze Rationale für weitere spezifische Sicherheitsziele**]

18.2.11.1 O.[CUSTOM_OBJECTIVE_1]

Adressierte Bedrohungen/OSPs: - [TODO: Liste Bedrohungen/OSPs auf]

Rationale: [TODO: Erkläre, wie das Ziel die Bedrohungen/OSPs bewältigt]

18.3 3. Rationale für Umgebungsziele

18.3.1 3.1 OE.PHYSICAL_PROTECTION

Erfüllte Annahmen: - A.PHYSICAL_SECURITY: Das TOE wird in einer physisch gesicherten Umgebung betrieben

Adressierte Bedrohungen: - T.PHYSICAL_ATTACK: Physischer Angriff auf das TOE

Rationale: Das Ziel OE.PHYSICAL_PROTECTION erfüllt die Annahme A.PHYSICAL_SECURITY, indem es sicherstellt, dass die Betriebsumgebung das TOE vor physischem Zugriff durch unbefugte Personen schützt. Dies bewältigt auch die Bedrohung T.PHYSICAL_ATTACK. Physische Schutzmaßnahmen wie Zugangskontrollen, Überwachung und sichere Räumlichkeiten verhindern, dass Angreifer direkten Zugriff auf die Hardware erhalten.

[**TODO: Definiere erforderliche physische Schutzmaßnahmen**]

18.3.2 3.2 OE.TRUSTED_ADMIN

Erfüllte Annahmen: - A.TRUSTED_ADMIN: Administratoren sind vertrauenswürdig und kompetent

Rationale: Das Ziel OE.TRUSTED_ADMIN erfüllt die Annahme A.TRUSTED_ADMIN, indem es sicherstellt, dass Administratoren vertrauenswürdig, geschult und kompetent sind. Dies reduziert das Risiko von Insider-Bedrohungen und Fehlkonfigurationen. Vertrauenswürdige Administratoren sind essentiell, da sie weitreichende Berechtigungen haben und Sicherheitsmechanismen umgehen könnten.

[**TODO: Beschreibe Anforderungen an Administratoren**]

18.3.3 3.3 OE.USER_TRAINING

Erfüllte Annahmen: - A.USER_TRAINING: Benutzer sind in der sicheren Verwendung des TOE geschult

Rationale: Das Ziel OE.USER_TRAINING erfüllt die Annahme A.USER_TRAINING, indem es sicherstellt, dass Benutzer in der sicheren Verwendung des TOE geschult sind. Dies reduziert das Risiko von Benutzerfehlern, Social Engineering und unbeabsichtigten Sicherheitsverletzungen. Geschulte Benutzer verstehen Sicherheitsrichtlinien und können verdächtige Aktivitäten erkennen.

[**TODO: Definiere Schulungsanforderungen**]

18.3.4 3.4 OE.NETWORK_PROTECTION

Erfüllte Annahmen: - A.NETWORK_SECURITY: Das Netzwerk ist durch Firewalls und andere Mechanismen geschützt

Rationale: Das Ziel OE.NETWORK_PROTECTION erfüllt die Annahme A.NETWORK_SECURITY, indem es sicherstellt, dass die Betriebsumgebung das TOE vor Netzwerkangriffen schützt. Firewalls, Intrusion Detection Systeme und Netzwerksegmentierung reduzieren die Angriffsfläche und verhindern unbefugten Netzwerkzugriff auf das TOE.

[**TODO: Spezifiziere erforderliche Netzwerkschutzmaßnahmen**]

18.3.5 3.5 OE.EXTERNAL_SYSTEMS

Erfüllte Annahmen: - A.EXTERNAL_SYSTEMS: Externe Systeme sind vertrauenswürdig und sicher

Rationale: Das Ziel OE.EXTERNAL_SYSTEMS erfüllt die Annahme A.EXTERNAL_SYSTEMS, indem es sicherstellt, dass externe Systeme, mit denen das TOE interagiert, vertrauenswürdig

und sicher sind. Dies reduziert Risiken durch kompromittierte Drittanbieter-Komponenten oder unsichere Schnittstellen. Die Umgebung muss die Sicherheit externer Systeme bewerten und überwachen.

[**TODO: Definiere Anforderungen an externe Systeme**]

18.3.6 3.6 OE.TIME_STAMPS

Erfüllte Annahmen: - A.TIME_SOURCE: Eine zuverlässige Zeitquelle ist verfügbar

Rationale: Das Ziel OE.TIME_STAMPS erfüllt die Annahme A.TIME_SOURCE, indem es sicherstellt, dass die Betriebsumgebung zuverlässige Zeitstempel für Audit-Aufzeichnungen und Sicherheitsereignisse bereitstellt. Genaue Zeitstempel sind essentiell für forensische Analysen, Korrelation von Ereignissen und Compliance-Nachweise. Das Ziel unterstützt O.AUDIT_GENERATION.

[**TODO: Beschreibe Anforderungen an Zeitquellen**]

18.3.7 3.7 Weitere Umgebungsziele

[**TODO: Ergänze Rationale für weitere Umgebungsziele**]

18.3.7.1 OE.[CUSTOM_ENV_OBJECTIVE]

Erfüllte Annahmen: - [TODO: Liste Annahmen auf]

Rationale: [TODO: Erkläre, wie das Ziel die Annahmen erfüllt]

18.4 4. Vollständigkeitsnachweis

18.4.1 4.1 Abdeckung der Bedrohungen

Die folgende Tabelle zeigt, dass jede identifizierte Bedrohung durch mindestens ein Sicherheitsziel adressiert wird:

Bedrohung	Adressierende Ziele	Status
T.UNAUTHORIZED_ACCESS	O.ACCESS_CONTROL	Abgedeckt
T.PRIVILEGE_ESCALATION	O.ACCESS_CONTROL	Abgedeckt
T.MASQUERADE	O.IDENTIFICATION_AUTHENTICATION	Abgedeckt
T.AUDIT_COMPROMISE	O.AUDIT_GENERATION, O.AUDIT_PROTECTION	Abgedeckt
T.DATA_DISCLOSURE	O.DATA_CONFIDENTIALITY, O.CRYPTOGRAPHIC_OPERATIONS	Abgedeckt
T.EAVESDROPPING	O.DATA_CONFIDENTIALITY, O.CRYPTOGRAPHIC_OPERATIONS	Abgedeckt
T.DATA_MODIFICATION	O.DATA_INTEGRITY, O.CRYPTOGRAPHIC_OPERATIONS	Abgedeckt
T.DATA_CORRUPTION	O.DATA_INTEGRITY	Abgedeckt
T.MALFUNCTION	O.SECURE_STATE	Abgedeckt
T.TSF_COMPROMISE	O.TSF_PROTECTION	Abgedeckt
T.TSF_BYPASS	O.TSF_PROTECTION	Abgedeckt
T.PHYSICAL_ATTACK	OE.PHYSICAL_PROTECTION	Abgedeckt

Bedrohung	Adressierende Ziele	Status
[**TODO: Weitere Bedrohungen**]		

Ergebnis: Alle Bedrohungen sind durch Sicherheitsziele abgedeckt.

18.4.2 4.2 Abdeckung der organisatorischen Sicherheitsrichtlinien

Die folgende Tabelle zeigt, dass jede OSP durch mindestens ein Sicherheitsziel umgesetzt wird:

OSP	Umsetzende Ziele	Status
P.ACCESS_CONTROL	O.ACCESS_CONTROL	Abgedeckt
P.ACCOUNTABILITY	O.AUDIT_GENERATION, O.AUDIT_PROTECTION	Abgedeckt
P.CONFIDENTIALITY	O.DATA_CONFIDENTIALITY	Abgedeckt
P.INTEGRITY	O.DATA_INTEGRITY	Abgedeckt
P.MANAGEMENT	O.SECURITY_MANAGEMENT	Abgedeckt
[**TODO: Weitere OSPs**]		

Ergebnis: Alle OSPs sind durch Sicherheitsziele umgesetzt.

18.4.3 4.3 Abdeckung der Annahmen

Die folgende Tabelle zeigt, dass jede Annahme durch mindestens ein Umgebungsziel erfüllt wird:

Annahme	Erfüllende Ziele	Status
A.PHYSICAL_SECURITY	OE.PHYSICAL_PROTECTION	Abgedeckt
A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN	Abgedeckt
A.USER_TRAINING	OE.USER_TRAINING	Abgedeckt
A.NETWORK_SECURITY	OE.NETWORK_PROTECTION	Abgedeckt
A.EXTERNAL_SYSTEMS	OE.EXTERNAL_SYSTEMS	Abgedeckt
A.TIME_SOURCE	OE.TIME_STAMPS	Abgedeckt
[**TODO: Weitere Annahmen**]		

Ergebnis: Alle Annahmen sind durch Umgebungsziele erfüllt.

18.4.4 4.4 Rückverfolgbarkeit der Sicherheitsziele

Die folgende Tabelle zeigt, dass jedes Sicherheitsziel auf mindestens eine Bedrohung, OSP oder Annahme zurückgeführt werden kann:

Sicherheitsziel	Bedrohungen	OSPs	Annahmen	Status
O.ACCESS_CONTROL	T.UNAUTHORIZED_ACCESS, T.PRIVILEGE_ESCALATION	P.ACCESS_CONTROL	-	Gerechtfertigt
O.IDENTIFICATION_AUTHENTICATION	T.MASQUERADE	-	-	Gerechtfertigt
O.AUDIT_GENERATION	T.AUDIT_COMPROMISE	P.ACCOUNTABILITY	-	Gerechtfertigt
O.AUDIT_PROTECTION	T.AUDIT_COMPROMISE	-	-	Gerechtfertigt
O.DATA_CONFIDENTIALITY	T.DATA_DISCLOSURE, T.EAVESDROPPING	P.CONFIDENTIALITY	-	Gerechtfertigt
O.CRYPTOGRAPHIC_OPERATIONS	T.DATA_DISCLOSURE, T.DATA_MODIFICATION	-	-	Gerechtfertigt
O.DATA_INTEGRITY	T.DATA_MODIFICATION, T.DATA_CORRUPTION	P.INTEGRITY	-	Gerechtfertigt
O.SECURITY_MANAGEMENT	-	P.MANAGEMENT	-	Gerechtfertigt
O.SECURE_STATE	T.MALFUNCTION	-	-	Gerechtfertigt
O.TSF_PROTECTION	T.TSF_COMPROMISE, T.TSF_BYPASS	-	-	Gerechtfertigt
OE.PHYSICAL_PROTECTION	T.PHYSICAL_ATTACK	-	A.PHYSICAL_SECURITY	Gerechtfertigt
OE.TRUSTED_ADMIN	-	-	A.TRUSTED_ADMIN	Gerechtfertigt
OE.USER_TRAINING	-	-	A.USER_TRAINING	Gerechtfertigt
OE.NETWORK_PROTECTION	-	-	A.NETWORK_SECURITY	Gerechtfertigt
OE.EXTERNAL_SYSTEMS	-	-	A.EXTERNAL_SYSTEMS	Gerechtfertigt
OE.TIME_STAMPS	-	-	A.TIME_SOURCE	Gerechtfertigt
[**TODO: Weitere Ziele**]				

Ergebnis: Alle Sicherheitsziele sind gerechtfertigt.

18.5 5. Zusammenfassung

Die Rationale demonstriert, dass die definierten Sicherheitsziele:

1. **Vollständig** sind: Alle Bedrohungen, OSPs und Annahmen sind abgedeckt
2. **Angemessen** sind: Jedes Ziel ist geeignet, die zugeordneten Sicherheitsprobleme zu bewältigen
3. **Rückverfolgbar** sind: Jedes Ziel kann auf Sicherheitsprobleme zurückgeführt werden
4. **Konsistent** sind: Keine Widersprüche zwischen Zielen

Die Sicherheitsziele bilden eine solide Grundlage für die Ableitung der Sicherheitsanforderungen (SFRs und SARs) im nächsten Schritt des Security Target.

18.6 6. Nächste Schritte

Nach der Rationale für Sicherheitsziele: 1. Erstelle die Coverage Matrix (siehe Template 0320) 2. Leite die Sicherheitsanforderungen (SFRs und SARs) aus den Zielen ab (siehe Template 0400-0450)

18.7 7. Referenzen

- ISO/IEC 15408-1: Security Target Evaluation
- Template 0200-0240: Sicherheitsproblem-Definition
- Template 0300: Sicherheitsziele
- Template 0320: Security Objectives Coverage Matrix
- Template 0400-0450: Sicherheitsanforderungen

Dokumenthistorie:

Version	Datum	Autor	Änderungen
{{ meta.version }}	{{ meta.date }}	{{ meta.owner }}	Initiale Version

ewpage

Chapter 19

Security Objectives Coverage Matrix

Dokument-ID: 0320
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und passe die Inhalte an dein spezifisches TOE (Target of Evaluation) an.

19.1 1. Einleitung

Dieses Dokument präsentiert die Coverage Matrix (Abdeckungsmatrix) für die Sicherheitsziele des TOE **{{ meta.toe_name }}**. Die Matrix visualisiert die Beziehungen zwischen:

- Sicherheitszielen und Bedrohungen
- Sicherheitszielen und organisatorischen Sicherheitsrichtlinien (OSPs)
- Umgebungszielen und Annahmen

19.1.1 1.1 Zweck

Die Coverage Matrix dient als: - **Vollständigkeitsnachweis**: Alle Elemente der Sicherheitsproblem-Definition sind abgedeckt - **Rückverfolgbarkeitswerkzeug**: Schnelle Identifikation von Beziehungen - **Audit-Dokumentation**: Nachweis für Evaluatoren und Auditoren - **Änderungsmanagement**: Identifikation von Auswirkungen bei Änderungen

19.1.2 1.2 Legende

Symbol	Bedeutung
X	Primäre Zuordnung - Das Ziel adressiert direkt die Bedrohung/OSP/Annahme

Symbol	Bedeutung
•	Unterstützende Zuordnung - Das Ziel unterstützt indirekt
-	Keine Zuordnung

19.2 2. Bedrohungen vs. Sicherheitsziele

Die folgende Matrix zeigt, welche Sicherheitsziele welche Bedrohungen adressieren:

Bedrohung	O.ACCESS_CONTROL	O.IDENTIFICATION_AUTHENTICATION	O.AUDIT_GENERATION	O.CONFIDENTIALITY	O.INTEGRITY	O.MANAGEMENT	O.SECURE_STATE_PRESERVATION	O.SYSTEM_PROTECTION
T.UNAUTHORIZED_ACCESS	-	-	-	-	-	-	-	-
T.PRIVILEGE_ESCALATION	-	-	-	-	-	-	-	-
T.MASQUERADE	-	-	-	-	-	-	-	-
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: Weitere Bedrohungen]								

Analyse: - Alle Bedrohungen sind durch mindestens ein Sicherheitsziel abgedeckt - Mehrfachabdeckung zeigt Defense-in-Depth Ansatz - **[TODO: Ergänze spezifische Analysen für dein TOE]**

19.3 3. Organisatorische Sicherheitsrichtlinien vs. Sicherheitsziele

Die folgende Matrix zeigt, welche Sicherheitsziele welche OSPs umsetzen:

OSP	O.ACCESS_CONTROL	O.IDENTIFICATION_AUTHENTICATION	O.AUDIT_GENERATION	O.CONFIDENTIALITY	O.INTEGRITY	O.MANAGEMENT	O.SECURE_STATE_PRESERVATION	O.SYSTEM_PROTECTION
P.ACCESS_CONTROL	•	-	-	-	-	-	-	-
P.ACCOUNTABILITY	X	X	-	-	-	-	-	-
P.CONFIDENTIALITY	•	X	•	-	-	-	-	-
P.INTEGRITY	-	-	-	•	X	-	-	-
P.MANAGEMENT	-	-	-	-	-	X	-	-

OSP.ACCESS_CONTROL_ENFORCEMENT	[TODO: Weitere OSPs]

Analyse: - Alle OSPs sind durch mindestens ein Sicherheitsziel umgesetzt - Klare Zuordnung zwischen Richtlinien und technischen Zielen - [**TODO: Ergänze spezifische Analysen für dein TOE**]

19.4 4. Annahmen vs. Umgebungsziele

Die folgende Matrix zeigt, welche Umgebungsziele welche Annahmen erfüllen:

Annahme	OE.PHYSICAL_PROTECTION	OE.TRUSTED_ADMIN	OE.USER_TRAINING	OE.NETWORK_PROTECTION	OE.EXTERNAL_SYSTEMS	[TODO]
A.PHYSICAL_SECURITY	-	-	-	-		
A.TRUSTED_ADMIN	-	X	-	-		
A.USER_TRAINING	X	-	-	-		
A.NETWORK_SECURITY	-	X	-	-		
A.EXTERNAL_SYSTEMS	-	-	X	-		
A.TIME_SOURCE	-	-	-	X		
[**TODO: Weitere Annahmen**]						

Analyse: - Alle Annahmen sind durch mindestens ein Umgebungsziel erfüllt - Klare Trennung zwischen TOE- und Umgebungsverantwortlichkeiten - [**TODO: Ergänze spezifische Analysen für dein TOE**]

19.5 5. Umgekehrte Rückverfolgbarkeit: Sicherheitsziele zu Sicherheitsproblemen

Die folgende Matrix zeigt die umgekehrte Perspektive - welche Bedrohungen/OSPs/Annahmen jedes Sicherheitsziel rechtfertigen:

19.5.1 5.1 TOE-Sicherheitsziele

Sicherheitsziel	Adressierte Bedrohungen	Umgesetzte OSPs	Begründung
O.ACCESS_CONTROL	T.UNAUTHORIZED_ACCESS, T.PRIVILEGE_ESCALATION	P.ACCESS_CONTROL	Kontrolliert Zugriff auf Ressourcen
O.IDENTIFICATION_AUTHENTICATION	T.MASQUERADE	-	Verhindert Identitätsvortäuschung
O.AUDIT_GENERATION	T.AUDIT_COMPROMISE	P.ACCOUNTABILITY	Zeichnet sicherheitsrelevante Ereignisse auf
O.AUDIT_PROTECTION	T.AUDIT_COMPROMISE	-	Schützt Audit-Daten vor Manipulation
O.DATA_CONFIDENTIALITY	T.DATA_DISCLOSURE, T.EAVESDROPPING	P.CONFIDENTIALITY	Schützt sensible Daten vor Offenlegung
O.CRYPTOGRAPHIC_OPERATIONS	T.DATA_DISCLOSURE, T.DATA_MODIFICATION	-	Bietet kryptografische Mechanismen
O.DATA_INTEGRITY	T.DATA_MODIFICATION, T.DATA_CORRUPTION	P.INTEGRITY	Schützt Datenintegrität
O.SECURITY_MANAGEMENT	-	P.MANAGEMENT	Ermöglicht Verwaltung von Sicherheitsfunktionen
O.SECURE_STATE	T.MALFUNCTION	-	Gewährleistet sicheren Zustand bei Fehlern
O.TSF_PROTECTION	T.TSF_COMPROMISE, T.TSF_BYPASS	-	Schützt Sicherheitsfunktionen selbst
[**TODO: Weitere Ziele**]			

Ergebnis: Alle TOE-Sicherheitsziele sind durch Bedrohungen oder OSPs gerechtfertigt

19.5.2 5.2 Umgebungsziele

Umgebungszieł	Erfüllte Annahmen	Adressierte Bedrohungen	Begründung
OE.PHYSICAL_PROTECTION	A.PHYSICAL_SECURITY	T.PHYSICAL_ATTACK	Schützt TOE vor physischem Zugriff

Umgebungsziel	Erfüllte Annahmen	Adressierte Bedrohungen	Begründung
OE.TRUSTED_ADMIN	A.TRUSTED_ADMIN	-	Stellt vertrauenswürdige Administratoren sicher
OE.USER_TRAINING	A.USER_TRAINING	-	Schult Benutzer in sicherer Verwendung
OE.NETWORK_PROTECTION	A.NETWORK_SECURITY	-	Schützt TOE vor Netzwerkangriffen
OE.EXTERNAL_SYSTEMS	A.EXTERNAL_SYSTEMS	-	Stellt Sicherheit externer Systeme sicher
OE.TIME_STAMPS	A.TIME_SOURCE	-	Bietet zuverlässige Zeitstempel
[**TODO: Weitere Ziele**]			

Ergebnis: Alle Umgebungsziele sind durch Annahmen gerechtfertigt

19.6 6. Vollständigkeitsanalyse

19.6.1 6.1 Bedrohungsabdeckung

Gesamtzahl der Bedrohungen: 12 [**TODO: Aktualisiere Anzahl**]
Abgedeckte Bedrohungen: 12 [**TODO: Aktualisiere Anzahl**]
Nicht abgedeckte Bedrohungen: 0 [**TODO: Aktualisiere Anzahl**]

Status: Vollständig abgedeckt

[**TODO: Liste nicht abgedeckte Bedrohungen auf, falls vorhanden**]

19.6.2 6.2 OSP-Abdeckung

Gesamtzahl der OSPs: 5 [**TODO: Aktualisiere Anzahl**]
Umgesetzte OSPs: 5 [**TODO: Aktualisiere Anzahl**]
Nicht umgesetzte OSPs: 0 [**TODO: Aktualisiere Anzahl**]

Status: Vollständig umgesetzt

[**TODO: Liste nicht umgesetzte OSPs auf, falls vorhanden**]

19.6.3 6.3 Annahmenabdeckung

Gesamtzahl der Annahmen: 6 [**TODO: Aktualisiere Anzahl**]
Erfüllte Annahmen: 6 [**TODO: Aktualisiere Anzahl**]
Nicht erfüllte Annahmen: 0 [**TODO: Aktualisiere Anzahl**]

Status: Vollständig erfüllt

[**TODO: Liste nicht erfüllte Annahmen auf, falls vorhanden**]

19.6.4 6.4 Zielrechtfertigung

Gesamtzahl der Sicherheitsziele: 16 [**TODO: Aktualisiere Anzahl**]
Gerechtfertigte Ziele: 16 [**TODO: Aktualisiere Anzahl**]
Nicht gerechtfertigte Ziele: 0 [**TODO: Aktualisiere Anzahl**]

Status: Alle Ziele gerechtfertigt

[**TODO: Liste nicht gerechtfertigte Ziele auf, falls vorhanden**]

19.7 7. Lückenanalyse

19.7.1 7.1 Identifizierte Lücken

[**TODO: Dokumentiere identifizierte Lücken in der Abdeckung**]

Beispiel: - **Lücke 1:** Bedrohung T.XXX ist nicht durch Sicherheitsziele abgedeckt - **Auswirkung:** [Beschreibung] - **Empfohlene Maßnahme:** Ergänze Sicherheitsziel O.XXX

- **Lücke 2:** Sicherheitsziel O.YYY ist nicht durch Bedrohungen/OSPs gerechtfertigt
  - **Auswirkung:** [Beschreibung]
  - **Empfohlene Maßnahme:** Entferne Ziel oder identifiziere rechtfertigende Bedrohung

Aktueller Status: Keine Lücken identifiziert

19.7.2 7.2 Redundanzen und Überlappungen

[**TODO: Dokumentiere Redundanzen zwischen Sicherheitszielen**]

Beispiel: - **Überlappung 1:** O.XXX und O.YYY adressieren beide T.ZZZ - **Analyse:** [Ist dies beabsichtigt? Defense-in-Depth?] - **Empfehlung:** [Konsolidieren oder beibehalten]

Aktueller Status: Überlappungen sind beabsichtigt (Defense-in-Depth)

19.8 8. Änderungsmanagement

19.8.1 8.1 Auswirkungsanalyse bei Änderungen

Wenn Änderungen an der Sicherheitsproblem-Definition oder den Sicherheitszielen vorgenommen werden, muss die Coverage Matrix aktualisiert werden:

Bei Hinzufügen einer neuen Bedrohung: 1. Füge Zeile in Matrix 2 hinzu 2. Identifiziere adressierende Sicherheitsziele 3. Falls keine Ziele vorhanden: Erstelle neues Sicherheitsziel 4. Aktualisiere Vollständigkeitsanalyse

Bei Hinzufügen eines neuen Sicherheitsziels: 1. Füge Spalte in Matrix 2 und 3 hinzu 2. Identifiziere adressierte Bedrohungen/OSPs 3. Falls keine Bedrohungen/OSPs: Prüfe Notwendigkeit des Ziels 4. Aktualisiere umgekehrte Rückverfolgbarkeit

Bei Entfernen einer Bedrohung: 1. Entferne Zeile aus Matrix 2 2. Prüfe, ob zugeordnete Sicherheitsziele noch gerechtfertigt sind 3. Aktualisiere Vollständigkeitsanalyse

Bei Entfernen eines Sicherheitsziels: 1. Entferne Spalte aus Matrizen 2. Prüfe, ob alle Bedrohungen/OSPs noch abgedeckt sind 3. Falls nicht: Identifiziere alternatives Ziel oder erstelle neues Ziel

19.8.2 8.2 Änderungshistorie

Datum	Änderung	Auswirkung	Bearbeiter
{{ meta.date }} [**TODO**]	Initiale Version	-	{{ meta.owner }}

19.9 9. Zusammenfassung

Die Coverage Matrix demonstriert:

1. **Vollständigkeit:**
   - Alle Bedrohungen sind durch Sicherheitsziele abgedeckt
   - Alle OSPs sind durch Sicherheitsziele umgesetzt
   - Alle Annahmen sind durch Umgebungsziele erfüllt
2. **Rückverfolgbarkeit:**
   - Alle Sicherheitsziele sind durch Bedrohungen/OSPs gerechtfertigt
   - Alle Umgebungsziele sind durch Annahmen gerechtfertigt
3. **Konsistenz:**
   - Keine Lücken in der Abdeckung
   - Keine ungerechtfertigten Ziele

Die Sicherheitsziele bilden eine vollständige und konsistente Grundlage für die Ableitung der Sicherheitsanforderungen (SFRs und SARs).

19.10 10. Nächste Schritte

Nach der Coverage Matrix: 1. Leite Sicherheitsanforderungen (SFRs) aus den TOE-Sicherheitszielen ab (siehe Template 0400-0450) 2. Definiere Sicherheitsanforderungen für die Umgebung basierend auf Umgebungszielen 3. Erstelle Rationale für Sicherheitsanforderungen

19.11 11. Referenzen

- ISO/IEC 15408-1: Security Target Evaluation
- ISO/IEC 15408-2: Security Functional Components
- Template 0200-0240: Sicherheitsproblem-Definition
- Template 0300: Sicherheitsziele
- Template 0310: Rationale für Sicherheitsziele

- Template 0400-0450: Sicherheitsanforderungen

Dokumenthistorie:

Version	Datum	Autor	Änderungen
{{ meta.version }}	{{ meta.date }}	{{ meta.owner }}	Initiale Version

ewpage

Chapter 20

Zusammenfassung der Sicherheitsziele (Security Objectives Summary)

Dokument-ID: 0330
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und passe die Inhalte an dein spezifisches TOE (Target of Evaluation) an.

20.1 1. Einleitung

Dieses Dokument bietet eine kompakte Zusammenfassung aller Sicherheitsziele für das TOE **{{ meta.toe_name }}** und dessen Betriebsumgebung. Die Sicherheitsziele beschreiben die beabsichtigten Sicherheitseigenschaften, die zur Bewältigung der identifizierten Bedrohungen, zur Einhaltung der organisatorischen Sicherheitsrichtlinien und zur Erfüllung der Annahmen erforderlich sind.

20.1.1 1.1 Zweck

Diese Zusammenfassung dient als: - **Schnellreferenz** für alle Sicherheitsziele - **Executive Summary** für Management-Entscheidungen - **Kommunikationswerkzeug** für Stakeholder - **Audit-Dokumentation** für Evaluatoren

20.1.2 1.2 Dokumentstruktur

- Abschnitt 2: Übersicht der TOE-Sicherheitsziele
- Abschnitt 3: Übersicht der Umgebungsziele
- Abschnitt 4: Kategorisierung nach Sicherheitsbereichen
- Abschnitt 5: Abdeckungsstatistiken

- Abschnitt 6: Grafische Darstellungen

20.2 2. TOE-Sicherheitsziele (Übersicht)

Die folgenden Sicherheitsziele werden durch das TOE selbst erfüllt:

ID	Ziel	Kurzbeschreibung	Kategorie	Priorität
O.ACCESS_CONTROL	Zugriffskontrolle	Kontrolliert Zugriff auf geschützte Ressourcen basierend auf Benutzeridentität und Berechtigungen	Zugriffskontrolle	Hoch
O.IDENTIFICATION_AUTHENTICATION	Identifizierung & Authentifizierung	Identifiziert und authentifiziert alle Benutzer vor Zugriff auf geschützte Funktionen	Zugriffskontrolle	Hoch
O.AUDIT_GENERATION	Audit-Aufzeichnung	Zeichnet sicherheitsrelevante Ereignisse auf	Audit & Nachvollziehbarkeit	Hoch
O.AUDIT_PROTECTION	Audit-Schutz	Schützt Audit-Aufzeichnungen vor unbefugter Änderung und Löschung	Audit & Nachvollziehbarkeit	Hoch
O.DATA_CONFIDENTIALITY	Datenvertraulichkeit	Schützt sensible Benutzerdaten vor unbefugter Offenlegung	Datenschutz	Hoch
O.CRYPTOGRAPHIC_OPERATIONS	Kryptographische Operationen	Stellt korrekte kryptographische Operationen zur Verschlüsselung und Integritätssicherung durch	Datenschutz	Mittel
O.DATA_INTEGRITY	Datenintegrität	Schützt Datenintegrität gegen unbefugte Änderung	Integrität	Hoch
O.SECURITY_MANAGEMENT	Sicherheitsmanagement	Ermöglicht autorisierten Administratoren die Verwaltung von Sicherheitsfunktionen	Management	Mittel
O.SECURE_STATE	Sicherer Zustand	Startet in sicherem Zustand und geht bei Fehlern in sicheren Zustand über	Selbstschutz	Hoch
O.TSF_PROTECTION	TSF-Schutz	Schützt eigene Sicherheitsfunktionen vor Manipulation und Umgehung	Selbstschutz	Hoch

[**TODO**]

Gesamtzahl TOE-Sicherheitsziele: 10 [**TODO: Aktualisiere Anzahl**]

20.2.1 2.1 Kategorisierung der TOE-Sicherheitsziele

Zugriffskontrolle (2 Ziele): - O.ACCESS_CONTROL - O.IDENTIFICATION_AUTHENTICATION

Audit & Nachvollziehbarkeit (2 Ziele): - O.AUDIT_GENERATION - O.AUDIT_PROTECTION

Datenschutz (2 Ziele): - O.DATA_CONFIDENTIALITY - O.CRYPTOGRAPHIC_OPERATIONS

Integrität (1 Ziel): - O.DATA_INTEGRITY

Management (1 Ziel): - O.SECURITY_MANAGEMENT

Selbstschutz (2 Ziele): - O.SECURE_STATE - O.TSF_PROTECTION

[**TODO: Ergänze weitere Kategorien**]

20.3 3. Umgebungsziele (Übersicht)

Die folgenden Sicherheitsziele müssen durch die Betriebsumgebung erfüllt werden:

ID	Ziel	Kurzbeschreibung	Kategorie	Verantwortlich
OE.PHYSICAL_PROTECTION	Physischer Schutz	Stellt sicher, dass das TOE vor physischem Zugriff durch unbefugte Personen geschützt wird	Physische Sicherheit	Betreiber
OE.TRUSTED_ADMIN	Vertrauenswürdige Administratoren	Stellt sicher, dass Administratoren vertrauenswürdig, geschult und kompetent sind	Personal	Organisation
OE.USER_TRAINING	Benutzerschulung	Stellt sicher, dass Benutzer in sicherer Verwendung des TOE geschult sind	Personal	Organisation
OE.NETWORK_PROTECTION	Netzwerkschutz	Schützt das TOE vor Netzwerkangriffen durch Firewalls und andere Mechanismen	Netzwerk	IT-Abteilung
OE.EXTERNAL_SYSTEMS	Sichere externe Systeme	Stellt sicher, dass externe Systeme vertrauenswürdig und sicher sind	Integration	IT-Abteilung
OE.TIME_STAMPS	Zuverlässige Zeitstempel	Stellt zuverlässige Zeitstempel für Audit-Aufzeichnungen bereit	Infrastruktur	IT-Abteilung

[**TODO**]

Gesamtzahl Umgebungsziele: 6 [**TODO: Aktualisiere Anzahl**]

20.3.1 3.1 Kategorisierung der Umgebungsziele

Physische Sicherheit (1 Ziel): - OE.PHYSICAL_PROTECTION

Personal (2 Ziele): - OE.TRUSTED_ADMIN - OE.USER_TRAINING

Netzwerk (1 Ziel): - OE.NETWORK_PROTECTION

Integration (1 Ziel): - OE.EXTERNAL_SYSTEMS

Infrastruktur (1 Ziel): - OE.TIME_STAMPS

[**TODO: Ergänze weitere Kategorien**]

20.4 4. Sicherheitsziele nach Sicherheitsbereichen

20.4.1 4.1 Zugriffskontrolle und Authentifizierung

TOE-Ziele: - O.ACCESS_CONTROL: Zugriffskontrolle auf Ressourcen - O.IDENTIFICATION_AUTHENTICA Benutzeridentifikation und -authentifizierung

Umgebungsziele: - OE.TRUSTED_ADMIN: Vertrauenswürdige Administratoren

Zusammenfassung: Das TOE implementiert technische Zugriffskontroll- und Authentifizierungsmechanismen, während die Umgebung vertrauenswürdige Administratoren bereitstellt.

20.4.2 4.2 Audit und Nachvollziehbarkeit

TOE-Ziele: - O.AUDIT_GENERATION: Aufzeichnung sicherheitsrelevanter Ereignisse - O.AUDIT_PROTECTION: Schutz von Audit-Aufzeichnungen

Umgebungsziele: - OE.TIME_STAMPS: Zuverlässige Zeitstempel

Zusammenfassung: Das TOE zeichnet Ereignisse auf und schützt Audit-Daten, während die Umgebung zuverlässige Zeitstempel bereitstellt.

20.4.3 4.3 Datenschutz und Vertraulichkeit

TOE-Ziele: - O.DATA_CONFIDENTIALITY: Schutz sensibler Daten vor Offenlegung - O.CRYPTOGRAPHIC_OPERATIONS: Kryptografische Operationen

Umgebungsziele: - OE.NETWORK_PROTECTION: Netzwerkschutz

Zusammenfassung: Das TOE schützt Daten durch Zugriffskontrolle und Verschlüsselung, während die Umgebung Netzwerkschutz bereitstellt.

20.4.4 4.4 Datenintegrität

TOE-Ziele: - O.DATA_INTEGRITY: Schutz der Datenintegrität - O.CRYPTOGRAPHIC_OPERATIONS: Kryptografische Integritätssicherung

Umgebungsziele: - Keine direkten Umgebungsziele

Zusammenfassung: Das TOE ist primär verantwortlich für Integritätsschutz.

20.4.5 4.5 Sicherheitsmanagement

TOE-Ziele: - O.SECURITY_MANAGEMENT: Verwaltung von Sicherheitsfunktionen

Umgebungsziele: - OE.TRUSTED_ADMIN: Vertrauenswürdige Administratoren - OE.USER_TRAINING: Benutzerschulung

Zusammenfassung: Das TOE bietet Verwaltungsfunktionen, während die Umgebung geschultes Personal bereitstellt.

20.4.6 4.6 Selbstschutz und Verfügbarkeit

TOE-Ziele: - O.SECURE_STATE: Sicherer Zustand bei Start und Fehlern - O.TSF_PROTECTION: Schutz der Sicherheitsfunktionen

Umgebungsziele: - OE.PHYSICAL_PROTECTION: Physischer Schutz - OE.EXTERNAL_SYSTEMS: Sichere externe Systeme

Zusammenfassung: Das TOE schützt sich selbst, während die Umgebung physischen Schutz und sichere Integration bereitstellt.

[**TODO: Ergänze weitere Sicherheitsbereiche**]

20.5 5. Abdeckungsstatistiken

20.5.1 5.1 Bedrohungsabdeckung

Kategorie	Anzahl	Abgedeckt durch TOE-Ziele	Abgedeckt durch Umgebungsziele
Zugriffskontrolle	3	3	0
Datenoffenlegung	2	2	0
Datenmanipulation	2	2	0
Audit-Kompromittierung	1	1	0
Systemfehler	1	1	0
TSF-Kompromittierung	2	2	0
Physische Angriffe	1	0	1
Gesamt	**12**	**11**	**1**

[**TODO: Aktualisiere Statistiken basierend auf deinen Bedrohungen**]

20.5.2 5.2 OSP-Abdeckung

OSP	Umsetzende TOE-Ziele	Status
P.ACCESS_CONTROL	O.ACCESS_CONTROL	Umgesetzt
P.ACCOUNTABILITY	O.AUDIT_GENERATION, O.AUDIT_PROTECTION	Umgesetzt
P.CONFIDENTIALITY	O.DATA_CONFIDENTIALITY	Umgesetzt
P.INTEGRITY	O.DATA_INTEGRITY	Umgesetzt
P.MANAGEMENT	O.SECURITY_MANAGEMENT	Umgesetzt
[**TODO**]		

Gesamtzahl OSPs: 5 [**TODO: Aktualisiere Anzahl**]
Umgesetzte OSPs: 5 (100%)

20.5.3 5.3 Annahmenabdeckung

Annahme	Erfüllendes Umgebungsziel	Status
A.PHYSICAL_SECURITY	OE.PHYSICAL_PROTECTION	Erfüllt
A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN	Erfüllt

Annahme	Erfüllendes Umgebungsziel	Status
A.USER_TRAINING	OE.USER_TRAINING	Erfüllt
A.NETWORK_SECURITY	OE.NETWORK_PROTECTION	Erfüllt
A.EXTERNAL_SYSTEMS	OE.EXTERNAL_SYSTEMS	Erfüllt
A.TIME_SOURCE [**TODO**]	OE.TIME_STAMPS	Erfüllt

Gesamtzahl Annahmen: 6 [**TODO: Aktualisiere Anzahl**]
Erfüllte Annahmen: 6 (100%)

20.5.4 5.4 Vollständigkeitsbewertung

Kriterium	Status	Prozentsatz
Alle Bedrohungen abgedeckt	Ja	100%
Alle OSPs umgesetzt	Ja	100%
Alle Annahmen erfüllt	Ja	100%
Alle Ziele gerechtfertigt	Ja	100%

Gesamtbewertung: Vollständig und konsistent

20.6 6. Grafische Darstellungen

20.6.1 6.1 Verteilung der TOE-Sicherheitsziele nach Kategorie

```
Zugriffskontrolle:              (20%)
Audit & Nachvollziehbarkeit:       (20%)
Datenschutz:                    (20%)
Integrität:                   (10%)
Management:                   (10%)
Selbstschutz:                   (20%)
```

[**TODO: Erstelle Diagramm mit tatsächlichen Werten**]

20.6.2 6.2 Verteilung der Umgebungsziele nach Verantwortlichkeit

```
Betreiber (Physisch):               (17%)
Organisation (Personal):                      (33%)
IT-Abteilung (Technisch):                                 (50%)
```

[**TODO: Erstelle Diagramm mit tatsächlichen Werten**]

20.6.3 6.3 Beziehungsdiagramm (vereinfacht)

```
Bedrohungen (12)        TOE-Ziele (10)        SFRs
                                                    (nächster Schritt)
OSPs (5)                TOE-Ziele (10)
```

```
Annahmen (6)          Umgebungsziele (6)      Umgebungs-
                                                anforderungen
```

[**TODO: Erstelle detailliertes Diagramm**]

20.7 7. Prioritäten und Abhängigkeiten

20.7.1 7.1 Hochprioritäre Sicherheitsziele

Die folgenden Sicherheitsziele haben höchste Priorität und müssen zuerst implementiert werden:

1. **O.TSF_PROTECTION** - Fundamental für alle anderen Ziele
2. **O.ACCESS_CONTROL** - Basis für Zugriffskontrolle
3. **O.IDENTIFICATION_AUTHENTICATION** - Voraussetzung für Zugriffskontrolle
4. **O.DATA_CONFIDENTIALITY** - Schutz sensibler Daten
5. **O.DATA_INTEGRITY** - Schutz der Datenintegrität
6. **O.AUDIT_GENERATION** - Nachvollziehbarkeit
7. **O.SECURE_STATE** - Sicherer Betrieb

[**TODO: Passe Prioritäten an dein TOE an**]

20.7.2 7.2 Abhängigkeiten zwischen Sicherheitszielen

Ziel	Abhängig von	Begründung
O.ACCESS_CONTROL	O.IDENTIFICATION_AUTHENTICATION	Zugriffskontrolle erfordert Authentifizierung
O.AUDIT_GENERATION	O.TIME_STAMPS	Audit-Aufzeichnungen benötigen Zeitstempel
O.DATA_CONFIDENTIALITY	O.ACCESS_CONTROL	Vertraulichkeit erfordert Zugriffskontrolle
O.DATA_INTEGRITY	O.ACCESS_CONTROL	Integrität erfordert Zugriffskontrolle
O.SECURITY_MANAGEMENT	O.TRUSTED_ADMIN	Verwaltung erfordert vertrauenswürdige Admins

[**TODO**]

20.8 8. Zusammenfassung und Bewertung

20.8.1 8.1 Stärken der Sicherheitsziele

1. **Vollständige Abdeckung:** Alle Bedrohungen, OSPs und Annahmen sind adressiert
2. **Klare Trennung:** TOE- und Umgebungsverantwortlichkeiten sind klar definiert
3. **Defense-in-Depth:** Mehrfache Schutzschichten durch überlappende Ziele
4. **Rückverfolgbarkeit:** Alle Ziele sind durch Sicherheitsprobleme gerechtfertigt
5. **Ausgewogenheit:** Gute Balance zwischen verschiedenen Sicherheitsbereichen

[**TODO: Ergänze spezifische Stärken für dein TOE**]

20.8.2 8.2 Potenzielle Herausforderungen

1. **Komplexität:** Viele Sicherheitsziele erfordern sorgfältige Implementierung
2. **Abhängigkeiten:** Einige Ziele sind voneinander abhängig
3. **Umgebungsanforderungen:** Erfolg hängt von korrekter Umgebungskonfiguration ab

[**TODO: Identifiziere spezifische Herausforderungen für dein TOE**]

20.8.3 8.3 Empfehlungen

1. Priorisiere Implementierung hochprioritärer Ziele
2. Berücksichtige Abhängigkeiten bei der Implementierungsplanung
3. Stelle sicher, dass Umgebungsanforderungen erfüllbar sind
4. Dokumentiere Implementierungsentscheidungen für Evaluatoren

[**TODO: Ergänze spezifische Empfehlungen**]

20.9 9. Nächste Schritte

Nach der Zusammenfassung der Sicherheitsziele:

1. **Sicherheitsanforderungen ableiten** (Template 0400-0450)
   - Leite Security Functional Requirements (SFRs) aus TOE-Zielen ab
   - Definiere Security Assurance Requirements (SARs)
   - Wähle Evaluation Assurance Level (EAL)
2. **Rationale für Anforderungen erstellen**
   - Zeige, wie SFRs die Sicherheitsziele erfüllen
   - Dokumentiere SFR-Abhängigkeiten
3. **TOE Summary Specification entwickeln**
   - Beschreibe, wie das TOE die SFRs implementiert

20.10 10. Referenzen

- ISO/IEC 15408-1: Security Target Evaluation
- ISO/IEC 15408-2: Security Functional Components
- ISO/IEC 15408-3: Security Assurance Components
- Template 0200-0240: Sicherheitsproblem-Definition
- Template 0300: Sicherheitsziele
- Template 0310: Rationale für Sicherheitsziele
- Template 0320: Security Objectives Coverage Matrix
- Template 0400-0450: Sicherheitsanforderungen

Dokumenthistorie:

Version	Datum	Autor	Änderungen
{{ meta.version }}	{{ meta.date }}	{{ meta.owner }}	Initiale Version

ewpage

Chapter 21

Sicherheitsanforderungen (Security Requirements)

Dokument-ID: 0400
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und passe die Inhalte an dein spezifisches Target of Evaluation (TOE) an.

21.1 1. Einleitung

Dieses Kapitel spezifiziert die Sicherheitsanforderungen für das TOE gemäß ISO/IEC 15408 (Common Criteria). Die Sicherheitsanforderungen gliedern sich in:

- **Security Functional Requirements (SFRs)**: Funktionale Sicherheitsanforderungen, die das TOE erfüllen muss
- **Security Assurance Requirements (SARs)**: Vertrauenswürdigkeitsanforderungen für die Evaluierung des TOE

Alle Sicherheitsanforderungen sind aus den in Kapitel 0300 definierten Sicherheitszielen abgeleitet und adressieren die in Kapitel 0200 identifizierten Bedrohungen, organisatorischen Sicherheitsrichtlinien und Annahmen.

21.2 2. Security Functional Requirements (SFRs)

21.2.1 2.1 Übersicht der SFRs

Die folgenden Security Functional Requirements aus ISO/IEC 15408-2 wurden für das TOE ausgewählt:

SFR-ID	Klasse	Familie	Komponente	Beschreibung
[TODO]	[TODO: z.B. FAU]	[TODO: z.B. FAU_GEN]	[TODO: z.B. FAU_GEN.1]	[TODO: Kurzbeschreibung]
[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: Keine
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 Das TSF muss in der Lage sein, einen Audit-Datensatz für die folgenden auditierbaren Ereignisse zu erzeugen: - [assignment: Liste der auditierbaren Ereignisse] - [TODO: Spezifiziere konkrete Ereignisse]

FAU_GEN.1.2 Das TSF muss in jedem Audit-Datensatz mindestens die folgenden Informationen aufzeichnen: - Datum und Uhrzeit des Ereignisses - Art des Ereignisses - Subjekt-Identität - Ergebnis (Erfolg oder Fehler) des Ereignisses - [assignment: Weitere Audit-relevante Informationen]

21.2.3 2.3 Cryptographic Support (FCS)

21.2.3.1 FCS_COP.1 Cryptographic operation

Hierarchical to: Keine
Dependencies: - FDP_ITC.1 Import of user data without security attributes oder FDP_ITC.2 Import of user data with security attributes oder FCS_CKM.1 Cryptographic key generation

FCS_COP.1.1 Das TSF muss [assignment: kryptographische Operation] gemäß einem spezifizierten kryptographischen Algorithmus [assignment: kryptographischer Algorithmus] und kryptographischen Schlüssellängen [assignment: Schlüssellängen] durchführen, die [selection: Standards, Regeln, Richtlinien] entsprechen.

[TODO: Spezifiziere konkrete kryptographische Operationen, Algorithmen und Schlüssellängen]

21.2.4 2.4 User Data Protection (FDP)

21.2.4.1 FDP_ACC.1 Subset access control

Hierarchical to: Keine
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 Das TSF muss [assignment: Zugriffskontrollrichtlinie] auf [assignment: Subjekte, Objekte und Operationen] durchsetzen.

[TODO: Definiere Zugriffskontrollrichtlinie, Subjekte, Objekte und Operationen]

21.2.5 2.5 Identification and Authentication (FIA)

21.2.5.1 FIA_UID.1 Timing of identification

Hierarchical to: Keine
Dependencies: Keine

FIA_UID.1.1 Das TSF muss es jedem Benutzer erlauben, sich zu identifizieren, bevor das TSF dem Benutzer erlaubt, andere TSF-vermittelte Aktionen durchzuführen, die [selection: keine anderen Aktionen, [assignment: Liste der TSF-vermittelten Aktionen]] ausschließen.

[TODO: Spezifiziere Ausnahmen, falls vorhanden]

21.2.6 2.6 Security Management (FMT)

21.2.6.1 FMT_SMF.1 Specification of Management Functions

Hierarchical to: Keine
Dependencies: Keine

FMT_SMF.1.1 Das TSF muss in der Lage sein, die folgenden Sicherheitsmanagement-Funktionen durchzuführen: - [assignment: Liste der Sicherheitsmanagement-Funktionen]

[TODO: Liste alle Sicherheitsmanagement-Funktionen auf]

21.2.7 2.7 Protection of the TSF (FPT)

21.2.7.1 FPT_STM.1 Reliable time stamps

Hierarchical to: Keine
Dependencies: Keine

FPT_STM.1.1 Das TSF muss in der Lage sein, zuverlässige Zeitstempel für den eigenen Gebrauch bereitzustellen.

21.2.8 2.8 TOE Access (FTA)

21.2.9 2.9 Trusted Path/Channels (FTP)

21.2.10 2.10 Weitere SFR-Klassen

21.3 3. Security Assurance Requirements (SARs)

21.3.1 3.1 Übersicht der SARs

Die Security Assurance Requirements definieren die Vertrauenswürdigkeitsanforderungen für die Evaluierung des TOE. Die SARs sind durch die Auswahl des Evaluation Assurance Level (EAL) bestimmt.

Gewähltes EAL: [TODO: z.B. EAL4]

21.3.2 3.2 Assurance Class: Security Target Evaluation (ASE)

Die folgenden ASE-Komponenten sind für alle EALs erforderlich:

- **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: Passe an gewähltes EAL an]

21.3.3 3.3 Assurance Class: Development (ADV)

Für EAL [TODO: X] sind folgende ADV-Komponenten erforderlich:

- **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: Passe an gewähltes EAL an]

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)

Für EAL [TODO: X] sind folgende ALC-Komponenten erforderlich:

- **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: Passe an gewähltes EAL an]

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: Passe an gewähltes EAL an]

21.3.7 3.7 Assurance Class: Vulnerability Assessment (AVA)

- **AVA_VAN.3** Focused vulnerability analysis

[TODO: Passe an gewähltes EAL an]

21.4 4. Security Requirements Rationale

Die Begründung für die Auswahl der Sicherheitsanforderungen wird in Dokument 0420 detailliert dargestellt.

Zusammenfassung: - Alle SFRs sind aus den Sicherheitszielen für das TOE abgeleitet - Alle SFR-Abhängigkeiten sind erfüllt (siehe Dokument 0430) - Die gewählten SARs entsprechen dem Evaluation Assurance Level [TODO: X] - Die Sicherheitsanforderungen sind vollständig, konsistent und intern widerspruchsfrei

21.5 5. Operationen auf SFRs

Gemäß ISO/IEC 15408-2 können folgende Operationen auf SFRs durchgeführt werden:

- **Assignment**: Spezifizierung von Parametern (markiert mit [assignment: …])
- **Selection**: Auswahl aus vorgegebenen Optionen (markiert mit [selection: …])
- **Refinement**: Verfeinerung der Anforderung (kursiv dargestellt)
- **Iteration**: Mehrfache Verwendung einer Komponente (durch Suffix gekennzeichnet, z.B. FDP_ACC.1/1, FDP_ACC.1/2)

Alle durchgeführten Operationen sind in den SFR-Spezifikationen oben dokumentiert.

21.6 6. Referenzen

- ISO/IEC 15408-2:2022 - Security functional requirements
- ISO/IEC 15408-3:2022 - Security assurance requirements
- [TODO: Weitere relevante Standards und Spezifikationen]

21.7 7. Anhänge

21.7.1 7.1 SFR-Übersichtstabelle

Eine vollständige Übersicht aller SFRs mit Abhängigkeiten findet sich in Dokument 0430.

21.7.2 7.2 SAR-Übersichtstabelle

Eine vollständige Übersicht aller SARs entsprechend dem gewählten EAL findet sich in Dokument 0410.

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter 2. Spezifiziere alle Assignments und Selections in den SFRs 3. Verifiziere die Vollständigkeit der SFR-Abhängigkeiten (siehe Dokument 0430) 4. Stelle sicher, dass alle SFRs aus den Sicherheitszielen abgeleitet sind 5. Dokumentiere die Rationale in Dokument 0420

ewpage

Chapter 22

Evaluation Assurance Level (EAL)

Dokument-ID: 0410
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und passe die Inhalte an dein spezifisches Target of Evaluation (TOE) an.

22.1 1. Einleitung

Dieses Dokument beschreibt die Auswahl und Begründung des Evaluation Assurance Level (EAL) für das TOE. Das EAL definiert die Tiefe und Strenge der Sicherheitsevaluierung gemäß ISO/IEC 15408-3.

22.2 2. EAL-Übersicht

Common Criteria definiert sieben vordefinierte Evaluation Assurance Levels:

EAL	Bezeichnung	Beschreibung	Typische Anwendung
EAL1	Functionally tested	Grundlegende Funktionsprüfung	Kommerzielle Standardprodukte
EAL2	Structurally tested	Strukturelle Prüfung mit Entwicklerdokumentation	Kommerzielle Produkte mit Sicherheitsfunktionen
EAL3	Methodically tested and checked	Methodische Prüfung und Überprüfung	Sicherheitsprodukte mit moderaten Anforderungen
EAL4	Methodically designed, tested, and reviewed	Methodisches Design, Test und Review	Sicherheitsprodukte für kommerzielle Umgebungen

EAL	Bezeichnung	Beschreibung	Typische Anwendung
EAL5	Semiformally designed and tested	Semiformales Design und Test	Hochsicherheitsprodukte
EAL6	Semiformally verified design and tested	Semiformale Verifikation und Test	Hochsicherheitsumgebungen mit hohem Risiko
EAL7	Formally verified design and tested	Formale Verifikation und Test	Extrem hohe Sicherheitsanforderungen

22.3 3. Gewähltes EAL

Gewähltes Evaluation Assurance Level: [TODO: z.B. EAL4]

22.3.1 3.1 Begründung der EAL-Auswahl

[TODO: Begründe die Auswahl des EAL basierend auf:] - Bedrohungslandschaft und Risikobewertung - Schutzbedarf der zu schützenden Assets - Einsatzumgebung des TOE - Kosten-Nutzen-Verhältnis - Marktanforderungen und regulatorische Vorgaben - Entwicklungsressourcen und -zeitplan

Beispiel:

```
EAL4 wurde gewählt, da es ein ausgewogenes Verhältnis zwischen Sicherheitsvertrauen und Entwicklungsaufwand bietet. Das TOE wird in kommerziellen Umgebungen mit moderaten bis hohen Sicherheitsanforderungen eingesetzt. EAL4 erfordert methodisches Design, Test und Review, was den Sicherheitsanforderungen der Zielumgebung entspricht, ohne die formalen Verifikationsanforderungen höherer EALs zu benötigen.
```

22.3.2 3.2 Alternativen und Abwägungen

[TODO: Diskutiere alternative EALs und warum sie nicht gewählt wurden]

Niedrigere EALs (z.B. EAL3): - [TODO: Warum nicht ausreichend?]

Höhere EALs (z.B. EAL5+): - [TODO: Warum nicht erforderlich oder nicht praktikabel?]

22.4 4. Security Assurance Requirements (SARs) für gewähltes EAL

22.4.1 4.1 Mandatory SARs für EAL [TODO: X]

Die folgenden Security Assurance Requirements sind für EAL [TODO: X] verpflichtend:

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: Füge ADV-Komponenten für gewähltes EAL hinzu]

Für 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: Füge ALC-Komponenten für gewähltes EAL hinzu]

Für 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: Füge ATE-Komponenten für gewähltes EAL hinzu]

Für 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: Füge AVA-Komponenten für gewähltes EAL hinzu]

Für EAL4: - **AVA_VAN.3** Focused vulnerability analysis

22.4.2 4.2 Augmentation (Zusätzliche SARs)

[TODO: Falls zusätzliche SARs über das gewählte EAL hinaus verwendet werden, liste und begründe sie hier]

Beispiel:

```
Zusätzlich zu den EAL4-Anforderungen werden folgende SARs hinzugefügt:
- ALC_FLR.2 Flaw reporting procedures (aus EAL5)
  Begründung: Verbesserte Schwachstellenverwaltung für produktive Umgebungen
```

22.5 5. Entwicklungs- und Evaluierungsaufwand

22.5.1 5.1 Entwicklungsaufwand

[TODO: Schätze den zusätzlichen Entwicklungsaufwand für das gewählte EAL]

Dokumentationsaufwand: - [TODO: Erforderliche Dokumente und geschätzter Aufwand]

Prozessanforderungen: - [TODO: Erforderliche Entwicklungsprozesse und -werkzeuge]

Testaufwand: - [TODO: Erforderliche Tests und Testabdeckung]

22.5.2 5.2 Evaluierungsaufwand

[TODO: Schätze Dauer und Kosten der Evaluierung]

Geschätzte Evaluierungsdauer: [TODO: z.B. 6-12 Monate]
Geschätzte Evaluierungskosten: [TODO: Kostenrahmen]
Evaluierungslabor: [TODO: Geplantes oder ausgewähltes Labor]

22.6 6. Compliance und Zertifizierung

22.6.1 6.1 Zertifizierungsschema

[TODO: Spezifiziere das Zertifizierungsschema]

Beispiele: - Common Criteria Recognition Arrangement (CCRA) - Nationales Schema (z.B. BSI Deutschland, ANSSI Frankreich) - [TODO: Spezifisches Schema]

22.6.2 6.2 Mutual Recognition

[TODO: Beschreibe Mutual Recognition Agreements, falls relevant]

Das gewählte EAL und Zertifizierungsschema ermöglicht die Anerkennung in folgenden Ländern: - [TODO: Liste der Länder mit Mutual Recognition]

22.7 7. Zeitplan und Meilensteine

[TODO: Erstelle einen groben Zeitplan für die Evaluierung]

Meilenstein	Geplantes Datum	Status
ST-Fertigstellung	[TODO]	[TODO]
Evaluierungsbeginn	[TODO]	[TODO]
ADV-Phase abgeschlossen	[TODO]	[TODO]
ATE-Phase abgeschlossen	[TODO]	[TODO]
AVA-Phase abgeschlossen	[TODO]	[TODO]
Zertifizierung	[TODO]	[TODO]

22.8 8. Risiken und Mitigation

[TODO: Identifiziere Risiken für die Evaluierung]

Risiko	Wahrscheinlichkeit	Auswirkung	Mitigation
[TODO: z.B. Verzögerungen in der Dokumentation]	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]

22.9 9. Referenzen

- ISO/IEC 15408-3:2022 - Security assurance requirements
- Common Criteria for Information Technology Security Evaluation - Evaluation Assurance Levels
- [TODO: Nationale Zertifizierungsrichtlinien]
- [TODO: Weitere relevante Dokumente]

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter 2. Validiere die EAL-Auswahl mit Stakeholdern 3. Bestätige die Verfügbarkeit von Ressourcen für die Evaluierung 4. Kontaktiere potenzielle Evaluierungslabore 5. Erstelle detaillierten Projektplan für die Evaluierung

ewpage

Chapter 23

Begründung der Sicherheitsanforderungen (Requirements Rationale)

Dokument-ID: 0420
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und passe die Inhalte an dein spezifisches Target of Evaluation (TOE) an.

23.1 1. Einleitung

Dieses Dokument begründet die Auswahl der Sicherheitsanforderungen (Security Functional Requirements und Security Assurance Requirements) für das TOE. Die Begründung demonstriert, dass:

1. Alle SFRs notwendig und ausreichend sind, um die Sicherheitsziele für das TOE zu erfüllen
2. Alle SFR-Abhängigkeiten erfüllt sind
3. Die gewählten SARs dem Evaluation Assurance Level entsprechen
4. Die Sicherheitsanforderungen intern konsistent und widerspruchsfrei sind

23.2 2. Ableitung der SFRs aus Sicherheitszielen

23.2.1 2.1 Mapping: Sicherheitsziele → SFRs

Die folgende Tabelle zeigt die Zuordnung zwischen den Sicherheitszielen für das TOE (aus Dokument 0300) und den Security Functional Requirements (aus Dokument 0400):

Sicherheitsziel	Zugeordnete SFRs	Begründung
[TODO: O.AUDIT]	FAU_GEN.1, FAU_SAR.1, FPT_STM.1	[TODO: Begründung der Zuordnung]
[TODO: O.CRYPTO]	FCS_COP.1, FCS_CKM.1	[TODO: Begründung der Zuordnung]
[TODO: O.ACCESS]	FDP_ACC.1, FDP_ACF.1, FIA_UID.1, FIA_UAU.1	[TODO: Begründung der Zuordnung]
[TODO]	[TODO]	[TODO]

23.2.2 2.2 Detaillierte Begründung pro Sicherheitsziel

23.2.2.1 2.2.1 [TODO: Sicherheitsziel 1]

Sicherheitsziel: [TODO: Beschreibung aus Dokument 0300]

Zugeordnete SFRs: - [TODO: SFR-ID]: [TODO: Begründung, wie diese SFR das Ziel erfüllt] - [TODO: SFR-ID]: [TODO: Begründung]

Vollständigkeit: [TODO: Erklärung, warum diese SFRs ausreichend sind]

23.2.2.2 2.2.2 [TODO: Sicherheitsziel 2]

Sicherheitsziel: [TODO: Beschreibung aus Dokument 0300]

Zugeordnete SFRs: - [TODO: SFR-ID]: [TODO: Begründung]

Vollständigkeit: [TODO: Erklärung]

23.2.3 2.3 Vollständigkeitsanalyse

Abdeckung der Sicherheitsziele: - Anzahl der Sicherheitsziele für TOE: [TODO: X] - Anzahl der durch SFRs adressierten Ziele: [TODO: X] - Abdeckungsgrad: [TODO: 100%]

Nicht durch SFRs adressierte Ziele: [TODO: Falls vorhanden, liste und begründe, warum keine SFRs erforderlich sind]

23.3 3. Notwendigkeit der SFRs

23.3.1 3.1 Begründung pro SFR

Jede ausgewählte SFR muss notwendig sein, um mindestens ein Sicherheitsziel zu erfüllen.

23.3.1.1 3.1.1 [TODO: SFR-ID 1]

SFR: [TODO: Name und Beschreibung]

Adressierte Sicherheitsziele: - [TODO: Ziel-ID]: [TODO: Wie die SFR zum Ziel beiträgt]

Notwendigkeit: [TODO: Warum diese SFR unverzichtbar ist]

Alternativen: [TODO: Warum alternative SFRs nicht gewählt wurden]

23.3.1.2 3.1.2 [TODO: SFR-ID 2]

SFR: [TODO: Name und Beschreibung]

Adressierte Sicherheitsziele: - [TODO: Ziel-ID]: [TODO: Begründung]

Notwendigkeit: [TODO: Begründung]

23.3.2 3.2 Überflüssige SFRs

[TODO: Bestätige, dass keine überflüssigen SFRs enthalten sind]

Alle ausgewählten SFRs sind notwendig und tragen zur Erfüllung mindestens eines Sicherheitsziels bei. Es wurden keine überflüssigen SFRs identifiziert.

23.4 4. SFR-Abhängigkeiten

23.4.1 4.1 Übersicht der Abhängigkeiten

Die folgende Tabelle zeigt alle SFR-Abhängigkeiten und deren Erfüllung:

SFR	Abhängigkeit	Erfüllt durch	Status
FAU_GEN.1	FPT_STM.1	FPT_STM.1	Erfüllt
FCS_COP.1	FCS_CKM.1 oder FDP_ITC.1/2	FCS_CKM.1	Erfüllt
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	Erfüllt
[TODO]	[TODO]	[TODO]	[TODO]

23.4.2 4.2 Erfüllung aller Abhängigkeiten

Zusammenfassung: - Anzahl der SFRs mit Abhängigkeiten: [TODO: X] - Anzahl der erfüllten Abhängigkeiten: [TODO: X] - Anzahl der unerfüllten Abhängigkeiten: [TODO: 0]

[TODO: Falls Abhängigkeiten nicht erfüllt sind, begründe dies ausführlich]

23.4.3 4.3 Detaillierte Begründung für kritische Abhängigkeiten

[TODO: Für komplexe oder kritische Abhängigkeiten, gebe detaillierte Erklärungen]

Beispiel:

```
FCS_COP.1 erfordert FCS_CKM.1 (Cryptographic key generation), da kryptographische
Operationen nur mit korrekt generierten Schlüsseln sicher durchgeführt werden können.
Diese Abhängigkeit wird durch die Implementierung von FCS_CKM.1 erfüllt, welche die
Generierung von Schlüsseln gemäß [Standard] spezifiziert.
```

23.5 5. Interne Konsistenz der SFRs

23.5.1 5.1 Konsistenzprüfung

[TODO: Demonstriere, dass die SFRs intern konsistent sind]

Geprüfte Aspekte: - Keine widersprüchlichen Anforderungen - Kompatible Operationen (Assignments, Selections) - Konsistente Terminologie - Keine Überlappungen oder Redundanzen

Ergebnis: [TODO: Bestätigung der Konsistenz]

23.5.2 5.2 Identifizierte Konflikte und Auflösung

[TODO: Falls Konflikte identifiziert wurden, beschreibe deren Auflösung]

Beispiel:

```
Konflikt: FDP_ACC.1 und FMT_MSA.1 könnten unterschiedliche Interpretationen von
"Sicherheitsattributen" haben.

Auflösung: Die Sicherheitsattribute wurden in Abschnitt X.Y eindeutig definiert und
beide SFRs verwenden diese konsistente Definition.
```

23.6 6. Begründung der SARs

23.6.1 6.1 EAL-Auswahl

Gewähltes EAL: [TODO: z.B. EAL4]

Begründung: [TODO: Verweis auf Dokument 0410 und Zusammenfassung]

Die Auswahl von EAL [TODO: X] ist angemessen, da: - [TODO: Begründung 1] - [TODO: Begründung 2] - [TODO: Begründung 3]

23.6.2 6.2 Augmentation

[TODO: Falls zusätzliche SARs über das EAL-Paket hinaus verwendet werden]

Zusätzliche SARs: - [TODO: SAR-ID]: [TODO: Begründung für Hinzufügung]

Keine Augmentation: [TODO: Falls keine Augmentation, bestätige dies]

Die Standard-SARs für EAL [TODO: X] sind ausreichend für die Evaluierung des TOE. Keine zusätzlichen SARs sind erforderlich.

23.7 7. Adressierung der Sicherheitsziele für die Umgebung

23.7.1 7.1 Nicht-TOE-Sicherheitsanforderungen

[TODO: Erkläre, wie Sicherheitsziele für die Umgebung adressiert werden]

Die Sicherheitsziele für die Umgebung (aus Dokument 0300) werden nicht durch SFRs adressiert, sondern durch: - Organisatorische Maßnahmen - Physische Sicherheitsmaßnahmen - Umgebungsannahmen

Beispiel:

```
O.ENV_PHYSICAL (Physischer Schutz) wird durch organisatorische Maßnahmen wie
Zugangskontrollen und Überwachung adressiert, nicht durch TOE-Funktionalität.
```

23.8 8. Rückverfolgbarkeit

23.8.1 8.1 Traceability Matrix

Die vollständige Rückverfolgbarkeit zwischen Bedrohungen, Sicherheitszielen und SFRs ist in der folgenden Matrix dargestellt:

Bedrohung	Sicherheitsziel	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

Eine detaillierte Coverage Matrix findet sich in Dokument 0440.

23.9 9. Zusammenfassung

23.9.1 9.1 Vollständigkeit

Die ausgewählten Sicherheitsanforderungen sind vollständig: - Alle Sicherheitsziele für das TOE werden durch SFRs adressiert - Alle SFR-Abhängigkeiten sind erfüllt - Die SARs entsprechen dem gewählten EAL

23.9.2 9.2 Konsistenz

Die Sicherheitsanforderungen sind konsistent: - Keine widersprüchlichen Anforderungen - Interne Konsistenz der SFRs - Konsistente Terminologie

23.9.3 9.3 Angemessenheit

Die Sicherheitsanforderungen sind angemessen: - Notwendig zur Erfüllung der Sicherheitsziele - Ausreichend zur Adressierung der Bedrohungen - Praktisch umsetzbar im TOE

23.10 10. Referenzen

- Dokument 0200: Security Problem Definition
- Dokument 0300: Security Objectives
- Dokument 0400: Security Requirements
- Dokument 0410: Evaluation Assurance Level
- Dokument 0430: SFR Dependencies
- Dokument 0440: Coverage Matrix
- ISO/IEC 15408-2:2022 - Security functional requirements
- ISO/IEC 15408-3:2022 - Security assurance requirements

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter 2. Erstelle vollständige Mapping-Tabellen 3. Verifiziere alle Abhängigkeiten 4. Führe Peer-Review der Rationale durch 5. Aktualisiere bei Änderungen an Zielen oder Anforderungen

ewpage

Chapter 24

SFR-Abhängigkeiten (SFR Dependencies)

Dokument-ID: 0430
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und passe die Inhalte an dein spezifisches Target of Evaluation (TOE) an.

24.1 1. Einleitung

Dieses Dokument dokumentiert alle Abhängigkeiten zwischen den Security Functional Requirements (SFRs) des TOE und demonstriert deren Erfüllung. Gemäß ISO/IEC 15408-2 können SFRs Abhängigkeiten zu anderen SFRs haben, die erfüllt sein müssen, damit die Anforderung korrekt funktioniert.

24.2 2. Übersicht der SFR-Abhängigkeiten

24.2.1 2.1 Zusammenfassung

Statistik: - Anzahl der ausgewählten SFRs: [TODO: X] - Anzahl der SFRs mit Abhängigkeiten: [TODO: X] - Gesamtzahl der Abhängigkeiten: [TODO: X] - Anzahl der erfüllten Abhängigkeiten: [TODO: X] - Anzahl der nicht erfüllten Abhängigkeiten: [TODO: 0]

Status: [TODO: Alle Abhängigkeiten erfüllt / Abhängigkeiten nicht erfüllt]

24.2.2 2.2 Vollständige Abhängigkeitstabelle

SFR-ID	SFR-Name	Abhängigkeit	Erfüllt durch	Status	Anmerkungen
FAU_GEN.1	Audit data generation	FPT_STM.1	FPT_STM.1		Zeitstempel für Audit-Einträge
FAU_SAR.1	Audit review	FAU_GEN.1	FAU_GEN.1		Audit-Daten müssen generiert werden
FCS_CKM.1	Cryptographic key generation	[FCS_CKM.2 oder FCS_COP.1]	FCS_COP.1		Schlüssel für kryptographische Operationen
FCS_COP.1	Cryptographic operation	[FDP_ITC.1 oder FDP_ITC.2 oder FCS_CKM.1]	FCS_CKM.1		Schlüsselgenerierung
FDP_ACC.1	Subset access control	FDP_ACF.1	FDP_ACF.1		Zugriffskontrollfunktionen
FDP_ACF.1	Security attribute based access control	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3		Zugriffskontrollrichtlinie und Attributverwaltung
FIA_UAU.1	Timing of authentication	FIA_UID.1	FIA_UID.1		Identifikation vor Authentisierung
FIA_UID.1	Timing of identification	Keine	N/A		Keine Abhängigkeiten
FMT_MSA.1	Management of security attributes	[FDP_ACC.1 oder FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1		Zugriffskontrolle und Rollenverwaltung
FMT_MSA.3	Static attribute initialisation	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1		Attributverwaltung und Rollen
FMT_SMF.1	Specification of Management Functions	Keine	N/A		Keine Abhängigkeiten
FMT_SMR.1	Security roles	FIA_UID.1	FIA_UID.1		Identifikation für Rollenzuweisung
FPT_STM.1	Reliable time stamps	Keine	N/A		Keine Abhängigkeiten
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

24.3 3. Detaillierte Abhängigkeitsanalyse

24.3.1 3.1 Security Audit (FAU)

24.3.1.1 FAU_GEN.1 Audit data generation

Abhängigkeiten: - FPT_STM.1 Reliable time stamps

Erfüllung: FPT_STM.1 ist im Security Target enthalten und stellt zuverlässige Zeitstempel für Audit-Einträge bereit.

Begründung: Audit-Einträge müssen mit präzisen Zeitstempeln versehen werden, um eine chronologische Nachvollziehbarkeit von Sicherheitsereignissen zu gewährleisten.

24.3.1.2 FAU_SAR.1 Audit review

Abhängigkeiten: - FAU_GEN.1 Audit data generation

Erfüllung: FAU_GEN.1 ist im Security Target enthalten und generiert die Audit-Daten, die durch FAU_SAR.1 überprüft werden.

Begründung: Audit-Daten müssen existieren, bevor sie überprüft werden können.

24.3.2 3.2 Cryptographic Support (FCS)

24.3.2.1 FCS_CKM.1 Cryptographic key generation

Abhängigkeiten: - [FCS_CKM.2 Cryptographic key distribution] oder FCS_COP.1 Cryptographic operation

Erfüllung: FCS_COP.1 ist im Security Target enthalten. Generierte Schlüssel werden für kryptographische Operationen verwendet.

Begründung: Schlüssel müssen für einen Zweck generiert werden. In diesem Fall werden sie für kryptographische Operationen (FCS_COP.1) verwendet.

24.3.2.2 FCS_COP.1 Cryptographic operation

Abhängigkeiten: - [FDP_ITC.1 Import of user data without security attributes] oder [FDP_ITC.2 Import of user data with security attributes] oder FCS_CKM.1 Cryptographic key generation

Erfüllung: FCS_CKM.1 ist im Security Target enthalten und generiert die für kryptographische Operationen benötigten Schlüssel.

Begründung: Kryptographische Operationen benötigen Schlüssel, die entweder importiert oder generiert werden müssen.

24.3.3 3.3 User Data Protection (FDP)

24.3.3.1 FDP_ACC.1 Subset access control

Abhängigkeiten: - FDP_ACF.1 Security attribute based access control

Erfüllung: FDP_ACF.1 ist im Security Target enthalten und definiert die Zugriffskontrollfunktionen.

Begründung: Eine Zugriffskontrollrichtlinie (FDP_ACC.1) benötigt Zugriffskontrollfunktionen (FDP_ACF.1) für die Durchsetzung.

24.3.3.2 FDP_ACF.1 Security attribute based access control

Abhängigkeiten: - FDP_ACC.1 Subset access control - FMT_MSA.3 Static attribute initialisation

Erfüllung: Beide Abhängigkeiten sind im Security Target enthalten.

Begründung: - FDP_ACC.1: Zugriffskontrollfunktionen benötigen eine Zugriffskontrollrichtlinie - FMT_MSA.3: Sicherheitsattribute müssen initialisiert werden, bevor sie für Zugriffsentscheidungen verwendet werden können

24.3.4 3.4 Identification and Authentication (FIA)

24.3.4.1 FIA_UID.1 Timing of identification

Abhängigkeiten: Keine

Erfüllung: N/A

24.3.4.2 FIA_UAU.1 Timing of authentication

Abhängigkeiten: - FIA_UID.1 Timing of identification

Erfüllung: FIA_UID.1 ist im Security Target enthalten.

Begründung: Benutzer müssen identifiziert werden, bevor sie authentisiert werden können.

24.3.5 3.5 Security Management (FMT)

24.3.5.1 FMT_MSA.1 Management of security attributes

Abhängigkeiten: - FDP_ACC.1 Subset access control oder [FDP_IFC.1 Subset information flow control] - FMT_SMR.1 Security roles - FMT_SMF.1 Specification of Management Functions

Erfüllung: Alle Abhängigkeiten sind im Security Target enthalten.

Begründung: - FDP_ACC.1: Sicherheitsattribute werden für Zugriffskontrolle verwendet - FMT_SMR.1: Verwaltung von Attributen erfordert Rollendefinitionen - FMT_SMF.1: Verwaltungsfunktionen müssen spezifiziert sein

24.3.5.2 FMT_MSA.3 Static attribute initialisation

Abhängigkeiten: - FMT_MSA.1 Management of security attributes - FMT_SMR.1 Security roles

Erfüllung: Beide Abhängigkeiten sind im Security Target enthalten.

Begründung: Attributinitialisierung benötigt Attributverwaltung und Rollendefinitionen.

24.3.5.3 FMT_SMF.1 Specification of Management Functions

Abhängigkeiten: Keine

Erfüllung: N/A

24.3.5.4 FMT_SMR.1 Security roles

Abhängigkeiten: - FIA_UID.1 Timing of identification

Erfüllung: FIA_UID.1 ist im Security Target enthalten.

Begründung: Rollen können nur identifizierten Benutzern zugewiesen werden.

24.3.6 3.6 Protection of the TSF (FPT)

24.3.6.1 FPT_STM.1 Reliable time stamps

Abhängigkeiten: Keine

Erfüllung: N/A

24.3.7 3.7 [TODO: Weitere SFR-Klassen]

[TODO: Füge Abhängigkeitsanalysen für alle weiteren verwendeten SFRs hinzu]

24.4 4. Abhängigkeitsgraph

24.4.1 4.1 Visualisierung

[TODO: Erstelle einen Abhängigkeitsgraphen, der die Beziehungen zwischen SFRs visualisiert]

```
Beispiel-Graph (als 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 Kritische Pfade

[TODO: Identifiziere kritische Abhängigkeitspfade]

Kritischer Pfad 1: Zugriffskontrolle

```
FIA_UID.1 → FMT_SMR.1 → FMT_MSA.1 → FDP_ACF.1   FDP_ACC.1
```

Kritischer Pfad 2: Audit

```
FPT_STM.1 → FAU_GEN.1 → FAU_SAR.1
```

24.5 5. Nicht erfüllte Abhängigkeiten

24.5.1 5.1 Übersicht

[TODO: Falls Abhängigkeiten nicht erfüllt sind, dokumentiere sie hier]

Status: [TODO: Keine nicht erfüllten Abhängigkeiten / X nicht erfüllte Abhängigkeiten]

24.5.2 5.2 Begründung für nicht erfüllte Abhängigkeiten

[TODO: Für jede nicht erfüllte Abhängigkeit, gebe eine detaillierte Begründung]

Beispiel (falls zutreffend):

```
SFR: FCS_CKM.1
Abhängigkeit: FCS_CKM.2 oder FCS_COP.1
Status: Teilweise erfüllt (nur FCS_COP.1)

Begründung: FCS_CKM.2 (Key distribution) ist nicht erforderlich, da das TOE keine
Schlüsselverteilung an externe Entitäten durchführt. Alle Schlüssel werden intern
generiert und verwendet (FCS_COP.1).
```

24.6 6. Hierarchische Beziehungen

24.6.1 6.1 Verwendung hierarchischer Komponenten

[TODO: Dokumentiere, falls hierarchisch höhere SFR-Komponenten verwendet werden]

Gemäß ISO/IEC 15408-2 erfüllt eine hierarchisch höhere Komponente automatisch die Abhängigkeiten niedrigerer Komponenten.

Beispiel:

```
Falls FDP_ACC.2 (Complete access control) verwendet wird, erfüllt dies automatisch
die Abhängigkeit zu FDP_ACC.1 (Subset access control).
```

24.7 7. Iterationen

24.7.1 7.1 Iterierte SFRs

[TODO: Falls SFRs mehrfach verwendet werden (Iteration), dokumentiere die Abhängigkeiten für jede Iteration]

Iterierte SFR	Iteration	Abhängigkeiten	Erfüllung
[TODO: z.B. FDP_ACC.1/1]	1	FDP_ACF.1/1	
[TODO: z.B. FDP_ACC.1/2]	2	FDP_ACF.1/2	

24.8 8. Validierung

24.8.1 8.1 Validierungscheckliste

- ☐ Alle SFRs sind in der Abhängigkeitstabelle aufgeführt
- ☐ Alle Abhängigkeiten sind gemäß ISO/IEC 15408-2 korrekt identifiziert
- ☐ Alle Abhängigkeiten sind erfüllt oder begründet
- ☐ Hierarchische Beziehungen sind korrekt berücksichtigt
- ☐ Iterationen sind vollständig dokumentiert
- ☐ Abhängigkeitsgraph ist konsistent mit der Tabelle

24.8.2 8.2 Peer-Review

Reviewer: [TODO: Name]
Datum: [TODO: Datum]
Status: [TODO: Approved / Changes requested]
Kommentare: [TODO: Kommentare]

24.9 9. Referenzen

- Dokument 0400: Security Requirements
- Dokument 0420: Requirements Rationale
- ISO/IEC 15408-2:2022 - Security functional requirements (Anhang B: Dependencies)
- [TODO: Weitere relevante Dokumente]

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter 2. Erstelle vollständige Abhängigkeitstabelle 3. Verifiziere alle Abhängigkeiten gegen ISO/IEC 15408-2 4. Erstelle Abhängigkeitsgraph 5. Führe Peer-Review durch 6. Aktualisiere bei Änderungen an SFRs

ewpage

Chapter 25

Coverage Matrix

Dokument-ID: 0440
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und passe die Inhalte an dein spezifisches Target of Evaluation (TOE) an.

25.1 1. Einleitung

Dieses Dokument stellt umfassende Coverage Matrices bereit, die die Rückverfolgbarkeit zwischen allen Elementen des Security Target demonstrieren:

- Bedrohungen (Threats)
- Organisatorische Sicherheitsrichtlinien (OSPs)
- Annahmen (Assumptions)
- Sicherheitsziele (Security Objectives)
- Sicherheitsanforderungen (Security Requirements)

Die Matrices gewährleisten vollständige Abdeckung und Konsistenz des Security Target.

25.2 2. Bedrohungen → Sicherheitsziele

25.2.1 2.1 Threat Coverage Matrix

Diese Matrix zeigt, wie jede identifizierte Bedrohung durch Sicherheitsziele adressiert wird.

Bedrohung	Beschreibung	Adressierende Sicherheitsziele	Abdeckung
T.UNAUTH_ACCESS	Unautorisierter Zugriff auf TOE-Funktionen	O.ACCESS, O.IDENTIFY, O.AUTHENTICATE	Vollständig
T.DATA_DISCLOSURE	Unbefugte Offenlegung von Daten	O.CRYPTO, O.ACCESS	Vollständig
T.DATA_MANIPULATION	Unbefugte Manipulation von Daten	O.INTEGRITY, O.ACCESS, O.AUDIT	Vollständig
T.MASQUERADE	Identitätsvortäuschung	O.AUTHENTICATE, O.IDENTIFY	Vollständig
T.AUDIT_COMPROMISE	Kompromittierung von Audit-Daten	O.AUDIT, O.PROTECT_TSF	Vollständig
[TODO]	[TODO]	[TODO]	[TODO]

25.2.2 2.2 Vollständigkeitsanalyse

Statistik: - Anzahl identifizierter Bedrohungen: [TODO: X] - Anzahl vollständig adressierter Bedrohungen: [TODO: X] - Anzahl teilweise adressierter Bedrohungen: [TODO: 0] - Anzahl nicht adressierter Bedrohungen: [TODO: 0]

Status: [TODO: Alle Bedrohungen adressiert / Lücken vorhanden]

25.2.3 2.3 Nicht adressierte Bedrohungen

[TODO: Falls Bedrohungen nicht vollständig adressiert sind, begründe dies]

Beispiel (falls zutreffend):

```
Bedrohung: T.PHYSICAL_ATTACK
Status: Nicht durch TOE adressiert
Begründung: Physische Angriffe werden durch Umgebungsannahmen (A.PHYSICAL_PROTECTION)
und organisatorische Maßnahmen adressiert, nicht durch TOE-Funktionalität.
```

25.3 3. OSPs → Sicherheitsziele

25.3.1 3.1 OSP Coverage Matrix

Diese Matrix zeigt, wie organisatorische Sicherheitsrichtlinien durch Sicherheitsziele umgesetzt werden.

OSP	Beschreibung	Adressierende Sicherheitsziele	Abdeckung
P.ACCOUNTABILITY	Benutzeraktionen müssen nachvollziehbar sein	O.AUDIT, O.IDENTIFY	Vollständig
P.AUTHORIZED_USERS	Nur autorisierte Benutzer dürfen auf TOE zugreifen	O.ACCESS, O.AUTHENTICATE	Vollständig

OSP	Beschreibung	Adressierende Sicherheitsziele	Abdeckung
P.CRYPTOGRAPHY	Sensible Daten müssen verschlüsselt werden	O.CRYPTO	Vollständig
[TODO]	[TODO]	[TODO]	[TODO]

25.3.2 3.2 Vollständigkeitsanalyse

Statistik: - Anzahl definierter OSPs: [TODO: X] - Anzahl vollständig umgesetzter OSPs: [TODO: X] - Anzahl teilweise umgesetzter OSPs: [TODO: 0] - Anzahl nicht umgesetzter OSPs: [TODO: 0]

Status: [TODO: Alle OSPs umgesetzt / Lücken vorhanden]

25.4 4. Annahmen → Sicherheitsziele für die Umgebung

25.4.1 4.1 Assumption Coverage Matrix

Diese Matrix zeigt, wie Annahmen durch Sicherheitsziele für die Umgebung adressiert werden.

Annahme	Beschreibung	Adressierende Umgebungsziele	Abdeckung
A.PHYSICAL_PROTECTION	Die TOE ist physisch geschützt	OE.PHYSICAL	Vollständig
A.TRUSTED_ADMIN	Administratoren sind vertrauenswürdig	OE.ADMIN_TRAINING, OE.ADMIN_VETTING	Vollständig
A.NETWORK_PROTECTION	Netzwerk ist gegen externe Angriffe geschützt	OE.NETWORK_SECURITY	Vollständig
[TODO]	[TODO]	[TODO]	[TODO]

25.4.2 4.2 Vollständigkeitsanalyse

Statistik: - Anzahl definierter Annahmen: [TODO: X] - Anzahl vollständig adressierter Annahmen: [TODO: X] - Anzahl teilweise adressierter Annahmen: [TODO: 0] - Anzahl nicht adressierter Annahmen: [TODO: 0]

Status: [TODO: Alle Annahmen adressiert / Lücken vorhanden]

25.5 5. Sicherheitsziele für TOE → SFRs

25.5.1 5.1 Security Objectives to SFRs Matrix

Diese Matrix zeigt, wie Sicherheitsziele für das TOE durch Security Functional Requirements erfüllt werden.

Sicherheitsziel	Beschreibung	Erfüllende SFRs	Abdeckung
O.ACCESS	Zugriffskontrolle auf TOE-Ressourcen	FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3	Vollständig
O.IDENTIFY	Identifikation von Benutzern	FIA_UID.1	Vollständig
O.AUTHENTICATE	Authentisierung von Benutzern	FIA_UAU.1, FIA_AFL.1	Vollständig
O.AUDIT	Audit-Aufzeichnung sicherheitsrelevanter Ereignisse	FAU_GEN.1, FAU_SAR.1, FPT_STM.1	Vollständig
O.CRYPTO	Kryptographischer Schutz sensibler Daten	FCS_CKM.1, FCS_COP.1	Vollständig
O.INTEGRITY	Schutz der Datenintegrität	FDP_SDI.1, FPT_TST.1	Vollständig
O.PROTECT_TSF	Schutz der TSF-Funktionalität	FPT_STM.1, FPT_TST.1	Vollständig
O.MANAGE	Sichere Verwaltung des TOE	FMT_SMF.1, FMT_SMR.1, FMT_MOF.1	Vollständig
[TODO]	[TODO]	[TODO]	[TODO]

25.5.2 5.2 Vollständigkeitsanalyse

Statistik: - Anzahl Sicherheitsziele für TOE: [TODO: X] - Anzahl vollständig erfüllter Ziele: [TODO: X] - Anzahl teilweise erfüllter Ziele: [TODO: 0] - Anzahl nicht erfüllter Ziele: [TODO: 0]

Status: [TODO: Alle Ziele erfüllt / Lücken vorhanden]

25.5.3 5.3 Nicht erfüllte Sicherheitsziele

[TODO: Falls Sicherheitsziele nicht vollständig durch SFRs erfüllt sind, begründe dies]

25.6 6. Umgekehrte Rückverfolgbarkeit: SFRs → Sicherheitsziele

25.6.1 6.1 SFRs to Security Objectives Matrix

Diese Matrix zeigt die umgekehrte Rückverfolgbarkeit: Jede SFR muss mindestens ein Sicherheitsziel erfüllen.

SFR	Erfüllte Sicherheitsziele	Notwendigkeit
FAU_GEN.1	O.AUDIT	Notwendig
FAU_SAR.1	O.AUDIT	Notwendig
FCS_CKM.1	O.CRYPTO	Notwendig

SFR	Erfüllte Sicherheitsziele	Notwendigkeit
FCS_COP.1	O.CRYPTO	Notwendig
FDP_ACC.1	O.ACCESS	Notwendig
FDP_ACF.1	O.ACCESS	Notwendig
FDP_SDI.1	O.INTEGRITY	Notwendig
FIA_AFL.1	O.AUTHENTICATE	Notwendig
FIA_UAU.1	O.AUTHENTICATE	Notwendig
FIA_UID.1	O.IDENTIFY	Notwendig
FMT_MOF.1	O.MANAGE	Notwendig
FMT_MSA.1	O.ACCESS, O.MANAGE	Notwendig
FMT_MSA.3	O.ACCESS	Notwendig
FMT_SMF.1	O.MANAGE	Notwendig
FMT_SMR.1	O.MANAGE	Notwendig
FPT_STM.1	O.AUDIT, O.PROTECT_TSF	Notwendig
FPT_TST.1	O.INTEGRITY, O.PROTECT_TSF	Notwendig
[TODO]	[TODO]	[TODO]

25.6.2 6.2 Überflüssige SFRs

[TODO: Identifiziere SFRs, die kein Sicherheitsziel erfüllen (sollte keine geben)]

Status: [TODO: Keine überflüssigen SFRs / Überflüssige SFRs identifiziert]

25.7 7. Vollständige Traceability Matrix

25.7.1 7.1 End-to-End Traceability

Diese Matrix zeigt die vollständige Rückverfolgbarkeit von Bedrohungen bis zu SFRs.

Bedrohung/OSP/Annahme	Sicherheitsziel	SFR	Rationale
T.UNAUTH_ACCESS	O.ACCESS	FDP_ACC.1, FDP_ACF.1	Zugriffskontrolle verhindert unautorisierten Zugriff
T.UNAUTH_ACCESS	O.IDENTIFY	FIA_UID.1	Identifikation erforderlich vor Zugriff
T.UNAUTH_ACCESS	O.AUTHENTICATE	FIA_UAU.1	Authentisierung verifiziert Identität
T.DATA_DISCLOSURE	O.CRYPTO	FCS_COP.1	Verschlüsselung schützt vor Offenlegung
T.DATA_DISCLOSURE	O.ACCESS	FDP_ACC.1	Zugriffskontrolle begrenzt Datenzugriff

Bedrohung/OSP/Annahme	Sicherheitsziel	SFR	Rationale
T.DATA_MANIPULATION	O.INTEGRITY	FDP_SDI.1	Integritätsprüfung erkennt Manipulation
T.DATA_MANIPULATION	O.ACCESS	FDP_ACC.1	Zugriffskontrolle verhindert unbefugte Änderungen
T.DATA_MANIPULATION	O.AUDIT	FAU_GEN.1	Audit-Aufzeichnung dokumentiert Änderungen
[TODO]	[TODO]	[TODO]	[TODO]

25.8 8. Coverage Gaps Analysis

25.8.1 8.1 Identifizierte Lücken

[TODO: Identifiziere und dokumentiere Lücken in der Abdeckung]

Lückentypen: - Bedrohungen ohne Sicherheitsziele - Sicherheitsziele ohne SFRs - SFRs ohne Sicherheitsziele - OSPs ohne Umsetzung

Status: [TODO: Keine Lücken / X Lücken identifiziert]

25.8.2 8.2 Begründung für Lücken

[TODO: Für jede identifizierte Lücke, gebe eine Begründung]

Beispiel (falls zutreffend):

```
Lücke: Bedrohung T.PHYSICAL_ATTACK hat kein TOE-Sicherheitsziel
Begründung: Physische Bedrohungen werden durch Umgebungsannahmen und -ziele adressiert,
nicht durch TOE-Funktionalität. Siehe A.PHYSICAL_PROTECTION und OE.PHYSICAL.
```

25.9 9. Visualisierung

25.9.1 9.1 Traceability Diagram

[TODO: Erstelle ein Diagramm, das die Rückverfolgbarkeit visualisiert]

```
Beispiel (als Text):

Bedrohungen          Sicherheitsziele         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. Validierung und Wartung

25.10.1 10.1 Validierungscheckliste

- ☐ Alle Bedrohungen sind durch Sicherheitsziele adressiert
- ☐ Alle OSPs sind durch Sicherheitsziele umgesetzt
- ☐ Alle Annahmen sind durch Umgebungsziele adressiert
- ☐ Alle Sicherheitsziele für TOE sind durch SFRs erfüllt
- ☐ Alle SFRs erfüllen mindestens ein Sicherheitsziel
- ☐ Keine Lücken in der Abdeckung (oder begründet)
- ☐ Traceability ist bidirektional vollständig

25.10.2 10.2 Wartungshinweise

Bei Änderungen: - Neue Bedrohung → Sicherheitsziel hinzufügen → SFR hinzufügen - Neue SFR → Sicherheitsziel zuordnen → Bedrohung/OSP zuordnen - Entfernte Bedrohung → Prüfe, ob Sicherheitsziel noch benötigt wird - Entfernte SFR → Prüfe, ob Sicherheitsziel noch erfüllt ist

Aktualisierungsfrequenz: - Bei jeder Änderung an Bedrohungen, Zielen oder Anforderungen - Vor jedem Review-Meilenstein - Vor Einreichung zur Evaluierung

25.11 11. Zusammenfassung

25.11.1 11.1 Coverage Summary

Vollständigkeit: - Alle Bedrohungen adressiert: [TODO: X/X] - Alle OSPs umgesetzt: [TODO: X/X] - Alle Annahmen adressiert: [TODO: X/X] - Alle Sicherheitsziele erfüllt: [TODO: X/X] - Alle SFRs notwendig: [TODO: X/X]

Gesamtstatus: [TODO: Vollständig / Lücken vorhanden]

25.11.2 11.2 Audit-Bereitschaft

[TODO: Bestätige Bereitschaft für Audit]

Die Coverage Matrices demonstrieren vollständige und konsistente Rückverfolgbarkeit zwischen allen Elementen des Security Target. Das TOE ist bereit für die Evaluierung.

25.12 12. Referenzen

- Dokument 0200: Security Problem Definition

- Dokument 0300: Security Objectives
- Dokument 0400: Security Requirements
- Dokument 0420: Requirements Rationale
- Dokument 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

Nächste Schritte: 1. Vervollständige alle [TODO]-Platzhalter 2. Erstelle vollständige Coverage Matrices 3. Identifiziere und begründe Lücken 4. Erstelle Traceability Diagram 5. Führe Peer-Review durch 6. Halte Matrices bei Änderungen aktuell

ewpage

Chapter 26

TOE Summary Specification

Dokument-ID: 0500
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und passe die Inhalte an dein spezifisches TOE (Target of Evaluation) an.

26.1 1. Einleitung

26.1.1 1.1 Zweck

Dieses Dokument beschreibt die TOE Summary Specification (TSS) für [**TODO: TOE-Name**]. Die TSS zeigt, wie das TOE die in Kapitel 4 (Security Requirements) definierten Sicherheitsfunktionsanforderungen (SFRs) und Sicherungsanforderungen (SARs) erfüllt.

26.1.2 1.2 Struktur der TSS

Die TOE Summary Specification ist wie folgt strukturiert:

- **Kapitel 2**: Übersicht der TOE-Sicherheitsfunktionen (TSFs)
- **Kapitel 3**: Detaillierte Beschreibung der Sicherheitsfunktionen
- **Kapitel 4**: Zuordnung von Sicherheitsfunktionen zu SFRs (Coverage Matrix)
- **Kapitel 5**: Sicherungsmaßnahmen (Assurance Measures)
- **Kapitel 6**: Stärke der Sicherheitsfunktionen (Strength of Function)

26.2 2. Übersicht der TOE-Sicherheitsfunktionen

26.2.1 2.1 Sicherheitsfunktionen - Übersicht

Das TOE implementiert folgende Sicherheitsfunktionen (TSFs):

TSF-ID	Sicherheitsfunktion	Beschreibung	Zugeordnete SFRs
TSF-1	[TODO: Name]	[TODO: Kurzbeschreibung]	[TODO: SFR-IDs]
TSF-2	[TODO: Name]	[TODO: Kurzbeschreibung]	[TODO: SFR-IDs]
TSF-3	[TODO: Name]	[TODO: Kurzbeschreibung]	[TODO: SFR-IDs]

26.2.2 2.2 Architektur der Sicherheitsfunktionen

```
[TODO: Diagramm einfügen - Architektur der TSFs]

Beispiel:

            TOE Security Functions


    TSF-1: I&A        TSF-2: Access
                      Control


    TSF-3: Audit      TSF-4: Crypto
```

Beschreibung:

[TODO: Beschreibe die Architektur der Sicherheitsfunktionen. Erkläre, wie die verschiedenen TSFs zusammenarbeiten und welche Abhängigkeiten bestehen.]

26.3 3. Detaillierte Beschreibung der Sicherheitsfunktionen

26.3.1 3.1 TSF-1: [TODO: Name der Sicherheitsfunktion]

TSF-ID: TSF-1
Zugeordnete SFRs: [TODO: z.B. FIA_UID.1, FIA_UAU.1]

26.3.1.1 3.1.1 Funktionsbeschreibung

[TODO: Beschreibe die Sicherheitsfunktion im Detail. Erkläre: - Was die Funktion tut - Wie sie funktioniert (auf angemessenem Abstraktionsniveau) - Welche Eingaben sie verarbeitet - Welche Ausgaben sie erzeugt - Welche Sicherheitseigenschaften sie gewährleistet]

Beispiel: Die Identifikations- und Authentisierungsfunktion (TSF-1) stellt sicher, dass alle Benutzer vor dem Zugriff auf TOE-Funktionen identifiziert und authentisiert werden. Die Funktion verwendet einen Benutzernamen zur Identifikation und ein Passwort zur Authentisierung. Passwörter werden mit SHA-256 gehasht und gesalzen gespeichert.

26.3.1.2 3.1.2 Erfüllung der SFRs

[TODO: Erkläre für jede zugeordnete SFR, wie diese Sicherheitsfunktion die Anforderung erfüllt.]

SFR [TODO: ID]: - [TODO: Beschreibung, wie die SFR erfüllt wird]

SFR [TODO: ID]: - [TODO: Beschreibung, wie die SFR erfüllt wird]

26.3.1.3 3.1.3 Schnittstellen

[TODO: Beschreibe die Schnittstellen dieser TSF zu anderen TSFs oder externen Komponenten.]

- **Schnittstelle zu TSF-X:** [TODO: Beschreibung]
- **Externe Schnittstellen:** [TODO: Beschreibung]

26.3.2 3.2 TSF-2: [TODO: Name der Sicherheitsfunktion]

TSF-ID: TSF-2
Zugeordnete SFRs: [TODO: SFR-IDs]

26.3.2.1 3.2.1 Funktionsbeschreibung

[TODO: Beschreibung analog zu 3.1.1]

26.3.2.2 3.2.2 Erfüllung der SFRs

[TODO: Beschreibung analog zu 3.1.2]

26.3.2.3 3.2.3 Schnittstellen

[TODO: Beschreibung analog zu 3.1.3]

26.3.3 3.3 TSF-3: [TODO: Name der Sicherheitsfunktion]

[TODO: Weitere Sicherheitsfunktionen nach dem gleichen Schema beschreiben]

26.4 4. Zuordnung von Sicherheitsfunktionen zu SFRs

26.4.1 4.1 Coverage Matrix

Die folgende Tabelle zeigt die Zuordnung zwischen Sicherheitsfunktionen (TSFs) und Sicherheitsfunktionsanforderungen (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 Vollständigkeitsprüfung

Abdeckung der SFRs: - Anzahl der SFRs: [TODO: Anzahl] - Anzahl der abgedeckten SFRs: [TODO: Anzahl] - Abdeckungsgrad: [TODO: Prozent]

Nicht abgedeckte SFRs: [TODO: Liste alle SFRs auf, die nicht durch TSFs abgedeckt sind. Wenn alle abgedeckt sind, schreibe “Keine”.]

26.5 5. Sicherungsmaßnahmen (Assurance Measures)

26.5.1 5.1 Übersicht

Die folgenden Sicherungsmaßnahmen (Assurance Measures) werden implementiert, um die Sicherungsanforderungen (SARs) zu erfüllen:

SAR-ID	SAR-Name	Assurance Measure	Beschreibung
[TODO]	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]

26.5.2 5.2 Zuordnung zu Evaluation Assurance Level

Das TOE wird auf **[TODO: EAL-Level, z.B. EAL4]** evaluiert. Die folgenden Assurance Measures unterstützen dieses EAL:

[TODO: Liste die Assurance Measures auf, die für das gewählte EAL erforderlich sind.]

Beispiel für 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. Stärke der Sicherheitsfunktionen (Strength of Function)

26.6.1 6.1 SOF-Claim

Das TOE beansprucht folgende Stärke der Sicherheitsfunktionen (Strength of Function):

SOF-Claim: [TODO: SOF-basic / SOF-medium / SOF-high]

26.6.2 6.2 SOF-Analyse

Die folgende Tabelle zeigt die Stärke der einzelnen probabilistischen oder permutationsbasierten Sicherheitsmechanismen:

TSF-ID	Mechanismus	SOF-Level	Begründung
[TODO]	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]

26.6.3 6.3 Erfüllung des SOF-Claims

[TODO: Erkläre, wie die analysierten Mechanismen den SOF-Claim erfüllen. Zeige, dass alle relevanten Mechanismen mindestens das beanspruchte SOF-Level erreichen.]

Zusammenfassung: - Anzahl der analysierten Mechanismen: [TODO] - Niedrigstes SOF-Level: [TODO] - Erfüllung des SOF-Claims: [TODO: Ja/Nein]

26.7 7. Zusammenfassung

26.7.1 7.1 Vollständigkeit der TSS

Die TOE Summary Specification ist vollständig und deckt alle Aspekte ab:

- Alle SFRs sind durch TSFs abgedeckt
- Alle SARs sind durch Assurance Measures abgedeckt
- SOF-Claim ist analysiert und begründet
- Alle Sicherheitsfunktionen sind detailliert beschrieben

26.7.2 7.2 Verweis auf weitere Dokumente

Für detaillierte Informationen siehe:

- **0510_Assurance_Measures.md**: Detaillierte Beschreibung der Sicherungsmaßnahmen
- **0520_Functions_Rationale.md**: Begründung der Zuordnung von TSFs zu SFRs
- **0530_Coverage_Matrix.md**: Vollständige Coverage Matrix
- **0540_Strength_of_Function.md**: Detaillierte SOF-Analyse

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	[TODO]	[TODO]	Initiale Version
1.0	[TODO]	[TODO]	[TODO]

ewpage

Chapter 27

Assurance Measures (Sicherungsmaßnahmen)

Dokument-ID: 0510
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und passe die Inhalte an dein spezifisches TOE (Target of Evaluation) an.

27.1 1. Einleitung

27.1.1 1.1 Zweck

Dieses Dokument beschreibt die Assurance Measures (Sicherungsmaßnahmen), die implementiert werden, um die Security Assurance Requirements (SARs) für **[TODO: TOE-Name]** zu erfüllen.

Die Assurance Measures demonstrieren, dass: - Das TOE korrekt entwickelt wurde - Das TOE angemessen getestet wurde - Das TOE ordnungsgemäß dokumentiert ist - Das TOE sicher ausgeliefert und betrieben werden kann

27.1.2 1.2 Evaluation Assurance Level

Das TOE wird auf **[TODO: EAL-Level, z.B. EAL4]** evaluiert.

Begründung für EAL-Wahl: [TODO: Erkläre, warum dieses EAL für das TOE angemessen ist. Berücksichtige: - Die Bedrohungslandschaft - Die Kritikalität des TOE - Die Anforderungen der Stakeholder - Die Kosten-Nutzen-Abwägung]

27.2 2. Assurance Measures nach SAR-Klassen

27.2.1 2.1 Configuration Management (ACM)

27.2.1.1 2.1.1 ACM_CAP: CM Capabilities

SAR: [TODO: z.B. ACM_CAP.4 - Generation support and acceptance procedures]

Assurance Measure:

[TODO: Beschreibe die Configuration Management Capabilities. Beispiel:]

Das Projekt verwendet Git als Versionskontrollsystem. Alle TOE-Komponenten (Quellcode, Konfigurationsdateien, Build-Skripte) und Dokumentation sind im Repository versioniert.

CM-Prozess: 1. Alle Änderungen werden in Feature-Branches entwickelt 2. Code Reviews sind vor dem Merge erforderlich 3. Automatisierte Tests müssen erfolgreich sein 4. Releases werden mit Git-Tags markiert 5. Jeder Release hat eine eindeutige Versionsnummer

CM-Tools: - Versionskontrolle: Git - Repository: [TODO: URL] - Issue Tracking: [TODO: System] - Build System: [TODO: System]

Nachweise: - CM-Plan: [TODO: Dokumentpfad] - Repository-Zugriff: [TODO: URL] - Build-Logs: [TODO: Speicherort]

27.2.1.2 2.1.2 ACM_SCP: CM Scope

SAR: [TODO: z.B. ACM_SCP.2 - Problem tracking CM coverage]

Assurance Measure:

[TODO: Beschreibe den Umfang des Configuration Management. Beispiel:]

Das Configuration Management umfasst: - Alle Quellcode-Dateien des TOE - Build-Skripte und Konfigurationsdateien - Security Target und zugehörige Dokumentation - Test-Suites und Test-Dokumentation - Evaluations-Artefakte

CM-Items: | Item-ID | Beschreibung | Typ | Repository-Pfad | |———|————–|—|————–| | [TODO] | [TODO] | Source Code | [TODO] | | [TODO] | [TODO] | Documentation | [TODO] | | [TODO] | [TODO] | Test Suite | [TODO] |

Nachweise: - CM-Scope-Dokument: [TODO: Dokumentpfad] - Configuration Item List: [TODO: Dokumentpfad]

27.2.2 2.2 Delivery and Operation (ADO)

27.2.2.1 2.2.1 ADO_DEL: Delivery

SAR: [TODO: z.B. ADO_DEL.2 - Detection of modification]

Assurance Measure:

[TODO: Beschreibe die Delivery-Maßnahmen. Beispiel:]

Das TOE wird mit folgenden Sicherheitsmaßnahmen ausgeliefert:

Integritätsschutz: - Alle Releases werden mit SHA-256 gehasht - Hashes werden auf der offiziellen Website veröffentlicht - Releases werden digital signiert (GPG/PGP) - Signaturschlüssel sind über sichere Kanäle verfügbar

Auslieferungsprozess: 1. Build des TOE aus versioniertem Quellcode 2. Automatisierte Tests 3. Erstellung von Checksums 4. Digitale Signatur 5. Upload auf sichere Download-Server 6. Veröffentlichung von Checksums und Signaturen

Nachweise: - Delivery Procedures: [TODO: Dokumentpfad] - Beispiel-Checksums: [TODO: URL] - Public Key: [TODO: URL]

27.2.2.2 2.2.2 ADO_IGS: Installation, Generation, and Start-up

SAR: [TODO: z.B. ADO_IGS.1 - Installation, generation, and start-up procedures]

Assurance Measure:

[TODO: Beschreibe die Installations- und Start-Prozeduren. Beispiel:]

Installationsanleitung: - Detaillierte Schritt-für-Schritt-Anleitung - Systemvoraussetzungen - Sicherheitskonfiguration - Verifikation der Installation

Nachweise: - Installation Guide: [TODO: Dokumentpfad] - Administrator Guide: [TODO: Dokumentpfad]

27.2.3 2.3 Development (ADV)

27.2.3.1 2.3.1 ADV_FSP: Functional Specification

SAR: [TODO: z.B. ADV_FSP.2 - Security-enforcing functional specification]

Assurance Measure:

[TODO: Beschreibe die Functional Specification. Beispiel:]

Die Functional Specification beschreibt alle externen Schnittstellen des TOE:

Dokumentation: - TOE Security Functions (TSFs) sind vollständig spezifiziert - Alle TSF-Schnittstellen sind dokumentiert - Parameter, Rückgabewerte und Fehlerbehandlung sind beschrieben - Sicherheitsrelevante Effekte sind dokumentiert

Nachweise: - Functional Specification: [TODO: Dokumentpfad] - API Documentation: [TODO: Dokumentpfad]

27.2.3.2 2.3.2 ADV_IMP: Implementation Representation

SAR: [TODO: z.B. ADV_IMP.1 - Implementation representation of the TSF]

Assurance Measure:

[TODO: Beschreibe die Implementation Representation. Beispiel:]

Der Quellcode des TOE ist verfügbar und dokumentiert:

Code-Dokumentation: - Inline-Kommentare für komplexe Logik - Funktions- und Klassen-Dokumentation - Architektur-Dokumentation - Mapping zwischen Design und Code

Nachweise: - Source Code: [TODO: Repository-URL] - Code Documentation: [TODO: Dokumentpfad] - Architecture Document: [TODO: Dokumentpfad]

27.2.3.3 2.3.3 ADV_TDS: TOE Design

SAR: [TODO: z.B. ADV_TDS.2 - Architectural design]

Assurance Measure:

[TODO: Beschreibe das TOE Design. Beispiel:]

Das TOE-Design ist auf mehreren Abstraktionsebenen dokumentiert:

Design-Dokumentation: - High-Level Architecture - Subsystem-Design - Modul-Design - Sicherheitsarchitektur

Nachweise: - TOE Design Document: [TODO: Dokumentpfad] - Architecture Diagrams: [TODO: Dokumentpfad]

27.2.4 2.4 Guidance Documents (AGD)

27.2.4.1 2.4.1 AGD_ADM: Administrator Guidance

SAR: [TODO: z.B. AGD_ADM.1 - Administrator guidance]

Assurance Measure:

[TODO: Beschreibe die Administrator Guidance. Beispiel:]

Administrator-Dokumentation umfasst: - Sichere Installation und Konfiguration - Sicherheitsparameter und deren Bedeutung - Wartung und Updates - Audit-Log-Verwaltung - Backup und Recovery - Incident Response

Nachweise: - Administrator Guide: [TODO: Dokumentpfad] - Security Configuration Guide: [TODO: Dokumentpfad]

27.2.4.2 2.4.2 AGD_USR: User Guidance

SAR: [TODO: z.B. AGD_USR.1 - User guidance]

Assurance Measure:

[TODO: Beschreibe die User Guidance. Beispiel:]

Benutzer-Dokumentation umfasst: - Sichere Nutzung des TOE - Sicherheitsfunktionen und deren Verwendung - Sicherheitshinweise und Warnungen - Verantwortlichkeiten der Benutzer

Nachweise: - User Guide: [TODO: Dokumentpfad] - Security User Manual: [TODO: Dokumentpfad]

27.2.5 2.5 Life Cycle Support (ALC)

27.2.5.1 2.5.1 ALC_DVS: Development Security

SAR: [TODO: z.B. ALC_DVS.1 - Identification of security measures]

Assurance Measure:

[TODO: Beschreibe die Development Security Measures. Beispiel:]

Sicherheitsmaßnahmen in der Entwicklung: - Zugriffskontrolle auf Entwicklungssysteme - Sichere Entwicklungsumgebung - Code Review-Prozess - Security Testing während der Entwicklung - Vertraulichkeitsvereinbarungen für Entwickler

Nachweise: - Development Security Policy: [TODO: Dokumentpfad] - Access Control Matrix: [TODO: Dokumentpfad]

27.2.5.2 2.5.2 ALC_LCD: Life Cycle Definition

SAR: [TODO: z.B. ALC_LCD.1 - Developer defined life-cycle model]

Assurance Measure:

[TODO: Beschreibe das Life Cycle Model. Beispiel:]

Entwicklungslebenszyklus: 1. Requirements Analysis 2. Design 3. Implementation 4. Testing 5. Release 6. Maintenance

Nachweise: - Life Cycle Model Document: [TODO: Dokumentpfad] - Development Process Description: [TODO: Dokumentpfad]

27.2.5.3 2.5.3 ALC_TAT: Tools and Techniques

SAR: [TODO: z.B. ALC_TAT.1 - Well-defined development tools]

Assurance Measure:

[TODO: Beschreibe die verwendeten Tools und Techniken. Beispiel:]

Entwicklungs-Tools: | Tool | Version | Zweck | Sicherheitsrelevanz | |——|———|——-|———————| | [TODO] | [TODO] | [TODO] | [TODO] |

Nachweise: - Tools and Techniques Document: [TODO: Dokumentpfad]

27.2.6 2.6 Tests (ATE)

27.2.6.1 2.6.1 ATE_COV: Coverage

SAR: [TODO: z.B. ATE_COV.2 - Analysis of coverage]

Assurance Measure:

[TODO: Beschreibe die Test Coverage. Beispiel:]

Test-Abdeckung: - Alle TSF-Schnittstellen werden getestet - Alle SFRs werden durch Tests abgedeckt - Coverage-Analyse wird durchgeführt

Test-Coverage-Matrix: | TSF-ID | Test-ID | SFR-ID | Coverage | |———|———|———|———-| | [TODO] | [TODO] | [TODO] | [TODO]% |

Nachweise: - Test Coverage Report: [TODO: Dokumentpfad] - Coverage Matrix: [TODO: Dokumentpfad]

27.2.6.2 2.6.2 ATE_DPT: Depth

SAR: [TODO: z.B. ATE_DPT.1 - Testing: high-level design]

Assurance Measure:

[TODO: Beschreibe die Test Depth. Beispiel:]

Test-Tiefe: - Unit Tests für einzelne Module - Integration Tests für Subsysteme - System Tests für das gesamte TOE - Security Tests für TSFs

Nachweise: - Test Plan: [TODO: Dokumentpfad] - Test Results: [TODO: Dokumentpfad]

27.2.6.3 2.6.3 ATE_FUN: Functional Tests

SAR: [TODO: z.B. ATE_FUN.1 - Functional testing]

Assurance Measure:

[TODO: Beschreibe die Functional Tests. Beispiel:]

Funktionale Tests: - Alle TSFs werden getestet - Positive und negative Testfälle - Grenzwert-Tests - Fehlerbehandlungs-Tests

Nachweise: - Test Specification: [TODO: Dokumentpfad] - Test Results: [TODO: Dokumentpfad]

27.2.6.4 2.6.4 ATE_IND: Independent Testing

SAR: [TODO: z.B. ATE_IND.2 - Independent testing - sample]

Assurance Measure:

[TODO: Beschreibe die Independent Testing Measures. Beispiel:]

Unabhängige Tests: - Evaluator führt eine Auswahl von Tests durch - Evaluator kann eigene Tests entwickeln - Testumgebung wird bereitgestellt

Nachweise: - Test Environment Description: [TODO: Dokumentpfad] - Sample Test Results: [TODO: Dokumentpfad]

27.2.7 2.7 Vulnerability Assessment (AVA)

27.2.7.1 2.7.1 AVA_MSU: Misuse

SAR: [TODO: z.B. AVA_MSU.2 - Validation of analysis]

Assurance Measure:

[TODO: Beschreibe die Misuse Analysis. Beispiel:]

Misuse-Analyse: - Analyse von Fehlkonfigurationen - Analyse von unsicherer Nutzung - Dokumentation von Sicherheitshinweisen

Nachweise: - Misuse Analysis: [TODO: Dokumentpfad] - Security Warnings: [TODO: Dokumentpfad]

27.2.7.2 2.7.2 AVA_SOF: Strength of Function

SAR: [TODO: z.B. AVA_SOF.1 - Strength of TOE security function evaluation]

Assurance Measure:

[TODO: Beschreibe die SOF Evaluation. Beispiel:]

SOF-Evaluation: - Analyse aller probabilistischen Mechanismen - Berechnung der Angriffsstärke - Vergleich mit SOF-Claim

Nachweise: - SOF Analysis: [TODO: Dokumentpfad, siehe 0540_Strength_of_Function.md]

27.2.7.3 2.7.3 AVA_VLA: Vulnerability Analysis

SAR: [TODO: z.B. AVA_VLA.2 - Independent vulnerability analysis]

Assurance Measure:

[TODO: Beschreibe die Vulnerability Analysis. Beispiel:]

Vulnerability-Analyse: - Analyse bekannter Schwachstellen - Penetration Testing - Code-Analyse auf Sicherheitslücken - Analyse öffentlicher Vulnerability Databases

Nachweise: - Vulnerability Analysis Report: [TODO: Dokumentpfad] - Penetration Test Results: [TODO: Dokumentpfad]

27.3 3. Zusammenfassung der Assurance Measures

27.3.1 3.1 Vollständigkeitsprüfung

Die folgende Tabelle zeigt die Zuordnung aller SARs zu Assurance Measures:

SAR-ID	SAR-Name	Assurance Measure	Status
[TODO]	[TODO]	[TODO]	
[TODO]	[TODO]	[TODO]	

Zusammenfassung: - Anzahl der SARs: [TODO] - Anzahl der abgedeckten SARs: [TODO] - Abdeckungsgrad: [TODO]%

27.3.2 3.2 Nachweise und Artefakte

Die folgenden Dokumente und Artefakte dienen als Nachweise für die Assurance Measures:

Dokument	Typ	Speicherort	SAR-Zuordnung
[TODO]	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]

27.4 4. Evaluator-Aktivitäten

27.4.1 4.1 Erforderliche Evaluator-Aktivitäten

Für jede SAR sind spezifische Evaluator-Aktivitäten erforderlich:

[TODO: Liste die Evaluator-Aktivitäten für jede SAR auf. Beispiel:]

ACM_CAP.4: - Prüfung des CM-Systems - Verifikation der Versionskontrolle - Prüfung der Acceptance Procedures

ADV_FSP.2: - Review der Functional Specification - Verifikation der TSF-Beschreibungen - Prüfung der Vollständigkeit

27.4.2 4.2 Bereitstellung von Nachweisen

Alle erforderlichen Nachweise werden dem Evaluator bereitgestellt:

Bereitstellungsmethode: - [TODO: z.B. Secure File Transfer, Evaluator Portal, etc.]

Zugriff auf Systeme: - [TODO: Beschreibe, wie der Evaluator Zugriff auf Entwicklungssysteme, Test-Umgebungen, etc. erhält]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	[TODO]	[TODO]	Initiale Version
1.0	[TODO]	[TODO]	[TODO]

ewpage

Chapter 28

Functions Rationale (Begründung der Sicherheitsfunktionen)

Dokument-ID: 0520
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und passe die Inhalte an dein spezifisches TOE (Target of Evaluation) an.

28.1 1. Einleitung

28.1.1 1.1 Zweck

Dieses Dokument begründet die Zuordnung von TOE Security Functions (TSFs) zu Security Functional Requirements (SFRs) für **[TODO: TOE-Name]**.

Die Functions Rationale demonstriert, dass: - Jede SFR durch mindestens eine TSF erfüllt wird - Die TSFs die SFRs vollständig und korrekt implementieren - Keine Lücken in der Sicherheitsfunktionalität existieren - Die Zuordnung zwischen TSFs und SFRs nachvollziehbar ist

28.1.2 1.2 Struktur

Dieses Dokument ist wie folgt strukturiert:

- **Kapitel 2**: Übersicht der Zuordnung TSF SFR
- **Kapitel 3**: Detaillierte Begründung für jede SFR
- **Kapitel 4**: Vollständigkeitsanalyse
- **Kapitel 5**: Zusammenfassung

28.2 2. Übersicht der Zuordnung

28.2.1 2.1 Zuordnungsmatrix

Die folgende Matrix zeigt die Zuordnung zwischen TSFs und 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]						

Legende: - = TSF erfüllt diese SFR (vollständig oder teilweise)

28.2.2 2.2 TSF-Übersicht

TSF-ID	TSF-Name	Anzahl zugeordneter SFRs	Beschreibung
TSF-1	[TODO]	[TODO]	[TODO: Kurzbeschreibung]
TSF-2	[TODO]	[TODO]	[TODO: Kurzbeschreibung]
TSF-3	[TODO]	[TODO]	[TODO: Kurzbeschreibung]

28.3 3. Detaillierte Begründung

28.3.1 3.1 Security Audit (FAU)

28.3.1.1 3.1.1 FAU_GEN.1: Audit Data Generation

SFR-Beschreibung: [TODO: Kurze Beschreibung der SFR. Beispiel:] Das TOE muss in der Lage sein, Audit-Einträge für sicherheitsrelevante Ereignisse zu generieren.

Zugeordnete TSFs: - TSF-[TODO]: [TODO: TSF-Name]

Begründung:

[TODO: Detaillierte Begründung. Beispiel:]

TSF-3 (Audit-Funktion) erfüllt FAU_GEN.1 durch folgende Mechanismen:

1. **Ereigniserkennung**: Die Audit-Funktion überwacht alle sicherheitsrelevanten Ereignisse, einschließlich:
   - Authentisierungsversuche (erfolgreich und fehlgeschlagen)
   - Zugriffe auf geschützte Ressourcen
   - Änderungen an Sicherheitsparametern
   - Administrative Aktionen
2. **Audit-Einträge**: Für jedes Ereignis wird ein Audit-Eintrag generiert, der folgende Informationen enthält:
   - Zeitstempel
   - Ereignistyp

- Benutzer-ID
- Ergebnis (Erfolg/Fehler)
- Zusätzliche ereignisspezifische Informationen

3. **Vollständigkeit**: Alle in FAU_GEN.1 geforderten Ereignisse werden erfasst.

Erfüllungsgrad: Vollständig erfüllt

28.3.1.2 3.1.2 FAU_SAR.1: Audit Review

SFR-Beschreibung: [TODO: Beschreibung der SFR]

Zugeordnete TSFs: - TSF-[TODO]: [TODO: TSF-Name]

Begründung:

[TODO: Detaillierte Begründung analog zu 3.1.1]

Erfüllungsgrad: [TODO: Vollständig erfüllt / Teilweise erfüllt / Mit Einschränkungen]

28.3.2 3.2 Cryptographic Support (FCS)

28.3.2.1 3.2.1 FCS_CKM.1: Cryptographic Key Generation

SFR-Beschreibung: [TODO: Beschreibung der SFR]

Zugeordnete TSFs: - TSF-[TODO]: [TODO: TSF-Name]

Begründung:

[TODO: Detaillierte Begründung]

Erfüllungsgrad: [TODO]

28.3.2.2 3.2.2 FCS_COP.1: Cryptographic Operation

SFR-Beschreibung: [TODO: Beschreibung der SFR]

Zugeordnete TSFs: - TSF-[TODO]: [TODO: TSF-Name]

Begründung:

[TODO: Detaillierte Begründung]

Erfüllungsgrad: [TODO]

28.3.3 3.3 User Data Protection (FDP)

28.3.3.1 3.3.1 FDP_ACC.1: Subset Access Control

SFR-Beschreibung: [TODO: Beschreibung der SFR]

Zugeordnete TSFs: - TSF-[TODO]: [TODO: TSF-Name]

Begründung:

[TODO: Detaillierte Begründung]

Erfüllungsgrad: [TODO]

28.3.3.2 3.3.2 FDP_ACF.1: Security Attribute Based Access Control

SFR-Beschreibung: [TODO: Beschreibung der SFR]

Zugeordnete TSFs: - TSF-[TODO]: [TODO: TSF-Name]

Begründung:

[TODO: Detaillierte Begründung]

Erfüllungsgrad: [TODO]

28.3.4 3.4 Identification and Authentication (FIA)

28.3.4.1 3.4.1 FIA_UID.1: Timing of Identification

SFR-Beschreibung: [TODO: Beschreibung der SFR]

Zugeordnete TSFs: - TSF-[TODO]: [TODO: TSF-Name]

Begründung:

[TODO: Detaillierte Begründung]

Erfüllungsgrad: [TODO]

28.3.4.2 3.4.2 FIA_UAU.1: Timing of Authentication

SFR-Beschreibung: [TODO: Beschreibung der SFR]

Zugeordnete TSFs: - TSF-[TODO]: [TODO: TSF-Name]

Begründung:

[TODO: Detaillierte Begründung]

Erfüllungsgrad: [TODO]

28.3.4.3 3.4.3 FIA_AFL.1: Authentication Failure Handling

SFR-Beschreibung: [TODO: Beschreibung der SFR]

Zugeordnete TSFs: - TSF-[TODO]: [TODO: TSF-Name]

Begründung:

[TODO: Detaillierte Begründung]

Erfüllungsgrad: [TODO]

28.3.5 3.5 Security Management (FMT)

28.3.5.1 3.5.1 FMT_SMF.1: Specification of Management Functions

SFR-Beschreibung: [TODO: Beschreibung der SFR]

Zugeordnete TSFs: - TSF-[TODO]: [TODO: TSF-Name]

Begründung:

[TODO: Detaillierte Begründung]

Erfüllungsgrad: [TODO]

28.3.5.2 3.5.2 FMT_SMR.1: Security Roles

SFR-Beschreibung: [TODO: Beschreibung der SFR]

Zugeordnete TSFs: - TSF-[TODO]: [TODO: TSF-Name]

Begründung:

[TODO: Detaillierte Begründung]

Erfüllungsgrad: [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-Beschreibung: [TODO: Beschreibung der SFR]

Zugeordnete TSFs: - TSF-[TODO]: [TODO: TSF-Name]

Begründung:

[TODO: Detaillierte Begründung]

Erfüllungsgrad: [TODO]

28.3.7 3.7 TOE Access (FTA)

28.3.7.1 3.7.1 FTA_SSL.1: TSF-initiated Session Locking

SFR-Beschreibung: [TODO: Beschreibung der SFR]

Zugeordnete TSFs: - TSF-[TODO]: [TODO: TSF-Name]

Begründung:

[TODO: Detaillierte Begründung]

Erfüllungsgrad: [TODO]

28.3.8 3.8 Trusted Path/Channels (FTP)

28.3.8.1 3.8.1 FTP_TRP.1: Trusted Path

SFR-Beschreibung: [TODO: Beschreibung der SFR]

Zugeordnete TSFs: - TSF-[TODO]: [TODO: TSF-Name]

Begründung:

[TODO: Detaillierte Begründung]

Erfüllungsgrad: [TODO]

28.4 4. Vollständigkeitsanalyse

28.4.1 4.1 Abdeckung der SFRs

Statistik: - Gesamtanzahl der SFRs: [TODO] - Vollständig erfüllte SFRs: [TODO] - Teilweise erfüllte SFRs: [TODO] - Nicht erfüllte SFRs: [TODO]

Abdeckungsgrad: [TODO]%

28.4.2 4.2 Nicht erfüllte oder teilweise erfüllte SFRs

[TODO: Falls SFRs nicht vollständig erfüllt sind, liste sie hier auf und begründe:]

SFR-ID	Status	Begründung	Maßnahmen
[TODO]	Teilweise erfüllt	[TODO: Warum nur teilweise?]	[TODO: Geplante Maßnahmen]

Hinweis: Wenn alle SFRs vollständig erfüllt sind, schreibe: "Alle SFRs sind vollständig erfüllt."

28.4.3 4.3 Mehrfach-Zuordnungen

Einige SFRs werden durch mehrere TSFs erfüllt. Dies ist in folgenden Fällen der Fall:

SFR-ID	Zugeordnete TSFs	Begründung für Mehrfach-Zuordnung
[TODO]	TSF-X, TSF-Y	[TODO: Warum mehrere TSFs?]

28.4.4 4.4 TSF-Abdeckung

Die folgende Tabelle zeigt, welche TSFs wie viele SFRs erfüllen:

TSF-ID	TSF-Name	Anzahl erfüllter SFRs	Prozentsatz
TSF-1	[TODO]	[TODO]	[TODO]%
TSF-2	[TODO]	[TODO]	[TODO]%
TSF-3	[TODO]	[TODO]	[TODO]%

Analyse: [TODO: Analysiere die Verteilung. Gibt es TSFs, die sehr viele SFRs erfüllen? Ist die Verteilung ausgewogen?]

28.5 5. Zusammenfassung

28.5.1 5.1 Vollständigkeit der Zuordnung

Die Zuordnung zwischen TSFs und SFRs ist vollständig:

- Alle SFRs sind durch mindestens eine TSF abgedeckt
- Alle Zuordnungen sind begründet
- Keine Lücken in der Sicherheitsfunktionalität
- Mehrfach-Zuordnungen sind erklärt

28.5.2 5.2 Korrektheit der Zuordnung

Die Begründungen demonstrieren, dass:

- Die TSFs die SFRs korrekt implementieren
- Die TSFs die geforderte Funktionalität bereitstellen
- Die TSFs die Sicherheitseigenschaften gewährleisten
- Die Zuordnung nachvollziehbar und überzeugend ist

28.5.3 5.3 Verweis auf weitere Dokumente

Für weitere Informationen siehe:

- **0500_TOE_Summary_Specification.md**: Detaillierte Beschreibung der TSFs
- **0530_Coverage_Matrix.md**: Vollständige Coverage Matrix
- **Kapitel 4 des Security Target**: Definition der SFRs

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	[TODO]	[TODO]	Initiale Version
1.0	[TODO]	[TODO]	[TODO]

ewpage

Chapter 29

Coverage Matrix (Abdeckungsmatrix)

Dokument-ID: 0530
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und passe die Inhalte an dein spezifisches TOE (Target of Evaluation) an.

29.1 1. Einleitung

29.1.1 1.1 Zweck

Dieses Dokument enthält die vollständige Coverage Matrix für **[TODO: TOE-Name]**. Die Matrix zeigt die Zuordnung zwischen:

- Security Objectives Threats, OSPs, Assumptions
- Security Functional Requirements (SFRs) Security Objectives
- TOE Security Functions (TSFs) SFRs
- Tests TSFs und SFRs
- Assurance Measures Security Assurance Requirements (SARs)

29.1.2 1.2 Legende

Abdeckungsgrade: - = Vollständige Abdeckung - = Teilweise Abdeckung - = Unterstützende Abdeckung - (leer) = Keine Abdeckung

29.2 2. Security Objectives Coverage

29.2.1 2.1 Security Objectives for TOE Threats

Diese Matrix zeigt, wie die Security Objectives for TOE die identifizierten Threats adressieren:

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]					

Vollständigkeitsprüfung: - Anzahl Threats: [TODO] - Anzahl abgedeckter Threats: [TODO] - Nicht abgedeckte Threats: [TODO: Liste oder “Keine”]

29.2.2 2.2 Security Objectives for TOE Organizational Security Policies

Diese Matrix zeigt, wie die Security Objectives for TOE die OSPs erfüllen:

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]					

Vollständigkeitsprüfung: - Anzahl OSPs: [TODO] - Anzahl abgedeckter OSPs: [TODO] - Nicht abgedeckte OSPs: [TODO: Liste oder “Keine”]

29.2.3 2.3 Security Objectives for Environment Threats

Diese Matrix zeigt, wie die Security Objectives for Environment die Threats adressieren:

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

Diese Matrix zeigt, wie die Security Objectives for Environment die Assumptions erfüllen:

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]				

Vollständigkeitsprüfung: - Anzahl Assumptions: [TODO] - Anzahl abgedeckter Assumptions: [TODO] - Nicht abgedeckte Assumptions: [TODO: Liste oder “Keine”]

29.3 3. Security Functional Requirements Coverage

29.3.1 3.1 SFRs Security Objectives for TOE

Diese Matrix zeigt, wie die SFRs die Security Objectives for TOE erfüllen:

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					

Vollständigkeitsprüfung: - Anzahl SFRs: [TODO] - Anzahl Security Objectives for TOE: [TODO] - Nicht abgedeckte SFRs: [TODO: Liste oder “Keine”] - Nicht abgedeckte Objectives: [TODO: Liste oder “Keine”]

29.4 4. TOE Security Functions Coverage

29.4.1 4.1 TSFs SFRs

Diese Matrix zeigt, wie die TSFs die SFRs implementieren:

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-Beschreibungen:

TSF-ID	TSF-Name	Beschreibung
TSF-1	[TODO]	[TODO: Kurzbeschreibung]
TSF-2	[TODO]	[TODO: Kurzbeschreibung]
TSF-3	[TODO]	[TODO: Kurzbeschreibung]
TSF-4	[TODO]	[TODO: Kurzbeschreibung]
TSF-5	[TODO]	[TODO: Kurzbeschreibung]
TSF-6	[TODO]	[TODO: Kurzbeschreibung]

Vollständigkeitsprüfung: - Anzahl SFRs: [TODO] - Anzahl abgedeckter SFRs: [TODO] - Nicht abgedeckte SFRs: [TODO: Liste oder “Keine”]

29.5 5. Test Coverage

29.5.1 5.1 Tests TSFs

Diese Matrix zeigt, wie die Tests die TSFs verifizieren:

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-Beschreibungen:

Test-ID	Test-Name	Beschreibung	Testtyp
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

Vollständigkeitsprüfung: - Anzahl TSFs: [TODO] - Anzahl getesteter TSFs: [TODO] - Nicht getestete TSFs: [TODO: Liste oder “Keine”]

29.5.2 5.2 Tests SFRs (indirekt über TSFs)

Diese Matrix zeigt die indirekte Abdeckung von SFRs durch 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						

Vollständigkeitsprüfung: - Anzahl SFRs: [TODO] - Anzahl getesteter SFRs: [TODO] - Nicht getestete SFRs: [TODO: Liste oder “Keine”]

29.6 6. Assurance Measures Coverage

29.6.1 6.1 Assurance Measures SARs

Diese Matrix zeigt, wie die Assurance Measures die SARs erfüllen:

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 Beschreibungen:

AM-ID	AM-Name	Beschreibung
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]

Vollständigkeitsprüfung: - Anzahl SARs: [TODO] - Anzahl abgedeckter SARs: [TODO] - Nicht abgedeckte SARs: [TODO: Liste oder “Keine”]

29.7 7. Gesamtübersicht

29.7.1 7.1 End-to-End Traceability

Diese Übersicht zeigt die vollständige Rückverfolgbarkeit von Threats bis zu Tests:

```
Threats/OSPs/Assumptions
    ↓
Security Objectives (TOE & Environment)
    ↓
Security Functional Requirements (SFRs)
    ↓
TOE Security Functions (TSFs)
    ↓
Tests
```

Vollständigkeitsprüfung: - Alle Threats sind durch Security Objectives abgedeckt - Alle Security Objectives sind durch SFRs erfüllt - Alle SFRs sind durch TSFs implementiert - Alle TSFs sind durch Tests verifiziert - Alle SARs sind durch Assurance Measures erfüllt

29.7.2 7.2 Statistik

Kategorie	Anzahl	Abgedeckt	Abdeckungsgrad
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 Identifizierte Lücken

[TODO: Liste alle identifizierten Lücken in der Abdeckung auf. Wenn keine Lücken existieren, schreibe “Keine Lücken identifiziert”.]

Kategorie	Element	Lücke	Maßnahme
[TODO]	[TODO]	[TODO]	[TODO]

29.8 8. Zusammenfassung

Die Coverage Matrix demonstriert:

- Vollständige Rückverfolgbarkeit von Threats bis zu Tests
- Alle Sicherheitsanforderungen sind abgedeckt
- Alle Sicherheitsfunktionen sind getestet
- Alle Assurance Requirements sind erfüllt
- Keine kritischen Lücken in der Abdeckung

Status: [TODO: Vollständig / Mit Lücken / In Bearbeitung]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	[TODO]	[TODO]	Initiale Version
1.0	[TODO]	[TODO]	[TODO]

ewpage

Chapter 30

Strength of Function (Stärke der Sicherheitsfunktionen)

Dokument-ID: 0540
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und passe die Inhalte an dein spezifisches TOE (Target of Evaluation) an.

30.1 1. Einleitung

30.1.1 1.1 Zweck

Dieses Dokument analysiert die Strength of Function (SOF) für [**TODO: TOE-Name**]. Die SOF-Analyse bewertet die Stärke probabilistischer oder permutationsbasierter Sicherheitsmechanismen gegen verschiedene Angriffsarten.

30.1.2 1.2 SOF-Konzept

Definition: Die Strength of Function ist ein Maß für die Mindeststärke, die ein TOE-Sicherheitsmechanismus gegen direkte Angriffe bietet. Sie wird ausgedrückt als die Wahrscheinlichkeit, dass ein Angreifer den Mechanismus in einer bestimmten Zeit mit bestimmten Ressourcen überwinden kann.

SOF-Levels: - **SOF-basic**: Schutz gegen Angreifer mit begrenzten Ressourcen und Fähigkeiten - **SOF-medium**: Schutz gegen Angreifer mit moderaten Ressourcen und Fähigkeiten - **SOF-high**: Schutz gegen Angreifer mit hohen Ressourcen und Fähigkeiten

30.1.3 1.3 Anwendbarkeit

SOF gilt für folgende Arten von Mechanismen: - Passwort-basierte Authentisierung - Biometrische Authentisierung - Zufallszahlengeneratoren - Kryptografische Schlüsselgenerierung (bei probabilistischen Verfahren) - Challenge-Response-Mechanismen

SOF gilt NICHT für: - Deterministische Zugriffskontrollmechanismen - Kryptografische Algorithmen selbst (diese werden separat bewertet) - Audit-Mechanismen - Zeitstempel-Mechanismen

30.2 2. SOF-Claim

30.2.1 2.1 Beanspruchtes SOF-Level

Das TOE beansprucht folgendes SOF-Level:

SOF-Claim: [TODO: SOF-basic / SOF-medium / SOF-high]

Begründung für SOF-Claim:

[TODO: Begründe die Wahl des SOF-Levels. Beispiel:]

Das TOE wird in einer Umgebung eingesetzt, in der folgende Bedrohungen bestehen: - [TODO: Beschreibe die relevanten Threats aus Kapitel 2] - [TODO: Beschreibe die erwarteten Angreiferfähigkeiten] - [TODO: Beschreibe die Sicherheitsziele]

Basierend auf dieser Analyse ist SOF-[TODO] angemessen, da: - [TODO: Begründung 1] - [TODO: Begründung 2] - [TODO: Begründung 3]

30.3 3. Identifikation probabilistischer Mechanismen

30.3.1 3.1 Übersicht

Die folgenden probabilistischen oder permutationsbasierten Mechanismen wurden im TOE identifiziert:

Mechanismus-ID	Mechanismus-Name	TSF-ID	Typ	SOF-relevant
M-1	[TODO]	TSF-[TODO]	[TODO: Passwort/Biometrie/RNG/etc.]	Ja/Nein
M-2	[TODO]	TSF-[TODO]	[TODO]	Ja/Nein
M-3	[TODO]	TSF-[TODO]	[TODO]	Ja/Nein

30.3.2 3.2 Nicht-SOF-relevante Mechanismen

Die folgenden Mechanismen sind NICHT SOF-relevant, da sie deterministisch sind:

Mechanismus-ID	Mechanismus-Name	TSF-ID	Begründung
[TODO]	[TODO]	TSF-[TODO]	[TODO: Warum nicht SOF-relevant?]

30.4 4. SOF-Analyse

30.4.1 4.1 Mechanismus M-1: [TODO: Name]

Mechanismus-ID: M-1
TSF-ID: TSF-[TODO]
Typ: [TODO: z.B. Passwort-Authentisierung]

30.4.1.1 4.1.1 Mechanismus-Beschreibung

[TODO: Beschreibe den Mechanismus im Detail. Beispiel:]

Der Passwort-Authentisierungsmechanismus verwendet: - Passwortlänge: Minimum [TODO] Zeichen, Maximum [TODO] Zeichen - Zeichensatz: [TODO: z.B. Groß-/Kleinbuchstaben, Ziffern, Sonderzeichen] - Passwort-Komplexitätsregeln: [TODO: Beschreibe die Regeln] - Speicherung: [TODO: z.B. SHA-256 Hash mit Salt] - Fehlversuch-Handling: [TODO: z.B. Account-Sperre nach X Versuchen]

30.4.1.2 4.1.2 Angriffsszenarien

Mögliche Angriffsarten:

1. **Brute-Force-Angriff**
   - Beschreibung: Systematisches Ausprobieren aller möglichen Passwörter
   - Ressourcen: [TODO: Beschreibe erforderliche Ressourcen]
   - Zeitaufwand: [TODO: Berechne den Zeitaufwand]
2. **Wörterbuch-Angriff**
   - Beschreibung: Ausprobieren häufig verwendeter Passwörter
   - Ressourcen: [TODO: Beschreibe erforderliche Ressourcen]
   - Zeitaufwand: [TODO: Berechne den Zeitaufwand]
3. **Guessing-Angriff**
   - Beschreibung: Erraten von Passwörtern basierend auf Benutzerinformationen
   - Ressourcen: [TODO: Beschreibe erforderliche Ressourcen]
   - Erfolgswahrscheinlichkeit: [TODO: Schätze die Wahrscheinlichkeit]

30.4.1.3 4.1.3 SOF-Berechnung

Annahmen: - [TODO: Liste alle Annahmen auf, z.B.:] - Benutzer wählen Passwörter zufällig aus dem erlaubten Zeichensatz - Angreifer hat keinen Zugriff auf den Passwort-Hash - Angreifer kann maximal [TODO] Versuche pro Zeiteinheit durchführen

Berechnung:

[TODO: Führe die SOF-Berechnung durch. Beispiel:]

Zeichensatz-Größe: - Kleinbuchstaben: 26 - Großbuchstaben: 26 - Ziffern: 10 - Sonderzeichen: 10 - Gesamt: 72 Zeichen

Passwort-Raum: - Minimale Passwortlänge: 8 Zeichen - Anzahl möglicher Passwörter: 72^8 = 7,22 × 10^14

Brute-Force-Angriff: - Versuche pro Sekunde: [TODO: z.B. 1000] - Zeit für vollständige Enumeration: 7,22 × 10^14 / 1000 / 86400 / 365 = ca. 22,9 Millionen Jahre - Erfolgswahrscheinlichkeit

nach 1 Jahr: 1 / 22.900.000 4,4 × 10^-8

Account-Sperre: - Maximale Fehlversuche: [TODO: z.B. 5] - Erfolgswahrscheinlichkeit: 5 / 7,22 × 10^14 6,9 × 10^-15

Wörterbuch-Angriff: - Größe des Wörterbuchs: [TODO: z.B. 1 Million häufige Passwörter] - Erfolgswahrscheinlichkeit (ohne Account-Sperre): 1.000.000 / 7,22 × 10^14 1,4 × 10^-9 - Erfolgswahrscheinlichkeit (mit Account-Sperre): 5 / 1.000.000 = 5 × 10^-6

30.4.1.4 4.1.4 SOF-Bewertung

Ermitteltes SOF-Level: [TODO: SOF-basic / SOF-medium / SOF-high]

Begründung:

[TODO: Begründe das ermittelte SOF-Level. Beispiel:]

Basierend auf der Analyse: - Brute-Force-Angriffe sind praktisch unmöglich (Erfolgswahrscheinlichkeit < 10^-10) - Wörterbuch-Angriffe werden durch Account-Sperre effektiv verhindert (Erfolgswahrscheinlichkeit < 10^-5) - Der Mechanismus bietet Schutz gegen Angreifer mit [TODO: begrenzten/moderaten/hohen] Ressourcen

Das ermittelte SOF-Level ist **SOF-[TODO]**.

Vergleich mit SOF-Claim: - SOF-Claim: SOF-[TODO] - Ermitteltes SOF: SOF-[TODO] - Erfüllung: Ja / Nein

30.4.2 4.2 Mechanismus M-2: [TODO: Name]

Mechanismus-ID: M-2
TSF-ID: TSF-[TODO]
Typ: [TODO]

30.4.2.1 4.2.1 Mechanismus-Beschreibung

[TODO: Beschreibung analog zu 4.1.1]

30.4.2.2 4.2.2 Angriffsszenarien

[TODO: Analyse analog zu 4.1.2]

30.4.2.3 4.2.3 SOF-Berechnung

[TODO: Berechnung analog zu 4.1.3]

30.4.2.4 4.2.4 SOF-Bewertung

[TODO: Bewertung analog zu 4.1.4]

30.4.3 4.3 Mechanismus M-3: [TODO: Name]

[TODO: Weitere Mechanismen nach dem gleichen Schema analysieren]

30.5 5. Zusammenfassung der SOF-Analyse

30.5.1 5.1 Übersicht aller Mechanismen

Mechanismus-ID	Mechanismus-Name	Ermitteltes SOF	SOF-Claim	Erfüllung
M-1	[TODO]	SOF-[TODO]	SOF-[TODO]	/
M-2	[TODO]	SOF-[TODO]	SOF-[TODO]	/
M-3	[TODO]	SOF-[TODO]	SOF-[TODO]	/

30.5.2 5.2 Erfüllung des SOF-Claims

SOF-Claim: SOF-[TODO]

Analyse:

[TODO: Analysiere, ob alle Mechanismen den SOF-Claim erfüllen. Beispiel:]

- Anzahl analysierter Mechanismen: [TODO]
- Anzahl Mechanismen, die SOF-Claim erfüllen: [TODO]
- Anzahl Mechanismen, die SOF-Claim nicht erfüllen: [TODO]

Ergebnis:

[TODO: Wähle eine der folgenden Optionen:]

Alle Mechanismen erfüllen den SOF-Claim - Der SOF-Claim von SOF-[TODO] wird von allen analysierten Mechanismen erreicht oder übertroffen.

Nicht alle Mechanismen erfüllen den SOF-Claim - Die folgenden Mechanismen erfüllen den SOF-Claim nicht: [TODO: Liste] - Maßnahmen: [TODO: Beschreibe geplante Maßnahmen]

30.5.3 5.3 Schwächster Mechanismus

Schwächster Mechanismus: [TODO: Mechanismus-ID und Name]
SOF-Level: SOF-[TODO]

Begründung: [TODO: Erkläre, warum dieser Mechanismus der schwächste ist und ob dies akzeptabel ist.]

30.5.4 5.4 Annahmen und Einschränkungen

Annahmen: [TODO: Liste alle Annahmen auf, die für die SOF-Analyse getroffen wurden. Beispiel:] - Benutzer wählen Passwörter zufällig - Angreifer hat keinen physischen Zugriff auf das System - Angreifer hat keine Insider-Informationen - [TODO: Weitere Annahmen]

Einschränkungen: [TODO: Liste alle Einschränkungen der Analyse auf. Beispiel:] - Die Analyse berücksichtigt keine Side-Channel-Angriffe - Die Analyse berücksichtigt keine Social-Engineering-Angriffe - [TODO: Weitere Einschränkungen]

30.6 6. Empfehlungen

30.6.1 6.1 Verbesserungsmöglichkeiten

[TODO: Gib Empfehlungen zur Verbesserung der SOF. Beispiel:]

1. **Passwort-Komplexität erhöhen**
   - Aktuelle Mindestlänge: [TODO]
   - Empfohlene Mindestlänge: [TODO]
   - Erwartete SOF-Verbesserung: [TODO]
2. **Multi-Faktor-Authentisierung**
   - Implementierung eines zweiten Faktors (z.B. OTP, Hardware-Token)
   - Erwartete SOF-Verbesserung: [TODO]
3. **Adaptive Authentisierung**
   - Anpassung der Sicherheitsanforderungen basierend auf Risikobewertung
   - Erwartete SOF-Verbesserung: [TODO]

30.6.2 6.2 Wartung und Überwachung

[TODO: Beschreibe Maßnahmen zur Aufrechterhaltung der SOF. Beispiel:]

- Regelmäßige Überprüfung der Passwort-Richtlinien
- Monitoring von Authentisierungsversuchen
- Aktualisierung der SOF-Analyse bei Änderungen am TOE
- Berücksichtigung neuer Angriffstechniken

30.7 7. Zusammenfassung

30.7.1 7.1 Ergebnis der SOF-Analyse

Die SOF-Analyse für **[TODO: TOE-Name]** zeigt:

- Alle probabilistischen Mechanismen wurden identifiziert
- Alle Mechanismen wurden analysiert
- SOF-Berechnungen sind dokumentiert
- SOF-Claim wird erfüllt / SOF-Claim wird nicht erfüllt

Gesamtbewertung: [TODO: Zusammenfassende Bewertung]

30.7.2 7.2 Verweis auf weitere Dokumente

Für weitere Informationen siehe:

- **0500_TOE_Summary_Specification.md**: Detaillierte Beschreibung der TSFs
- **0510_Assurance_Measures.md**: AVA_SOF.1 Assurance Measure
- **Kapitel 4 des Security Target**: Definition der SFRs

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	[TODO]	[TODO]	Initiale Version
1.0	[TODO]	[TODO]	[TODO]

ewpage

Chapter 31

Protection Profile Konformität

Dokument-ID: 0600
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und HTML-Kommentare mit projektspezifischen Informationen.

31.1 Übersicht

Dieses Kapitel dokumentiert die Konformität des Security Target (ST) mit relevanten Protection Profiles (PP) gemäß ISO/IEC 15408.

PP-Konformitätsanspruch: [TODO: Strict / Demonstrable / Keine Konformität]

31.2 Protection Profile Identifikation

31.2.1 PP 1: [TODO: PP-Name]

- **PP-Titel:** [TODO: Vollständiger Titel des Protection Profile]
- **PP-Version:** [TODO: Version]
- **PP-Datum:** [TODO: Veröffentlichungsdatum]
- **PP-Registrierung:** [TODO: Registrierungsnummer falls vorhanden]
- **PP-Herausgeber:** [TODO: Organisation]
- **Konformitätstyp:** [TODO: Strict / Demonstrable]

Beschreibung:

[TODO: Beschreiben Sie das Protection Profile und warum es für dieses TOE relevant ist]

31.2.2 PP 2: [TODO: PP-Name] (falls zutreffend)

- **PP-Titel:** [TODO: Vollständiger Titel]
- **PP-Version:** [TODO: Version]
- **PP-Datum:** [TODO: Datum]
- **PP-Registrierung:** [TODO: Nummer]
- **PP-Herausgeber:** [TODO: Organisation]
- **Konformitätstyp:** [TODO: Strict / Demonstrable]

Beschreibung: [TODO: Beschreibung]

31.3 Konformitätsanspruch

31.3.1 Strict Conformance (Strikte Konformität)

[TODO: Dokumentieren Sie, dass das ST alle Anforderungen des PP ohne Änderungen übernimmt]

Konformitätserklärung: - Alle Security Functional Requirements (SFRs) aus dem PP sind im ST enthalten - Alle Security Assurance Requirements (SARs) aus dem PP sind im ST enthalten - Alle Sicherheitsziele aus dem PP sind im ST enthalten - Keine Abweichungen vom PP

31.3.2 Demonstrable Conformance (Nachweisbare Konformität)

[TODO: Dokumentieren Sie, wie das ST die Anforderungen des PP erfüllt, auch wenn Anpassungen vorgenommen wurden]

Konformitätserklärung: - Das ST erfüllt die Sicherheitsziele des PP - Das ST kann Zusatzanforderungen enthalten - Das ST kann PP-Anforderungen verfeinern oder erweitern - Alle Abweichungen sind dokumentiert und begründet

31.3.3 Keine PP-Konformität

[TODO: Begründen Sie, warum keine PP-Konformität beansprucht wird]

Begründung: [TODO: Erklären Sie die Gründe für die Entscheidung, keine PP-Konformität zu beanspruchen]

31.4 Konformitätsanalyse

31.4.1 Konformität mit [TODO: PP-Name]

31.4.1.1 Security Functional Requirements (SFR)

PP SFR	ST SFR	Status	Kommentar
[TODO: PP-SFR-ID]	[TODO: ST-SFR-ID]	Identisch / Erweitert / Verfeinert	[TODO: Erläuterung]
[TODO]	[TODO]	[TODO]	[TODO]

Zusammenfassung: [TODO: Fassen Sie die SFR-Konformität zusammen]

31.4.1.2 Security Assurance Requirements (SAR)

PP SAR	ST SAR	Status	Kommentar
[TODO: PP-SAR-ID]	[TODO: ST-SAR-ID]	Identisch / Erweitert	[TODO: Erläuterung]
[TODO]	[TODO]	[TODO]	[TODO]

Zusammenfassung: [TODO: Fassen Sie die SAR-Konformität zusammen]

31.4.1.3 Sicherheitsziele

PP-Sicherheitsziel	ST-Sicherheitsziel	Status	Kommentar
[TODO: PP-Ziel-ID]	[TODO: ST-Ziel-ID]	Identisch / Erweitert	[TODO: Erläuterung]
[TODO]	[TODO]	[TODO]	[TODO]

Zusammenfassung: [TODO: Fassen Sie die Konformität der Sicherheitsziele zusammen]

31.5 Abweichungen vom Protection Profile

31.5.1 Abweichung 1: [TODO: Titel]

- **Betroffener PP-Abschnitt:** [TODO: Abschnitt/Anforderung]
- **Art der Abweichung:** [TODO: Hinzufügung / Verfeinerung / Auslassung / Änderung]
- **Beschreibung:** [TODO: Beschreiben Sie die Abweichung im Detail]
- **Begründung:** [TODO: Erklären Sie, warum diese Abweichung notwendig ist]
- **Auswirkung auf Sicherheit:** [TODO: Bewerten Sie die Sicherheitsauswirkungen]
- **Verweis auf ST-Abschnitt:** [TODO: Abschnittsnummer im ST]

31.5.2 Abweichung 2: [TODO: Titel] (falls zutreffend)

- **Betroffener PP-Abschnitt:** [TODO]
- **Art der Abweichung:** [TODO]
- **Beschreibung:** [TODO]
- **Begründung:** [TODO]
- **Auswirkung auf Sicherheit:** [TODO]
- **Verweis auf ST-Abschnitt:** [TODO]

31.6 Zusätzliche Anforderungen

31.6.1 Zusätzliche SFRs

ST SFR	Beschreibung	Begründung
[TODO: SFR-ID]	[TODO: Kurzbeschreibung]	[TODO: Warum wurde diese SFR hinzugefügt?]
[TODO]	[TODO]	[TODO]

31.6.2 Zusätzliche SARs

ST SAR	Beschreibung	Begründung
[TODO: SAR-ID]	[TODO: Kurzbeschreibung]	[TODO: Warum wurde diese SAR hinzugefügt?]
[TODO]	[TODO]	[TODO]

31.6.3 Zusätzliche Sicherheitsziele

ST-Ziel	Beschreibung	Begründung
[TODO: Ziel-ID]	[TODO: Kurzbeschreibung]	[TODO: Warum wurde dieses Ziel hinzugefügt?]
[TODO]	[TODO]	[TODO]

31.7 Konformitätsbewertung

31.7.1 Konformitätsstatus

Gesamtbewertung: [TODO: Konform / Konform mit Abweichungen / Nicht konform]

Zusammenfassung: [TODO: Fassen Sie den Konformitätsstatus zusammen und bewerten Sie, ob das ST die Anforderungen des PP erfüllt]

31.7.2 Konformitätsnachweis

[TODO: Beschreiben Sie die Methodik und Nachweise für die PP-Konformität]

Nachweisdokumentation: - [TODO: Verweis auf relevante ST-Abschnitte] - [TODO: Verweis auf Mapping-Tabellen] - [TODO: Verweis auf Rationale-Dokumente]

31.8 Referenzen

1. [TODO: PP-Referenz 1]
2. [TODO: PP-Referenz 2]
3. [TODO: Weitere relevante Dokumente]

Nächste Schritte: 1. Identifizieren Sie alle relevanten Protection Profiles 2. Dokumentieren Sie den Konformitätsanspruch 3. Führen Sie eine detaillierte Konformitätsanalyse durch 4. Dokumentieren Sie alle Abweichungen und Zusatzanforderungen 5. Erstellen Sie Mapping-Tabellen zwischen PP und ST 6. Lassen Sie die PP-Konformität durch Evaluatoren prüfen

ewpage

Chapter 32

Rationale für Sicherheitsziele

Dokument-ID: 0610
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und HTML-Kommentare mit projektspezifischen Informationen.

32.1 Übersicht

Dieses Kapitel liefert die Rationale, die nachweist, dass die definierten Sicherheitsziele die identifizierten Sicherheitsprobleme (Bedrohungen, Organizational Security Policies, Annahmen) vollständig und angemessen adressieren.

32.2 Rationale-Methodik

32.2.1 Ansatz

[TODO: Beschreiben Sie den systematischen Ansatz zur Erstellung der Rationale]

Schritte: 1. Identifikation aller Sicherheitsprobleme (Bedrohungen, OSPs, Annahmen) 2. Zuordnung von Sicherheitszielen zu jedem Sicherheitsproblem 3. Begründung der Vollständigkeit und Angemessenheit 4. Überprüfung auf Lücken und Redundanzen

32.2.2 Vollständigkeitskriterien

[TODO: Definieren Sie, wann die Sicherheitsziele als vollständig betrachtet werden]

Kriterien: - Jede Bedrohung wird durch mindestens ein TOE-Sicherheitsziel adressiert - Jede OSP wird durch mindestens ein TOE-Sicherheitsziel adressiert - Jede Annahme wird durch mindestens ein Umgebungs-Sicherheitsziel adressiert - Keine Sicherheitsprobleme bleiben unbehandelt

32.3 Rationale für Bedrohungen

32.3.1 Bedrohung T.1: [TODO: Bedrohungsname]

Bedrohungsbeschreibung: [TODO: Kurze Zusammenfassung der Bedrohung aus Abschnitt 0210]

Adressierende Sicherheitsziele:

32.3.1.1 Sicherheitsziel O.1: [TODO: Zielname]

Begründung: [TODO: Erklären Sie detailliert, wie dieses Sicherheitsziel die Bedrohung adressiert]

Angemessenheit: [TODO: Begründen Sie, warum dieses Sicherheitsziel ausreichend ist, um die Bedrohung zu mitigieren]

32.3.1.2 Sicherheitsziel O.2: [TODO: Zielname] (falls zutreffend)

Begründung: [TODO: Erklären Sie die zusätzliche Abdeckung durch dieses Ziel]

Angemessenheit: [TODO: Begründen Sie die Notwendigkeit dieses zusätzlichen Ziels]

Zusammenfassung: [TODO: Fassen Sie zusammen, wie die Kombination der Sicherheitsziele die Bedrohung vollständig adressiert]

32.3.2 Bedrohung T.2: [TODO: Bedrohungsname]

Bedrohungsbeschreibung: [TODO: Kurze Zusammenfassung]

Adressierende Sicherheitsziele:

32.3.2.1 Sicherheitsziel O.X: [TODO: Zielname]

Begründung: [TODO: Detaillierte Erklärung]

Angemessenheit: [TODO: Begründung der Angemessenheit]

Zusammenfassung: [TODO: Zusammenfassung der Abdeckung]

32.3.3 Weitere Bedrohungen

[TODO: Dokumentieren Sie die Rationale für alle weiteren Bedrohungen]

32.4 Rationale für Organizational Security Policies (OSPs)

32.4.1 OSP P.1: [TODO: OSP-Name]

OSP-Beschreibung: [TODO: Kurze Zusammenfassung der OSP aus Abschnitt 0220]

Adressierende Sicherheitsziele:

32.4.1.1 Sicherheitsziel O.X: [TODO: Zielname]

Begründung: [TODO: Erklären Sie, wie dieses Sicherheitsziel die OSP implementiert oder unterstützt]

Angemessenheit: [TODO: Begründen Sie, warum dieses Sicherheitsziel ausreichend ist, um die OSP zu erfüllen]

Zusammenfassung: [TODO: Fassen Sie die Erfüllung der OSP zusammen]

32.4.2 OSP P.2: [TODO: OSP-Name]

OSP-Beschreibung: [TODO: Kurze Zusammenfassung]

Adressierende Sicherheitsziele:

32.4.2.1 Sicherheitsziel O.X: [TODO: Zielname]

Begründung: [TODO: Detaillierte Erklärung]

Angemessenheit: [TODO: Begründung der Angemessenheit]

Zusammenfassung: [TODO: Zusammenfassung der Erfüllung]

32.4.3 Weitere OSPs

[TODO: Dokumentieren Sie die Rationale für alle weiteren OSPs]

32.5 Rationale für Annahmen

32.5.1 Annahme A.1: [TODO: Annahmename]

Annahmebeschreibung: [TODO: Kurze Zusammenfassung der Annahme aus Abschnitt 0230]

Adressierende Sicherheitsziele:

32.5.1.1 Umgebungs-Sicherheitsziel OE.X: [TODO: Zielname]

Begründung: [TODO: Erklären Sie, wie dieses Umgebungs-Sicherheitsziel die Annahme unterstützt oder sicherstellt]

Angemessenheit: [TODO: Begründen Sie, warum dieses Ziel ausreichend ist, um die Annahme zu rechtfertigen]

Zusammenfassung: [TODO: Fassen Sie die Unterstützung der Annahme zusammen]

32.5.2 Annahme A.2: [TODO: Annahmename]

Annahmebeschreibung: [TODO: Kurze Zusammenfassung]

Adressierende Sicherheitsziele:

32.5.2.1 Umgebungs-Sicherheitsziel OE.X: [TODO: Zielname]

Begründung: [TODO: Detaillierte Erklärung]

Angemessenheit: [TODO: Begründung der Angemessenheit]

Zusammenfassung: [TODO: Zusammenfassung der Unterstützung]

32.5.3 Weitere Annahmen

[TODO: Dokumentieren Sie die Rationale für alle weiteren Annahmen]

32.6 Vollständigkeitsanalyse

32.6.1 Coverage-Matrix: Sicherheitsprobleme zu Sicherheitszielen

Sicherheitsproblem	Typ	Adressierende Sicherheitsziele	Status
T.1: [TODO]	Bedrohung	O.1, O.2	Vollständig
T.2: [TODO]	Bedrohung	O.3	Vollständig
P.1: [TODO]	OSP	O.4, O.5	Vollständig
P.2: [TODO]	OSP	O.6	Vollständig
A.1: [TODO]	Annahme	OE.1	Vollständig
A.2: [TODO]	Annahme	OE.2, OE.3	Vollständig

Legende: - **Vollständig:** Alle Aspekte des Sicherheitsproblems werden adressiert - **Teilweise:** Einige Aspekte werden adressiert, weitere Ziele erforderlich - **Unvollständig:** Sicherheitsproblem wird nicht ausreichend adressiert

32.6.2 Identifizierte Lücken

[TODO: Listen Sie alle Sicherheitsprobleme auf, die nicht vollständig durch Sicherheitsziele adressiert werden]

Lücke 1: [TODO: Beschreibung] - **Betroffenes Sicherheitsproblem:** [TODO] - **Fehlende Abdeckung:** [TODO] - **Geplante Maßnahme:** [TODO: Zusätzliches Ziel oder Begründung, warum keine Maßnahme erforderlich]

32.6.3 Redundanzanalyse

[TODO: Analysieren Sie, ob Sicherheitsziele redundant sind oder sich überschneiden]

Redundanz 1: [TODO: Beschreibung] - **Betroffene Ziele:** [TODO: O.X, O.Y] - **Überschneidung:** [TODO: Beschreiben Sie die Überschneidung] - **Begründung:** [TODO: Erklären Sie, warum beide Ziele notwendig sind, oder schlagen Sie Konsolidierung vor]

32.7 Angemessenheitsanalyse

32.7.1 Bewertungskriterien

[TODO: Definieren Sie die Kriterien für die Angemessenheit der Sicherheitsziele]

Kriterien: - Sicherheitsziele adressieren die Grundursache der Bedrohungen - Sicherheitsziele sind realistisch umsetzbar - Sicherheitsziele sind messbar und überprüfbar - Sicherheitsziele sind proportional zum Risiko

32.7.2 Angemessenheitsbewertung

Sicherheitsziel	Adressierte Probleme	Angemessenheit	Begründung
O.1: [TODO]	T.1, T.2	Angemessen	[TODO: Begründung]
O.2: [TODO]	T.1, P.1	Angemessen	[TODO: Begründung]
O.3: [TODO]	T.3	Zu prüfen	[TODO: Begründung]

Legende: - **Angemessen:** Ziel ist ausreichend, um das Problem zu adressieren - **Zu prüfen:** Weitere Analyse erforderlich - **Unzureichend:** Ziel muss verstärkt oder ergänzt werden

32.8 Zusammenfassung der Rationale

32.8.1 Vollständigkeit

[TODO: Bestätigen Sie, dass alle Sicherheitsprobleme durch Sicherheitsziele adressiert werden]

Status: [TODO: Vollständig / Unvollständig]

Begründung: [TODO: Erklären Sie den Vollständigkeitsstatus]

32.8.2 Angemessenheit

[TODO: Bestätigen Sie, dass die Sicherheitsziele angemessen sind]

Status: [TODO: Angemessen / Verbesserungsbedarf]

Begründung: [TODO: Erklären Sie den Angemessenheitsstatus]

32.8.3 Konsistenz

[TODO: Bestätigen Sie, dass die Sicherheitsziele konsistent und widerspruchsfrei sind]

Status: [TODO: Konsistent / Inkonsistenzen vorhanden]

Begründung: [TODO: Erklären Sie den Konsistenzstatus]

32.9 Referenzen

- **Abschnitt 0200:** Security Problem Definition
- **Abschnitt 0210:** Threats
- **Abschnitt 0220:** Organizational Security Policies
- **Abschnitt 0230:** Assumptions
- **Abschnitt 0300:** Security Objectives
- **Abschnitt 0320:** Security Objectives Coverage Matrix

Nächste Schritte: 1. Dokumentieren Sie die Rationale für jede Bedrohung 2. Dokumentieren Sie die Rationale für jede OSP 3. Dokumentieren Sie die Rationale für jede Annahme 4. Erstellen Sie die Coverage-Matrix 5. Führen Sie Vollständigkeits- und Angemessenheitsanalysen durch 6. Identifizieren und beheben Sie Lücken 7. Lassen Sie die Rationale durch Evaluatoren prüfen

ewpage

Chapter 33

Rationale für Sicherheitsanforderungen

Dokument-ID: 0620
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und HTML-Kommentare mit projektspezifischen Informationen.

33.1 Übersicht

Dieses Kapitel liefert die Rationale, die nachweist, dass die definierten Sicherheitsanforderungen (Security Functional Requirements - SFRs und Security Assurance Requirements - SARs) die Sicherheitsziele vollständig und angemessen erfüllen.

33.2 Rationale-Methodik

33.2.1 Ansatz

[TODO: Beschreiben Sie den systematischen Ansatz zur Erstellung der Rationale]

Schritte: 1. Zuordnung von SFRs zu TOE-Sicherheitszielen 2. Begründung der Vollständigkeit und Angemessenheit 3. Rechtfertigung aller SFR-Operationen 4. Überprüfung von SFR-Abhängigkeiten 5. Begründung der SAR-Auswahl

33.2.2 Vollständigkeitskriterien

[TODO: Definieren Sie, wann die Sicherheitsanforderungen als vollständig betrachtet werden]

Kriterien: - Jedes TOE-Sicherheitsziel wird durch mindestens eine SFR erfüllt - Alle SFR-Abhängigkeiten sind erfüllt - Alle SFR-Operationen sind begründet - SARs entsprechen dem gewählten EAL

33.3 Rationale für Security Functional Requirements (SFRs)

33.3.1 Zuordnung: Sicherheitsziele zu SFRs

33.3.1.1 Sicherheitsziel O.1: [TODO: Zielname]

Zielbeschreibung: [TODO: Kurze Zusammenfassung des Sicherheitsziels aus Abschnitt 0300]

Erfüllende SFRs:

33.3.1.1.1 SFR 1: [TODO: SFR-Identifier] - [TODO: SFR-Name] SFR-Beschreibung: [TODO: Kurze Beschreibung der SFR aus Abschnitt 0400]

Begründung: [TODO: Erklären Sie detailliert, wie diese SFR das Sicherheitsziel erfüllt]

Angemessenheit: [TODO: Begründen Sie, warum diese SFR ausreichend ist, um das Ziel zu erreichen]

Operationen:

- **Auswahl (Selection):** [TODO: Beschreiben Sie ausgewählte Optionen und Begründung]
- **Zuweisung (Assignment):** [TODO: Beschreiben Sie zugewiesene Werte und Begründung]
- **Verfeinerung (Refinement):** [TODO: Beschreiben Sie Verfeinerungen und Begründung]
- **Iteration (Iteration):** [TODO: Beschreiben Sie Iterationen und Begründung]

33.3.1.1.2 SFR 2: [TODO: SFR-Identifier] - [TODO: SFR-Name] (falls zutreffend) SFR-Beschreibung: [TODO: Kurze Beschreibung]

Begründung: [TODO: Detaillierte Erklärung]

Angemessenheit: [TODO: Begründung der Angemessenheit]

Operationen: [TODO: Dokumentieren Sie alle Operationen]

Zusammenfassung für O.1: [TODO: Fassen Sie zusammen, wie die Kombination der SFRs das Sicherheitsziel vollständig erfüllt]

33.3.1.2 Sicherheitsziel O.2: [TODO: Zielname]

Zielbeschreibung: [TODO: Kurze Zusammenfassung]

Erfüllende SFRs:

33.3.1.2.1 SFR X: [TODO: SFR-Identifier] - [TODO: SFR-Name] SFR-Beschreibung: [TODO: Kurze Beschreibung]

Begründung: [TODO: Detaillierte Erklärung]

Angemessenheit: [TODO: Begründung der Angemessenheit]

Operationen: [TODO: Dokumentieren Sie alle Operationen]

Zusammenfassung für O.2: [TODO: Zusammenfassung der Erfüllung]

33.3.2 Weitere Sicherheitsziele

[TODO: Dokumentieren Sie die Rationale für alle weiteren Sicherheitsziele]

33.4 SFR-Operationen Rationale

33.4.1 Auswahl (Selection)

SFR	Auswahloptionen	Gewählte Option	Begründung
[TODO: SFR-ID]	[TODO: Option A, B, C]	[TODO: Option B]	[TODO: Warum wurde diese Option gewählt?]
[TODO]	[TODO]	[TODO]	[TODO]

33.4.2 Zuweisung (Assignment)

SFR	Parameter	Zugewiesener Wert	Begründung
[TODO: SFR-ID]	[TODO: Parameter]	[TODO: Wert]	[TODO: Warum wurde dieser Wert zugewiesen?]
[TODO]	[TODO]	[TODO]	[TODO]

33.4.3 Verfeinerung (Refinement)

SFR	Original-Text	Verfeinerter Text	Begründung
[TODO: SFR-ID]	[TODO: Original]	[TODO: Verfeinert]	[TODO: Warum wurde verfeinert?]
[TODO]	[TODO]	[TODO]	[TODO]

33.4.4 Iteration (Iteration)

SFR	Iteration	Zweck	Begründung
[TODO: SFR-ID]	[TODO: Iteration 1]	[TODO: Zweck]	[TODO: Warum wurde iteriert?]
[TODO]	[TODO]	[TODO]	[TODO]

33.5 SFR-Abhängigkeiten Rationale

33.5.1 Abhängigkeitsanalyse

SFR	Abhängige SFR	Status	Begründung
[TODO: SFR-ID]	[TODO: Abhängige SFR]	Erfüllt / Nicht erfüllt	[TODO: Erklärung]
[TODO]	[TODO]	[TODO]	[TODO]

Legende: - **Erfüllt:** Die abhängige SFR ist im ST enthalten - **Nicht erfüllt:** Die abhängige SFR fehlt (Begründung erforderlich)

33.5.2 Nicht erfüllte Abhängigkeiten

33.5.2.1 Abhängigkeit 1: [TODO: SFR-ID] → [TODO: Abhängige SFR]

Beschreibung: [TODO: Beschreiben Sie die Abhängigkeit]

Grund für Nicht-Erfüllung: [TODO: Erklären Sie, warum die Abhängigkeit nicht erfüllt ist]

Kompensationsmaßnahmen: [TODO: Beschreiben Sie alternative Maßnahmen oder begründen Sie, warum keine Kompensation erforderlich ist]

Sicherheitsauswirkung: [TODO: Bewerten Sie die Auswirkung auf die Sicherheit]

33.6 Rationale für Security Assurance Requirements (SARs)

33.6.1 EAL-Auswahl Rationale

Gewähltes EAL: [TODO: EAL1 / EAL2 / EAL3 / EAL4 / EAL5 / EAL6 / EAL7]

Begründung: [TODO: Erklären Sie, warum dieses EAL gewählt wurde]

Faktoren: - **Bedrohungsumgebung:** [TODO: Beschreiben Sie die Bedrohungsumgebung] - **Schutzbedarf:** [TODO: Beschreiben Sie den Schutzbedarf] - **Kosten-Nutzen-Verhältnis:** [TODO: Bewerten Sie das Verhältnis] - **Marktanforderungen:** [TODO: Beschreiben Sie Marktanforderungen]

33.6.2 SAR-Komponenten Rationale

33.6.2.1 SAR-Familie: [TODO: Familie-Name]

SAR-Komponente	EAL-Standard	Augmentiert	Begründung
[TODO: SAR-ID]	Ja / Nein	Ja / Nein	[TODO: Erklärung]
[TODO]	[TODO]	[TODO]	[TODO]

Zusammenfassung: [TODO: Fassen Sie die SAR-Auswahl für diese Familie zusammen]

33.6.3 Augmentierte SARs

SAR	Standard-EAL	Gewähltes Level	Begründung
[TODO: SAR-ID]	[TODO: EAL]	[TODO: Höheres Level]	[TODO: Warum wurde augmentiert?]
[TODO]	[TODO]	[TODO]	[TODO]

33.6.4 Reduzierte SARs

SAR	Standard-EAL	Gewähltes Level	Begründung
[TODO: SAR-ID]	[TODO: EAL]	[TODO: Niedrigeres Level]	[TODO: Warum wurde reduziert?]
[TODO]	[TODO]	[TODO]	[TODO]

33.7 Vollständigkeitsanalyse

33.7.1 Coverage-Matrix: Sicherheitsziele zu SFRs

Sicherheitsziel	Erfüllende SFRs	Status
O.1: [TODO]	[TODO: SFR-IDs]	Vollständig
O.2: [TODO]	[TODO: SFR-IDs]	Vollständig
O.3: [TODO]	[TODO: SFR-IDs]	Vollständig

Legende: - **Vollständig:** Alle Aspekte des Ziels werden durch SFRs erfüllt - **Teilweise:** Einige Aspekte werden erfüllt, weitere SFRs erforderlich - **Unvollständig:** Ziel wird nicht ausreichend durch SFRs erfüllt

33.7.2 Identifizierte Lücken

[TODO: Listen Sie alle Sicherheitsziele auf, die nicht vollständig durch SFRs erfüllt werden]

Lücke 1: [TODO: Beschreibung] - **Betroffenes Sicherheitsziel:** [TODO] - **Fehlende Abdeckung:** [TODO] - **Geplante Maßnahme:** [TODO: Zusätzliche SFR oder Begründung, warum keine Maßnahme erforderlich]

33.7.3 Redundanzanalyse

[TODO: Analysieren Sie, ob SFRs redundant sind oder sich überschneiden]

Redundanz 1: [TODO: Beschreibung] - **Betroffene SFRs:** [TODO: SFR-IDs] - **Überschneidung:** [TODO: Beschreiben Sie die Überschneidung] - **Begründung:** [TODO: Erklären Sie, warum beide SFRs notwendig sind, oder schlagen Sie Konsolidierung vor]

33.8 Angemessenheitsanalyse

33.8.1 Bewertungskriterien

[TODO: Definieren Sie die Kriterien für die Angemessenheit der Sicherheitsanforderungen]

Kriterien: - SFRs sind technisch umsetzbar - SFRs sind messbar und testbar - SFRs sind proportional zum Risiko - SARs sind angemessen für das Vertrauensniveau

33.8.2 Angemessenheitsbewertung

SFR	Erfüllte Ziele	Angemessenheit	Begründung
[TODO: SFR-ID] [TODO]	[TODO: Ziele] [TODO]	Angemessen [TODO]	[TODO: Begründung] [TODO]

Legende: - **Angemessen:** SFR ist ausreichend, um die Ziele zu erfüllen - **Zu prüfen:** Weitere Analyse erforderlich - **Unzureichend:** SFR muss verstärkt oder ergänzt werden

33.9 Konsistenzanalyse

33.9.1 Interne Konsistenz

[TODO: Überprüfen Sie, ob die SFRs untereinander konsistent sind]

Identifizierte Inkonsistenzen: [TODO: Listen Sie alle Inkonsistenzen auf]

Inkonsistenz 1: [TODO: Beschreibung] - **Betroffene SFRs:** [TODO: SFR-IDs] - **Konflikt:** [TODO: Beschreiben Sie den Konflikt] - **Lösung:** [TODO: Beschreiben Sie die Lösung]

33.9.2 Konsistenz mit Sicherheitszielen

[TODO: Überprüfen Sie, ob die SFRs mit den Sicherheitszielen konsistent sind]

Identifizierte Inkonsistenzen: [TODO: Listen Sie alle Inkonsistenzen auf]

33.10 Zusammenfassung der Rationale

33.10.1 Vollständigkeit

[TODO: Bestätigen Sie, dass alle Sicherheitsziele durch SFRs erfüllt werden]

Status: [TODO: Vollständig / Unvollständig]

Begründung: [TODO: Erklären Sie den Vollständigkeitsstatus]

33.10.2 Angemessenheit

[TODO: Bestätigen Sie, dass die Sicherheitsanforderungen angemessen sind]

Status: [TODO: Angemessen / Verbesserungsbedarf]

Begründung: [TODO: Erklären Sie den Angemessenheitsstatus]

33.10.3 Konsistenz

[TODO: Bestätigen Sie, dass die Sicherheitsanforderungen konsistent sind]

Status: [TODO: Konsistent / Inkonsistenzen vorhanden]

Begründung: [TODO: Erklären Sie den Konsistenzstatus]

33.11 Referenzen

- **Abschnitt 0300:** Security Objectives
- **Abschnitt 0400:** Security Requirements
- **Abschnitt 0410:** Evaluation Assurance Level
- **Abschnitt 0430:** SFR Dependencies
- **Abschnitt 0440:** Coverage Matrix

Nächste Schritte: 1. Dokumentieren Sie die Rationale für jedes Sicherheitsziel 2. Begründen Sie alle SFR-Operationen 3. Überprüfen Sie alle SFR-Abhängigkeiten 4. Begründen Sie die SAR-Auswahl 5. Erstellen Sie die Coverage-Matrix 6. Führen Sie Vollständigkeits-, Angemessenheits- und Konsistenzanalysen durch 7. Identifizieren und beheben Sie Lücken und Inkonsistenzen 8. Lassen Sie die Rationale durch Evaluatoren prüfen

ewpage

Chapter 34

Glossar und Begriffsdefinitionen

Dokument-ID: 0630
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und HTML-Kommentare mit projektspezifischen Informationen.

34.1 Übersicht

Dieses Glossar definiert alle wichtigen Begriffe, Abkürzungen und Akronyme, die im Security Target verwendet werden. Es dient als zentrale Referenz für die Terminologie und stellt sicher, dass alle Begriffe konsistent verwendet werden.

34.2 Common Criteria Standardbegriffe

34.2.1 A

Asset (Schutzgut) [TODO: Definition oder Verweis auf ISO/IEC 15408-1] Ein Schutzgut ist eine Entität, die für den Eigentümer oder Nutzer einen Wert hat und daher geschützt werden muss.

Assumption (Annahme) [TODO: Definition oder Verweis auf ISO/IEC 15408-1] Eine Annahme ist eine Aussage über die Sicherheitsaspekte der Umgebung des TOE, die als wahr angenommen wird.

Attack Potential (Angriffspotenzial) [TODO: Definition oder Verweis auf ISO/IEC 18045] Das Angriffspotenzial ist ein Maß für die Fähigkeit eines Angreifers, einen erfolgreichen Angriff durchzuführen.

Augmentation (Augmentierung) [TODO: Definition oder Verweis auf ISO/IEC 15408-1]

Augmentierung ist das Hinzufügen von Anforderungen zu einem EAL, die über die Standard-Anforderungen hinausgehen.

34.2.2 C

Common Criteria (CC) [TODO: Definition] ISO/IEC 15408 - Internationale Norm für die Evaluierung der Sicherheit von IT-Produkten und -Systemen.

34.2.3 E

Evaluation Assurance Level (EAL) [TODO: Definition oder Verweis auf ISO/IEC 15408-3] Ein EAL ist ein Paket von Sicherheitsanforderungen (SARs), das ein bestimmtes Vertrauensniveau in die Sicherheit des TOE repräsentiert.

Evaluation Authority (Evaluierungsbehörde) [TODO: Definition] Eine Organisation, die für die Überwachung und Zertifizierung von Common Criteria-Evaluierungen verantwortlich ist.

34.2.4 O

Organizational Security Policy (OSP) [TODO: Definition oder Verweis auf ISO/IEC 15408-1] Eine OSP ist eine Sicherheitsrichtlinie, die von einer Organisation auferlegt wird und vom TOE durchgesetzt werden muss.

34.2.5 P

Protection Profile (PP) [TODO: Definition oder Verweis auf ISO/IEC 15408-1] Ein PP ist ein implementierungsunabhängiges Set von Sicherheitsanforderungen für eine Kategorie von TOEs.

34.2.6 S

Security Assurance Requirement (SAR) [TODO: Definition oder Verweis auf ISO/IEC 15408-3] Eine SAR ist eine Anforderung, die das Vertrauen in die korrekte Implementierung der Sicherheitsfunktionen sicherstellt.

Security Functional Requirement (SFR) [TODO: Definition oder Verweis auf ISO/IEC 15408-2] Eine SFR ist eine Anforderung, die eine Sicherheitsfunktion beschreibt, die das TOE bereitstellen muss.

Security Objective (Sicherheitsziel) [TODO: Definition oder Verweis auf ISO/IEC 15408-1] Ein Sicherheitsziel ist eine Aussage über die beabsichtigte Reaktion auf identifizierte Bedrohungen und/oder OSPs.

Security Target (ST) [TODO: Definition oder Verweis auf ISO/IEC 15408-1] Ein ST ist ein implementierungsspezifisches Set von Sicherheitsanforderungen und Spezifikationen für ein konkretes TOE.

Strength of Function (SOF) [TODO: Definition oder Verweis auf ISO/IEC 15408-1] SOF ist ein Maß für die Wirksamkeit einer Sicherheitsfunktion gegen direkte Angriffe.

34.2.7 T

Target of Evaluation (TOE) [TODO: Definition oder Verweis auf ISO/IEC 15408-1] Das TOE ist das IT-Produkt oder -System, das evaluiert wird.

Threat (Bedrohung) [TODO: Definition oder Verweis auf ISO/IEC 15408-1] Eine Bedrohung ist eine potenzielle Verletzung der Sicherheit durch einen Angreifer.

Threat Agent (Bedrohungsakteur) [TODO: Definition oder Verweis auf ISO/IEC 15408-1] Ein Bedrohungsakteur ist eine Entität, die eine Bedrohung ausführen kann.

TSF (TOE Security Functionality) [TODO: Definition oder Verweis auf ISO/IEC 15408-1] Die TSF ist die Gesamtheit aller Hardware-, Software- und Firmware-Komponenten des TOE, die für die Durchsetzung der Sicherheitspolitik verantwortlich sind.

TSP (TOE Security Policy) [TODO: Definition oder Verweis auf ISO/IEC 15408-1] Die TSP ist die Menge von Regeln, die die Sicherheit des TOE regeln.

34.3 TOE-spezifische Begriffe

34.3.1 [TODO: Begriff 1]

Definition: [TODO: Definieren Sie den Begriff im Kontext des TOE]

Verwendung im ST: [TODO: Beschreiben Sie, wie der Begriff im ST verwendet wird]

Verwandte Begriffe: [TODO: Listen Sie verwandte Begriffe auf]

34.3.2 [TODO: Begriff 2]

Definition: [TODO: Definition]

Verwendung im ST: [TODO: Verwendung]

Verwandte Begriffe: [TODO: Verwandte Begriffe]

34.4 Technische Begriffe

34.4.1 [TODO: Technischer Begriff 1]

Definition: [TODO: Definieren Sie den technischen Begriff]

Kontext: [TODO: Erklären Sie den Kontext, in dem der Begriff verwendet wird]

Beispiel: [TODO: Geben Sie ein Beispiel für die Verwendung]

34.4.2 [TODO: Technischer Begriff 2]

Definition: [TODO: Definition]

Kontext: [TODO: Kontext]

Beispiel: [TODO: Beispiel]

34.5 Abkürzungen und Akronyme

Abkürzung	Bedeutung	Erklärung
CC	Common Criteria	ISO/IEC 15408
EAL	Evaluation Assurance Level	Evaluierungsvertrauensstufe
IT	Information Technology	Informationstechnologie
OSP	Organizational Security Policy	Organisatorische Sicherheitsrichtlinie
PP	Protection Profile	Schutzprofil
SAR	Security Assurance Requirement	Sicherheitsvertrauensanforderung
SFR	Security Functional Requirement	Sicherheitsfunktionsanforderung
SOF	Strength of Function	Funktionsstärke
ST	Security Target	Sicherheitsvorgabe
TOE	Target of Evaluation	Evaluierungsgegenstand
TSF	TOE Security Functionality	TOE-Sicherheitsfunktionalität
TSP	TOE Security Policy	TOE-Sicherheitspolitik
[TODO]	[TODO]	[TODO]

34.6 Domänenspezifische Begriffe

34.6.1 [TODO: Domänenbegriff 1]

Definition: [TODO: Definieren Sie den domänenspezifischen Begriff]

Relevanz für TOE: [TODO: Erklären Sie die Relevanz für das TOE]

Standards-Referenz: [TODO: Verweisen Sie auf relevante Standards oder Spezifikationen]

34.6.2 [TODO: Domänenbegriff 2]

Definition: [TODO: Definition]

Relevanz für TOE: [TODO: Relevanz]

Standards-Referenz: [TODO: Referenz]

34.7 Sicherheitsbegriffe

34.7.1 [TODO: Sicherheitsbegriff 1]

Definition: [TODO: Definieren Sie den Sicherheitsbegriff]

Bedrohungskontext: [TODO: Erklären Sie den Kontext in Bezug auf Bedrohungen]

Schutzmaßnahmen: [TODO: Beschreiben Sie relevante Schutzmaßnahmen]

34.7.2 [TODO: Sicherheitsbegriff 2]

Definition: [TODO: Definition]

Bedrohungskontext: [TODO: Kontext]

Schutzmaßnahmen: [TODO: Maßnahmen]

34.8 Operationen auf SFRs

34.8.1 Assignment (Zuweisung)

Definition: Das Zuweisen eines spezifischen Wertes zu einem Parameter in einer SFR.

Notation: [assignment: Wert]

Beispiel: [assignment: 8 Zeichen] für Mindestpasswortlänge

34.8.2 Iteration (Iteration)

Definition: Das mehrfache Verwenden einer SFR mit unterschiedlichen Operationen oder für unterschiedliche Zwecke.

Notation: SFR-ID/Iteration (z.B., FDP_ACC.1/User, FDP_ACC.1/Admin)

Beispiel: Separate Zugriffskontrollrichtlinien für Benutzer und Administratoren

34.8.3 Refinement (Verfeinerung)

Definition: Das Hinzufügen von Details zu einer SFR, um sie präziser oder restriktiver zu machen.

Notation: Kursiver Text oder [refinement: Text]

Beispiel: Verfeinerung von “Benutzer” zu “authentifizierte Benutzer mit Rolle X”

34.8.4 Selection (Auswahl)

Definition: Das Auswählen einer oder mehrerer Optionen aus einer vorgegebenen Liste in einer SFR.

Notation: [selection: Option A, Option B, Option C]

Beispiel: [selection: symmetrische Verschlüsselung, asymmetrische Verschlüsselung]

34.9 Evaluierungsbegriffe

34.9.1 [TODO: Evaluierungsbegriff 1]

Definition: [TODO: Definieren Sie den Evaluierungsbegriff]

Evaluierungskontext: [TODO: Erklären Sie den Kontext in der Evaluierung]

Referenz: [TODO: Verweisen Sie auf ISO/IEC 18045 oder andere relevante Dokumente]

34.9.2 [TODO: Evaluierungsbegriff 2]

Definition: [TODO: Definition]

Evaluierungskontext: [TODO: Kontext]

Referenz: [TODO: Referenz]

34.10 Referenzen und 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 Weitere Standards

[TODO: Listen Sie weitere relevante Standards auf]

- [TODO: Standard 1]
- [TODO: Standard 2]

34.11 Terminologie-Konsistenz

34.11.1 Bevorzugte Begriffe

Bevorzugter Begriff	Vermeiden	Begründung
TOE	Produkt, System	Offizielle CC-Terminologie
Benutzer	User, Anwender	Konsistenz mit deutscher ST-Version
[TODO]	[TODO]	[TODO]

34.11.2 Groß-/Kleinschreibung

[TODO: Dokumentieren Sie Konventionen für die Groß-/Kleinschreibung von Begriffen]

Beispiele: - TOE (immer Großbuchstaben) - Security Target (Großschreibung als Eigenname) - [TODO: Weitere Beispiele]

34.12 Änderungshistorie

Version	Datum	Änderung	Autor
[TODO: 1.0]	[TODO: Datum]	Initiale Version	[TODO: Name]

Version	Datum	Änderung	Autor
[TODO]	[TODO]	[TODO]	[TODO]

Nächste Schritte: 1. Identifizieren Sie alle Begriffe, die im ST verwendet werden 2. Definieren Sie alle TOE-spezifischen Begriffe 3. Definieren Sie alle technischen und domänenspezifischen Begriffe 4. Erstellen Sie die Abkürzungsliste 5. Überprüfen Sie die Konsistenz der Terminologie im gesamten ST 6. Aktualisieren Sie das Glossar bei Änderungen am ST 7. Lassen Sie das Glossar durch Fachexperten prüfen

ewpage

Chapter 35

Referenzen und Quellenangaben

Dokument-ID: 0640
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und HTML-Kommentare mit projektspezifischen Informationen.

35.1 Übersicht

Dieses Kapitel enthält alle Referenzen und Quellenangaben, die im Security Target zitiert oder verwendet werden. Die Referenzen sind nach Kategorien organisiert, um die Navigation zu erleichtern.

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: Zugriffsdatum]

35.3 Protection Profiles

35.3.1 [TODO: PP 1 Name]

[PP1] [TODO: PP-Titel]
Version [TODO: Version], [TODO: Datum]
[TODO: Herausgeber/Organisation]
[TODO: Registrierungsnummer falls vorhanden]
[TODO: URL oder Bezugsquelle]

Relevanz: [TODO: Beschreiben Sie die Relevanz dieses PP für das TOE]

35.3.2 [TODO: PP 2 Name] (falls zutreffend)

[PP2] [TODO: PP-Titel]
Version [TODO: Version], [TODO: Datum]
[TODO: Herausgeber/Organisation]
[TODO: Registrierungsnummer]
[TODO: URL]

Relevanz: [TODO: Relevanz]

35.4 Technische Standards und Spezifikationen

35.4.1 Kryptographie-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: Weitere Krypto-Standards] [TODO: Fügen Sie weitere relevante Kryptographie-Standards hinzu]

35.4.2 Netzwerk- und Kommunikationsstandards

[**TODO: Standard 1**] [TODO: Vollständige Referenz]

[**TODO: Standard 2**] [TODO: Vollständige Referenz]

35.4.3 Hardware- und Plattform-Standards

[**TODO: Standard 1**] [TODO: Vollständige Referenz]

[**TODO: Standard 2**] [TODO: Vollständige Referenz]

35.4.4 Software-Standards

[**TODO: Standard 1**] [TODO: Vollständige Referenz]

[**TODO: Standard 2**] [TODO: Vollständige Referenz]

35.5 Sicherheitsstandards und Best Practices

35.5.1 ISO/IEC Sicherheitsstandards

[**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: Weitere ISO-Standards**] [TODO: Fügen Sie weitere relevante ISO-Standards hinzu]

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: Weitere NIST-Standards**] [TODO: Fügen Sie weitere relevante NIST-Standards hinzu]

35.5.3 Branchenspezifische Standards

[**TODO: Standard 1**] [TODO: Vollständige Referenz für branchenspezifische Standards]

[**TODO: Standard 2**] [TODO: Vollständige Referenz]

35.6 Produktdokumentation

35.6.1 TOE-Dokumentation

[TOE-SPEC] [TODO: TOE-Spezifikation Titel]
Version [TODO: Version], [TODO: Datum]
[TODO: Hersteller]
[TODO: Dokumentnummer]

[TOE-ARCH] [TODO: TOE-Architektur Dokument]
Version [TODO: Version], [TODO: Datum]
[TODO: Hersteller]
[TODO: Dokumentnummer]

[TOE-USER] [TODO: Benutzerhandbuch]
Version [TODO: Version], [TODO: Datum]
[TODO: Hersteller]
[TODO: Dokumentnummer]

[TOE-ADMIN] [TODO: Administratorhandbuch]
Version [TODO: Version], [TODO: Datum]
[TODO: Hersteller]
[TODO: Dokumentnummer]

35.6.2 Entwicklungsdokumentation

[DEV-DESIGN] [TODO: Design-Dokument]
Version [TODO: Version], [TODO: Datum]
[TODO: Internes Dokument]

[DEV-TEST] [TODO: Test-Dokumentation]
Version [TODO: Version], [TODO: Datum]
[TODO: Internes Dokument]

35.7 Evaluierungsdokumentation

35.7.1 Evaluierungsberichte

[EVAL-PLAN] [TODO: Evaluierungsplan]
Version [TODO: Version], [TODO: Datum]
[TODO: Evaluierungslabor]

[EVAL-REPORT] [TODO: Evaluierungsbericht] (falls bereits vorhanden)
Version [TODO: Version], [TODO: Datum]
[TODO: Evaluierungslabor]

35.7.2 Zertifizierungsdokumente

[CERT-SCHEME] [TODO: Zertifizierungsschema]
Version [TODO: Version], [TODO: Datum]
[TODO: Zertifizierungsstelle]
[TODO: URL]

35.8 Regulatorische Anforderungen

35.8.1 Gesetze und Verordnungen

[TODO: Gesetz/Verordnung 1] [TODO: Vollständige Referenz]

[TODO: Gesetz/Verordnung 2] [TODO: Vollständige Referenz]

35.8.2 Richtlinien und Vorgaben

[TODO: Richtlinie 1] [TODO: Vollständige Referenz]

[TODO: Richtlinie 2] [TODO: Vollständige Referenz]

35.9 Wissenschaftliche Literatur

35.9.1 Bücher

[TODO: Buch 1] [TODO: Autor(en)], *[TODO: Titel]*, [TODO: Verlag], [TODO: Jahr], ISBN [TODO: ISBN]

[TODO: Buch 2] [TODO: Vollständige Referenz]

35.9.2 Artikel und Papers

[TODO: Artikel 1] [TODO: Autor(en)], "[TODO: Titel]", *[TODO: Journal/Konferenz]*, [TODO: Jahr], [TODO: Seiten], DOI: [TODO: DOI]

[TODO: Artikel 2] [TODO: Vollständige Referenz]

35.10 Online-Ressourcen

35.10.1 Offizielle Websites

[TODO: Website 1] [TODO: Titel/Organisation]
[TODO: URL]
Zugriff: [TODO: Datum]

[TODO: Website 2] [TODO: Vollständige Referenz]

35.10.2 Technische Dokumentation

[TODO: Online-Doku 1] [TODO: Titel]
[TODO: URL]
Zugriff: [TODO: Datum]

[TODO: Online-Doku 2] [TODO: Vollständige Referenz]

35.11 Interne Dokumente

35.11.1 Sicherheitsrichtlinien

[INT-POL1] [TODO: Interne Sicherheitsrichtlinie]
Version [TODO: Version], [TODO: Datum]
[TODO: Organisation]
[TODO: Klassifizierung]

35.11.2 Prozessdokumentation

[INT-PROC1] [TODO: Interner Prozess]
Version [TODO: Version], [TODO: Datum]
[TODO: Organisation]
[TODO: Klassifizierung]

35.12 Referenz-Index

Kürzel	Titel	Kategorie	Abschnitt
[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 Verwendung im Security Target

35.13.1 Häufig zitierte Referenzen

Referenz	Verwendung im ST	Abschnitte
[CC2]	SFR-Definitionen	0400, 0420
[CC3]	SAR-Definitionen	0400, 0410
[PP1]	PP-Konformität	0600
[TODO]	[TODO]	[TODO]

35.14 Aktualisierungen und Versionierung

35.14.1 Änderungshistorie

Version	Datum	Änderung	Betroffene Referenzen
[TODO: 1.0]	[TODO: Datum]	Initiale Version	Alle
[TODO]	[TODO]	[TODO]	[TODO]

35.14.2 Veraltete Referenzen

Alte Referenz	Neue Referenz	Datum der Änderung	Grund
[TODO]	[TODO]	[TODO]	[TODO: Neue Version verfügbar]

35.15 Verfügbarkeit der Referenzen

35.15.1 Öffentlich verfügbare Dokumente

[TODO: Listen Sie auf, welche Referenzen öffentlich verfügbar sind und wo sie bezogen werden können]

35.15.2 Eingeschränkt verfügbare Dokumente

[TODO: Listen Sie auf, welche Referenzen eingeschränkt verfügbar sind und wie sie angefordert werden können]

35.15.3 Proprietäre Dokumente

[TODO: Listen Sie auf, welche Referenzen proprietär sind und unter welchen Bedingungen sie verfügbar sind]

35.16 Kontaktinformationen

35.16.1 Evaluierungslabor

Name: [TODO: Name des Evaluierungslabors]
Adresse: [TODO: Adresse]
Telefon: [TODO: Telefon]
E-Mail: [TODO: E-Mail]
Website: [TODO: Website]

35.16.2 Zertifizierungsstelle

Name: [TODO: Name der Zertifizierungsstelle]
Adresse: [TODO: Adresse]
Telefon: [TODO: Telefon]
E-Mail: [TODO: E-Mail]
Website: [TODO: Website]

35.16.3 TOE-Hersteller

Name: [TODO: Name des Herstellers]
Adresse: [TODO: Adresse]
Telefon: [TODO: Telefon]
E-Mail: [TODO: E-Mail]
Website: [TODO: Website]

Nächste Schritte: 1. Identifizieren Sie alle im ST verwendeten Referenzen 2. Sammeln Sie vollständige bibliographische Informationen 3. Organisieren Sie Referenzen nach Kategorien 4. Erstellen Sie den Referenz-Index 5. Dokumentieren Sie die Verwendung im ST 6. Überprüfen Sie die Aktualität aller Referenzen 7. Stellen Sie sicher, dass alle Referenzen verfügbar sind 8. Aktualisieren Sie die Referenzliste bei Änderungen am ST

ewpage

Chapter 36

Nachweise und Dokumentation

Dokument-ID: 0650
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Intern / Vertraulich / Streng vertraulich
Letzte Aktualisierung: {{ meta.date }}

> **Hinweis:** Dieses Dokument ist ein Template. Ersetze alle `[TODO]`-Platzhalter und HTML-Kommentare mit projektspezifischen Informationen.

36.1 Übersicht

Dieses Kapitel dokumentiert alle Nachweise und Dokumentationen, die für die Common Criteria-Evaluierung des TOE erforderlich sind. Die Nachweise sind nach SAR-Familien organisiert und entsprechen dem gewählten Evaluation Assurance Level (EAL).

Gewähltes EAL: [TODO: EAL1 / EAL2 / EAL3 / EAL4 / EAL5 / EAL6 / EAL7]

36.2 Nachweisübersicht

36.2.1 Nachweismatrix

SAR-Familie	SAR-Komponente	Erforderlicher Nachweis	Status	Verfügbarkeit
ADV	ADV_ARC.1	Security Architecture Description	[TODO: Status]	[TODO: Verfügbar/In Arbeit]
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-Familie	SAR-Komponente	Erforderlicher Nachweis	Status	Verfügbarkeit
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-Legende: - **Vollständig:** Nachweis ist vollständig und bereit für Evaluierung - **In Arbeit:** Nachweis wird erstellt - **Geplant:** Erstellung ist geplant - **Nicht erforderlich:** Für gewähltes EAL nicht erforderlich

36.3 ADV: Development (Entwicklung)

36.3.1 ADV_ARC: Security Architecture

36.3.1.1 ADV_ARC.1: Security Architecture Description

Erforderlicher Nachweis: [TODO: Beschreiben Sie den erforderlichen Nachweis gemäß ISO/IEC 15408-3]

Dokumentation: - **Dokumenttitel:** [TODO: Titel des Architekturdokuments] - **Dokumentnummer:** [TODO: Nummer] - **Version:** [TODO: Version] - **Datum:** [TODO: Datum] - **Speicherort:** [TODO: Pfad oder Referenz] - **Klassifizierung:** [TODO: Klassifizierung]

Inhalt: - Beschreibung der TOE-Sicherheitsarchitektur - Identifikation der TSF-Subsysteme - Beschreibung der Sicherheitsdomänen - Nachweis der Nicht-Umgehbarkeit - Nachweis der Domänentrennung

Status: [TODO: Vollständig / In Arbeit / Geplant]

Evaluierungshinweise: [TODO: Besondere Hinweise für Evaluatoren]

36.3.2 ADV_FSP: Functional Specification

36.3.2.1 ADV_FSP.1: Basic Functional Specification

Erforderlicher Nachweis: [TODO: Beschreiben Sie den erforderlichen Nachweis]

Dokumentation: - **Dokumenttitel:** [TODO: Titel der Funktionsspezifikation] - **Dokumentnummer:** [TODO: Nummer] - **Version:** [TODO: Version] - **Datum:** [TODO: Datum] - **Speicherort:** [TODO: Pfad] - **Klassifizierung:** [TODO: Klassifizierung]

Inhalt: - Beschreibung aller externen TSF-Schnittstellen - Beschreibung der Zwecke und Verwendung jeder Schnittstelle - Beschreibung der Parameter für jede Schnittstelle - Beschreibung der Aktionen für jede Schnittstelle - Zuordnung von SFRs zu TSF-Schnittstellen

Status: [TODO: Vollständig / In Arbeit / Geplant]

Evaluierungshinweise: [TODO: Besondere Hinweise]

36.3.3 Weitere ADV-Komponenten

[TODO: Fügen Sie weitere ADV-Komponenten hinzu, falls erforderlich (z.B., ADV_FSP.2, ADV_IMP.1, ADV_TDS.1)]

36.4 AGD: Guidance Documents (Anleitungsdokumente)

36.4.1 AGD_OPE: Operational User Guidance

36.4.1.1 AGD_OPE.1: Operational User Guidance

Erforderlicher Nachweis: [TODO: Beschreiben Sie den erforderlichen Nachweis]

Dokumentation: - **Dokumenttitel:** [TODO: Benutzerhandbuch] - **Dokumentnummer:** [TODO: Nummer] - **Version:** [TODO: Version] - **Datum:** [TODO: Datum] - **Speicherort:** [TODO: Pfad] - **Klassifizierung:** [TODO: Öffentlich / Vertraulich]

Inhalt: - Beschreibung der Sicherheitsfunktionen - Anleitung zur sicheren Nutzung - Warnungen vor unsicheren Zuständen - Beschreibung der Benutzerrollen - Anleitung zur Verwaltung von Sicherheitsattributen

Status: [TODO: Vollständig / In Arbeit / Geplant]

Zielgruppe: [TODO: Endbenutzer / Administratoren / Beide]

36.4.2 AGD_PRE: Preparative Procedures

36.4.2.1 AGD_PRE.1: Preparative Procedures

Erforderlicher Nachweis: [TODO: Beschreiben Sie den erforderlichen Nachweis]

Dokumentation: - **Dokumenttitel:** [TODO: Installations- und Konfigurationshandbuch] - **Dokumentnummer:** [TODO: Nummer] - **Version:** [TODO: Version] - **Datum:** [TODO: Datum] - **Speicherort:** [TODO: Pfad] - **Klassifizierung:** [TODO: Klassifizierung]

Inhalt: - Beschreibung der sicheren Installation - Beschreibung der sicheren Konfiguration - Beschreibung der Sicherheitsparameter - Anleitung zur Überprüfung der sicheren Konfiguration

Status: [TODO: Vollständig / In Arbeit / Geplant]

Zielgruppe: [TODO: Administratoren / Installateure]

36.5 ALC: Life-cycle Support (Lebenszyklus-Unterstützung)

36.5.1 ALC_CMC: CM Capabilities

36.5.1.1 ALC_CMC.1: Labelling of the TOE

Erforderlicher Nachweis: [TODO: Beschreiben Sie den erforderlichen Nachweis]

Dokumentation: - **Dokumenttitel:** [TODO: Configuration Management Plan] - **Dokumentnummer:** [TODO: Nummer] - **Version:** [TODO: Version] - **Datum:** [TODO: Datum] - **Speicherort:** [TODO: Pfad] - **Klassifizierung:** [TODO: Klassifizierung]

Inhalt: - Beschreibung des CM-Systems - Eindeutige Identifikation des TOE - Beschreibung der Versionskontrolle - Beschreibung der Änderungskontrolle

Status: [TODO: Vollständig / In Arbeit / Geplant]

TOE-Identifikation: - **TOE-Name:** [TODO: Name] - **TOE-Version:** [TODO: Version] - **TOE-Build:** [TODO: Build-Nummer]

36.5.2 ALC_CMS: CM Scope

36.5.2.1 ALC_CMS.1: TOE CM Coverage

Erforderlicher Nachweis: [TODO: Beschreiben Sie den erforderlichen Nachweis]

Dokumentation: - **Dokumenttitel:** [TODO: CM Scope Document] - **Dokumentnummer:** [TODO: Nummer] - **Version:** [TODO: Version] - **Datum:** [TODO: Datum] - **Speicherort:** [TODO: Pfad] - **Klassifizierung:** [TODO: Klassifizierung]

Inhalt: - Liste aller TOE-Komponenten unter CM-Kontrolle - Liste aller Evaluierungsnachweise unter CM-Kontrolle - Beschreibung der CM-Verfahren

Status: [TODO: Vollständig / In Arbeit / Geplant]

CM-Items: [TODO: Listen Sie alle CM-Items auf]

36.5.3 Weitere ALC-Komponenten

[TODO: Fügen Sie weitere ALC-Komponenten hinzu, falls erforderlich (z.B., ALC_DEL.1, ALC_DVS.1, ALC_LCD.1)]

36.6 ATE: Tests (Tests)

36.6.1 ATE_IND: Independent Testing

36.6.1.1 ATE_IND.1: Independent Testing - Conformance

Erforderlicher Nachweis: [TODO: Beschreiben Sie den erforderlichen Nachweis]

Dokumentation: - **Dokumenttitel:** [TODO: Test-Dokumentation] - **Dokumentnummer:** [TODO: Nummer] - **Version:** [TODO: Version] - **Datum:** [TODO: Datum] - **Speicherort:** [TODO: Pfad] - **Klassifizierung:** [TODO: Klassifizierung]

Inhalt: - TOE für unabhängige Tests - Testumgebung - Testdokumentation - Testressourcen

Status: [TODO: Vollständig / In Arbeit / Geplant]

Testumgebung: [TODO: Beschreiben Sie die Testumgebung]

36.6.2 Weitere ATE-Komponenten

[TODO: Fügen Sie weitere ATE-Komponenten hinzu, falls erforderlich (z.B., ATE_COV.1, ATE_FUN.1)]

36.7 AVA: Vulnerability Assessment (Schwachstellenbewertung)

36.7.1 AVA_VAN: Vulnerability Analysis

36.7.1.1 AVA_VAN.1: Vulnerability Survey

Erforderlicher Nachweis: [TODO: Beschreiben Sie den erforderlichen Nachweis]

Dokumentation: - **Dokumenttitel:** [TODO: Vulnerability Analysis Report] - **Dokumentnummer:** [TODO: Nummer] - **Version:** [TODO: Version] - **Datum:** [TODO: Datum] - **Speicherort:** [TODO: Pfad] - **Klassifizierung:** [TODO: Streng vertraulich]

Inhalt: - Analyse öffentlich bekannter Schwachstellen - Bewertung der Anwendbarkeit auf das TOE - Nachweis der Resistenz gegen Schwachstellen

Status: [TODO: Vollständig / In Arbeit / Geplant]

Schwachstellenquellen: [TODO: Listen Sie verwendete Schwachstellendatenbanken auf (z.B., CVE, NVD)]

36.7.2 Weitere AVA-Komponenten

[TODO: Fügen Sie weitere AVA-Komponenten hinzu, falls erforderlich (z.B., AVA_VAN.2, AVA_VAN.3)]

36.8 Zusätzliche Nachweise

36.8.1 Security Target (ST)

Dokumentation: - **Dokumenttitel:** Security Target für [TODO: TOE-Name] - **Dokumentnummer:** [TODO: Nummer] - **Version:** [TODO: Version] - **Datum:** [TODO: Datum] - **Speicherort:** [TODO: Pfad] - **Klassifizierung:** [TODO: Klassifizierung]

Status: [TODO: Vollständig / In Arbeit]

36.8.2 Evaluierungsplan

Dokumentation: - **Dokumenttitel:** [TODO: Evaluierungsplan] - **Dokumentnummer:** [TODO: Nummer] - **Version:** [TODO: Version] - **Datum:** [TODO: Datum] - **Speicherort:** [TODO: Pfad] - **Klassifizierung:** [TODO: Klassifizierung]

Status: [TODO: Vollständig / In Arbeit / Geplant]

36.8.3 Weitere Dokumente

[TODO: Listen Sie weitere relevante Dokumente auf]

36.9 Nachweisbereitstellung

36.9.1 Bereitstellungsplan

Nachweis	Bereitstellungsdatum	Empfänger	Übermittlungsweg
[TODO: Nachweis 1]	[TODO: Datum]	[TODO: Evaluierungslabor]	[TODO: Sicherer Upload / Physisch]
[TODO: Nachweis 2]	[TODO: Datum]	[TODO: Empfänger]	[TODO: Weg]

36.9.2 Zugriffskontrolle

Nachweis	Klassifizierung	Zugriffsberechtigte	Zugriffsmethode
[TODO: Nachweis 1]	[TODO: Klassifizierung]	[TODO: Rollen]	[TODO: Methode]
[TODO: Nachweis 2]	[TODO]	[TODO]	[TODO]

36.10 Nachweisvalidierung

36.10.1 Vollständigkeitsprüfung

Prüfdatum: [TODO: Datum]
Geprüft von: [TODO: Name/Rolle]

Ergebnis: - [ ] Alle erforderlichen Nachweise sind vorhanden - [ ] Alle Nachweise sind aktuell - [ ] Alle Nachweise sind vollständig - [ ] Alle Nachweise entsprechen den SAR-Anforderungen

Identifizierte Lücken: [TODO: Listen Sie fehlende oder unvollständige Nachweise auf]

36.10.2 Qualitätsprüfung

Prüfdatum: [TODO: Datum]
Geprüft von: [TODO: Name/Rolle]

Kriterien: - [ ] Nachweise sind klar und verständlich - [ ] Nachweise sind konsistent mit dem ST - [ ] Nachweise enthalten alle erforderlichen Informationen - [ ] Nachweise sind technisch korrekt

Identifizierte Probleme: [TODO: Listen Sie Qualitätsprobleme auf]

36.11 Nachweisarchivierung

36.11.1 Archivierungsplan

Archivierungsort: [TODO: Speicherort]
Archivierungsdauer: [TODO: Dauer]
Verantwortlich: [TODO: Rolle/Person]

Archivierte Versionen: | Nachweis | Version | Archivierungsdatum | Speicherort | |———-|———|——————-|————-| | [TODO] | [TODO] | [TODO] | [TODO] |

36.11.2 Wiederherstellungsverfahren

[TODO: Beschreiben Sie das Verfahren zur Wiederherstellung archivierter Nachweise]

36.12 Kontaktinformationen

36.12.1 Nachweis-Koordinator

Name: [TODO: Name]
Rolle: [TODO: Rolle]
E-Mail: [TODO: E-Mail]
Telefon: [TODO: Telefon]

36.12.2 Evaluierungslabor-Kontakt

Name: [TODO: Name]
Organisation: [TODO: Evaluierungslabor]
E-Mail: [TODO: E-Mail]
Telefon: [TODO: Telefon]

Nächste Schritte: 1. Identifizieren Sie alle erforderlichen Nachweise basierend auf dem gewählten EAL 2. Erstellen Sie einen Zeitplan für die Nachweiserstellung 3. Weisen Sie Verantwortlichkeiten für jeden Nachweis zu 4. Erstellen oder sammeln Sie alle erforderlichen Nachweise 5. Führen Sie Vollständigkeits- und Qualitätsprüfungen durch 6. Stellen Sie Nachweise dem Evaluierungslabor bereit 7. Archivieren Sie alle Nachweise gemäß den Anforderungen 8. Aktualisieren Sie die Nachweisdokumentation bei Änderungen

ewpage