DB NETZE

Common Criteria Schutzprofil (Protection Profile) für KISA-Module

Anforderungen an die Kommunikationsinfrastruktur für sicherheitsrelevante Anwendungen (KISA)

Certification-ID BSI-CC-PP-0085

Version 1.0, 25.Juli 2016

Final

Inhaltsverzeichnis

0 Allgemeine Dokumenteninformation

0.1 Änderungshistorie

Version	Ausgabedatum	Ersteller / Prüfer	Anmerkungen / Änderungen
0.6	3/16	D. Bossenz, extern (I.NPS214)	Initiale Erstellung durch Übernahme Text und Struktur des PP für KISA-Module Version 0.54
0.8	6.05.2016	D. Bossenz, extern (I.NPS214)	Einarbeitung Kommentierung BSI, vollständige Überarbeitung von Text und Struktur im Sinne des AG
0.85	24.06.2016	D. Bossenz, extern (I.NPS214)	Einarbeitung Kommentierung Observation_Report_2015-05-18 der Firma SRC
0.9	21.07.2016	D.Bossenz, extern (I.NPS214)	Einarbeitung Kommentierung SRC, EBA und I.NPS4
1.0	25.07.2016	D.Bossenz, extern (I.NPS214)	Übergabe an Prüfstelle

0.2 Abbildungsverzeichnis

0.3 Tabellenverzeichnis

0.4 Quellenverzeichnis

[KISA] Hans Herrmann Bock/FTZ 24, 08-P-544401-VTZ124-000001 Lastenheft KISA

[TR-IPsec] BSI TR-02102-3 "Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)"

[DIN126] DIN EN 50126 (VDE 0115 Teil 103):2000-03, Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS); Deutsche Fassung EN 50126:1999.

[DIN128] DIN EN 50128 (VDE 0831 Teil 128):2001-11, Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme; Deutsche Fassung EN 50128:2001.

[DIN129] DIN EN 50129 (VDE 0831-129):2003-12, Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik; Deutsche Fassung EN 50129:2003

[DIN159] DIN EN 50159 (VDE 0831-159):2011-04, Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante Kommunikation in Übertragungssystemen; (Deutsche Fassung EN 50159:2010)

[DIN102] DIN VDE V 0831-102 (VDE V 0831-102):2012-05, Elektrische Bahn-Signalanlagen Teil 102: Schutzprofil für technische Funktionen in der Eisenbahnsignaltechnik

[DIN104] DIN VDE V 0831-104 (VDE V 0831-104):2015-10, Elektrische Bahn-Signalanlagen – Teil 104: Leitfaden für die IT-Sicherheit auf Grundlage IEC 62443

0.5 Glossar

Logische Verbindung	Übertragungstechnische Beziehung zwischen zwei adressierbaren Punkten
Physische Verbindung	Übertragungstechnische Beziehung zwischen zwei elektrisch und/oder optisch verbundenen Punkten
Standardsoftware	Unter Standardsoftware wird Software (Programme, Programm-Module, Tools etc.) verstanden, die für die Bedürfnisse einer Mehrzahl von Kunden am Markt und nicht speziell vom Auftragnehmer für den Auftraggeber entwickelt wurde, einschließlich der zugehörigen Dokumentation. Sie zeichnet sich außerdem dadurch aus, dass sie vom Anwender selbst installiert werden soll und dass nur geringer Aufwand für die anwenderspezifische Anpassung notwendig ist.
Starke Authentisierung	Starke Authentisierung bezeichnet die Kombination von zwei Authentisierungstechniken, wie Passwort plus Transaktionsnummern (Einmalpasswörter) oder plus Chipkarte. Daher wird dies auch häufig als Zwei-Faktor-Authentisierung bezeichnet.
TK-Infrastruktur	Synonym, siehe offenes Übertragungssystem
TK-Komponenten	Telekommunikationspunkt als Abschluss einer logischen oder physischen Verbindung
Verbindlichkeit	Unter Verbindlichkeit werden die Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammengefasst. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.
Verfügbarkeit	Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.
Verschlüsselung	Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartextes aus dem Geheimtext - wird Entschlüsselung genannt.
Vertraulichkeit	Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen

	ausschließlich Befugten in der zulässigen Weise zugänglich sein.
Zertifikat (Schlüsselzertifikat)	Ein Schlüsselzertifikat ist eine elektronische Bescheinigung, mit der Signaturprüfschlüssel einer Person zugeordnet werden. Bei digitalen Signaturen wird ein Zertifikat als Bestätigung einer vertrauenswürdigen dritten Partei benötigt, um nachzuweisen, dass die zur Erzeugung der Digitalen Signatur eingesetzten kryptographischen Schlüssel wirklich zu dem Unterzeichnenden gehören.
Zugang	Mit Zugang wird die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet. Zugangsberechtigungen erlauben somit einer Person, bestimmte Ressourcen wie IT-Systeme bzw. System-Komponenten und Netze zu nutzen.
Zugriff	Mit Zugriff wird die Nutzung von Informationen bzw. Daten bezeichnet. Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen, zu nutzen oder Transaktionen auszuführen.
Zutritt	Mit Zutritt wird das Betreten von abgegrenzten Bereichen wie z. B. Räumen oder geschützten Arealen in einem Gelände bezeichnet. Zutrittsberechtigungen erlauben somit Personen, bestimmte Umgebungen zu betreten, also beispielsweise ein Gelände, ein Gebäude oder definierte Räume eines Gebäudes.

1 APE_INT: Protection Profile - Einführung

1.1 PP-Identifikation

Titel:	Common Criteria Schutzprofil (Protection Profile) für KISA-Module Anforderungen an die Kommunikationsinfrastruktur für sicherheitsrelevante Anwendungen (KISA)
Version des Dokuments:	1.0
Datum des Dokuments:	25.07.2016
Allgemeiner Status:	Final
Registrierung:	BSI-CC-PP-0085
CC Version:	CC v3.1 Revision 4
Vertrauenswürdigkeitsstufe:	EAL4+ augmentiert mit AVA_VAN.5
Auftraggeber und Autor:	Deutsche Bahn Netze AG
Stichwörter:	Elektrische Bahn-Signalanlagen, Kommunikationsinfrastruktur für sicherheitsrelevante Anwendungen, KISA, Leit- und Sicherungstechnik, LST

Dieses Schutzprofil wurde erstellt auf der Grundlage folgender Dokumente:

Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012, CCMB-2012-09-001

Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1,
Revision 4, September 2012, CCMB-2012-09-002

Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1,
Revision 4, September 2012, CCMB-2012-09-003

1.2 PP-Übersicht

Dieses Dokument resultiert aus den regulatorischen Anforderungen an die Deutsche Bahn durch die Aufsichts-, Genehmigungs- und Sicherheitsbehörde für Eisenbahnen und Eisenbahnverkehrsunternehmen (EVU), namentlich dem Eisenbahn-Bundesamt (EBA).

Die konkreten Anforderungen des EBA ergeben sich einerseits aus dem Zulassungsprozess, andererseits aus dem Lastenheft KISA Stand F1.0 B1 [KISA]. Dieses Schutzprofil ist in weiten Teilen kompatibel zu Vornorm DIN V 0831-102 [DIN102] und erweitert oder verfeinert diese wo nötig.

Das Dokument verfolgt die Intention, ein Schutzprofil (Protection Profile, PP) im Kontext der gültigen Richtlinien der CC V3.1 R4 zu definieren. Das Schutzprofil konstruiert einen Schutzbedarf des Evaluierungsgegenstandes (EVG) bzw. Target of Evaluation (TOE) anhand von Sicherheitszielen, möglichen Gefährdungen und Annahmen über die Betriebsumgebung.

Mit diesem Dokument:

- erkennen Hersteller hieraus die produkt- und verfahrensbezogenen Anforderungen für die Erstellung von Security Targets (STs) zu dem Zweck, die Evaluierung von Produkten des Herstellers nach CC zu beantragen
- erkennt der Betreiber die generischen verfahrensbezogenen Anforderungen für den Betrieb des Produktes

Das Schutzprofil spezifiziert die minimalen und generischen Sicherheitsanforderungen für Funktionen als Bestandteil einer Kommunikationsinfrastruktur für sicherheitsrelevante Anwendungen (KISA).

Als Kernfunktion wird der TOE als Start- und Endpunkt einer kryptografisch gesicherten Verbindung (KISA-Verbindung) über offene Übertragungssysteme definiert. Die kryptografische Funktion und ihre unterstützenden Funktionseinheiten werden über gesicherte Managementverbindungen von einem redundanten Sicherheitscenter überwacht und betriebsgeführt.

Einsatzumgebung sind sicherheitsrelevante Anwendungen und Systeme des Eisenbahnbetriebs. Es werden sicherheitsrelevante Nachrichten über offene Übertragungssysteme zwischen entfernten Orten des Eisenbahnbetriebs mit gleicher Integrität durch kryptografische Techniken gesichert.

Der Systemverbund aus mindestens zwei KISA-Modulen und einem redundanten Sicherheitscenter wird als KISA-Architektur bezeichnet. Das Prinzip ist in Abbildung 1 dargestellt.

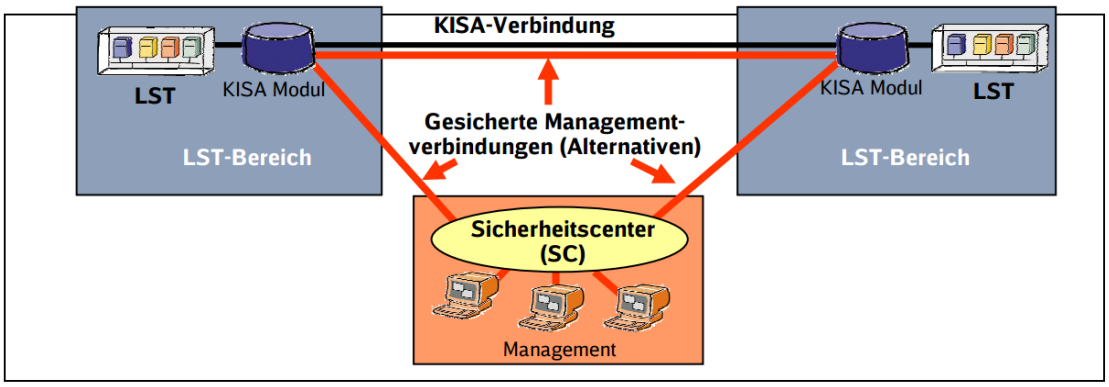

Abbildung 1: KISA-Architektur

Das KISA-Modul bezeichnet eine konzeptionelle Referenzimplementierung, welche weitere Funktionen beinhaltet, die nicht Bestandteil der Beschreibung und Gegenstand des Schutzprofils des Evaluierungsgegenstands (nachfolgend Target of Evaluation, TOE) sind. Zur eindeutigen Abgrenzung und der Tatsache, dass der TOE in verschiedene Bauformen implementiert werden kann, wird nachfolgend nur noch der TOE genannt.

1.3 Terminologie

In der Verwendung von Begriffen und Zusammenhängen gibt es im Eisenbahnwesen und der Informationssicherheit unterschiedliche Bedeutungen. Zusammen mit grundlegenden Regeln sind diese nachfolgend dargestellt:

Im Eisenbahnwesen wird der Begriff der **Sicherheit** als „Freisein von nicht akzeptierbaren Risiken eines Schadens“ [DIN129] bezeichnet. Als Risiko wird die Kombination aus Häufigkeit oder Wahrscheinlichkeit und den Folgen eines spezifizierten gefährlichen Ereignisses definiert.

Der dokumentierte Nachweis, dass das Produkt die spezifizierten Sicherheitsanforderungen erfüllt, wird als Sicherheitsnachweis bezeichnet. Der Sicherheitsnachweis bildet einen Teil der gesamten Nachweisdokumentation, die der zuständigen Sicherheitsbehörde unterbreitet wird, um die Sicherheitszulassung für ein generisches Produkt, eine Klasse von Anwendungen oder für eine spezifische Anwendung zu erlangen.

Sicherheitsrelevante (trägt Verantwortung für die Sicherheit) Information wird zwischen sicherheitsrelevanten Einrichtungen ausgetauscht [DIN159]. Einrichtungen sind als funktionale, physische Betrachtungseinheiten [DIN129] definiert.

Sicherheitsrelevante Anwendungen können **LST-Anwendungen** sein. Dies schließt auch sicherheitsrelevante elektrische, elektronische und programmierbare elektronische Systeme (E/E/PES einschließlich Teilsysteme und Einrichtungen) für elektrische Bahn-Signalanlagen [DIN104] mit ein. Bahn-Signalanlagen sichern Zugfahrten und umfassen Systeme zur Zugsteuerung, Zugsicherung zur Gewährleistung eines signaltechnisch sicheren Betriebes.

Ein **geschlossenes Übertragungssystem** mit einer festgelegten Anzahl oder festgelegten Höchstanzahl von Teilnehmern, die über ein Übertragungssystem mit wohlbekannten und festgelegten Eigenschaften miteinander verbunden sind, und bei dem das Risiko von nichtautorisiertem Zugriff als vernachlässigbar betrachtet wird [DIN159].

Ein **offenes Übertragungssystem**[1], welches für nicht bekannte Telekommunikationsdienste genutzt wird, mit einer unbekannten Anzahl von Teilnehmern, mit unbekannten und variablen Eigenschaften, denen nicht vertraut wird, und welches das Potenzial zu nicht autorisiertem Zugriff hat [DIN159].

1.4 Funktionsblöcke des TOE

Wie in Abbildung 2 dargestellt, besteht ein TOE aus vier Funktionseinheiten:

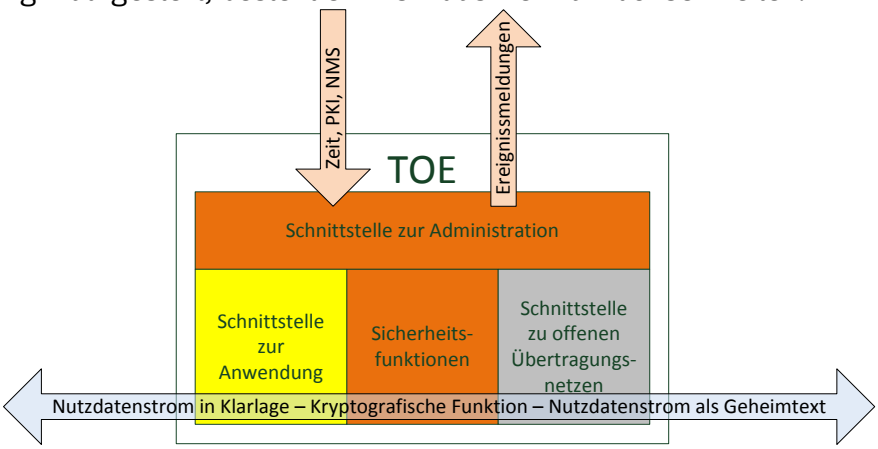

Abbildung 2: Funktionale Darstellung des TOE

Im Folgenden werden die einzelnen Funktionseinheiten beschrieben.

1.4.1 Sicherheitsfunktion: Kernfunktion Kryptografie

Der kryptografische Funktionsblock gewährleistet einen Zugriffsschutz auf sicherheitsrelevante Information. Vor dem Aufbau einer Sicherheitsbeziehung zwischen einem Quell-TOE und einem Ziel-TOE wird eine zertifikatsbasierte Authentisierung und Etablierung eines verschlüsselten Kanals ermöglicht. Jeder verschlüsselte Kanal ist mit einem Quell- und Zielbezeichner eindeutig innerhalb der KISA-Architektur adressierbar.

Die kryptografischen Funktionen verwenden als standardisiertes Verfahren die Protokollimplementierungen des IPsec. Für den Aufbau einer Sicherheitsbeziehung – engl. Security Association (SA) – wird das Internet Key Exchange (IKE) Protocol in der Version 2 eingesetzt. Die zugehörigen kryptographischen Parameter, Algorithmen, Schlüssel und Betriebsmodi für diese Verbindung müssen im Voraus durch die Rolle KISA-Supervisor festgelegt werden.

Mit der administrativen Zuweisung eines Zertifikats für einen TOE wird dieser als Teilnehmer der KISA-Architektur autorisiert. Die PKI-Endgeräteimplementierung auf dem TOE nutzt für die Validierung des X.509v3-Zertifikats das Online Certificate Status Protocol (OCSP) oder die lokal gespeicherte und täglich aktualisierte Zertifikatsperrliste. Erfolgt innerhalb einer Zeit T_{AUTH} keine Aktualisierung der lokalen Zertifikatsperrliste, sind die Zertifikate nicht mehr vertrauenswürdig.

1.4.2 Funktionseinheit: Schnittstelle zur Anwendung

Der TOE stellt eine externe Schnittstelle zu der Anwendung mit sicherheitsrelevanter Information bereit. Die Schnittstelle zur sicherheitsrelevanten Anwendung wird als „trusted interface“ (vertrauenswürdige Schnittstelle) bezeichnet. Zur Gewährleistung der authentischen Nachrichtenquelle der sicherheitsrelevanten Anwendung wird eine Filterfunktion in dem Schnittstellenmodul genutzt. Die administrative Konfiguration des Filters erfolgt als explizite Berechtigung mit den Parametern des Quell- und Zielbezeichners der Anwendung. Die Quell- und Zielbezeichner

[1] Nachfolgend wird das offene Übertragungssystem gleichbedeutend, zur besseren Verständlichkeit, auch als offenes Übertragungsnetz bezeichnet.

setzen sich aus einer Netzwerk-Adresse, Transportprotokolltyp und Portnummer der Anwendungsschicht zusammen. Die Anschaltung der vertrauenswürdigen Anwendung erfolgt physisch oder logisch, Näheres wird durch das Lastenheft definiert.

Der TOE bietet die Möglichkeit, mehrere IPsec-Verbindungen von KISA-Modulen aus verschiedenen LST-Bereichen (Konzentratorfunktion) zu verwalten. Hierbei findet keine Überschneidung der Verbindungskanäle statt. Die voneinander verschiedenen IPsec-Verbindungen werden somit logisch voneinander getrennt vom TOE verarbeitet.

1.4.2.1 Nutzdatenstrom

Als Nutzdatenstrom wird der Austausch sicherheitsrelevanter Information der Anwendung in einer Ende-zu-Ende-Beziehung zwischen zwei sicherheitsrelevanten Einrichtungen bezeichnet. Jeder Anwendung wird ein Quellbezeichner des verschlüsselten Kanals zugeordnet. Jeder Anwendung wird ein Zielbezeichner des verschlüsselten Kanals zugeordnet. Die Weiterleitung (statischer Routing-Eintrag) erfolgt als erzwungene Nutzung des verschlüsselten Kanals. Ohne erfolgreich etablierte Sicherheitsverbindung erfolgt keine Weiterleitung.

Die administrative Konfiguration der Filterfunktion und die Zuordnung von vertrauenswürdiger Anwendung und verschlüsseltem Kanal werden als ein autorisierter und geschützter Informationsfluss betrachtet.

1.4.3 Funktionseinheit: Schnittstelle zu offenen Übertragungsnetzen

Der TOE kann über eine physikalische und mindestens eine logische Schnittstelle an ein offenes Übertragungsnetz angebunden werden. Die Schnittstelle zu einem offenen Übertragungsnetz gilt als „unsichere“ Seite und wird als „untrusted interface“ (nicht vertrauenswürdige Seite) bezeichnet. Die Schnittstelle ermöglicht den Aufbau von Verbindungen in dem offenen Übertragungssystem zur Übertragung eines verschlüsselten Kanals. Die Funktionseinheit schützt sich selbst und die Kernfunktion vor Angriffen aus dem offenen Übertragungsnetz.

1.4.4 Funktionseinheit: Schnittstelle zur Betriebsführung

Die Administration und Statusüberwachung des TOE und seiner inkludierten Funktionseinheiten erfolgt mit dem Betriebsführungsmodul. Das Betriebsführungsmodul umfasst eine physische und/oder logische Schnittstelle zu mindestens einem zentralen Sicherheitscenter. Das zentrale Sicherheitscenter stellt die Infrastrukturdienste Zeit, Netzmanagement und einen Verzeichnisdienst für Zertifikate bereit.

1.5 APE_CCL: Konformität / Postulat der Übereinstimmung mit den CC

Das Schutzprofil wurde gemäß Common Criteria Version 3.1 Revision 4 erstellt und ist

CC Teil 2 konform (conformant) und
CC Teil 3 konform (conformant).

1.6 Schutzprofil-Konformität

Dieses Schutzprofil behauptet keine Konformität zu einem anderen Schutzprofil.

1.7 Paket-Konformität

Das Schutzprofil fordert die Vertrauenswürdigkeitsstufe EAL4, augmentiert mit AVA_VAN.5 wie in CC Teil 3 definiert, daher ist das Schutzprofil CC Teil 3 konform (conformant). Daraus resultiert die Bezeichnung „EAL4+“.

1.8 Begründung der Übereinstimmung

Es wurden keine über den Teil 2 hinausgehenden funktionalen Anforderungen und keine über den Teil 3 hinausgehenden Anforderungen an die Vertrauenswürdigkeit definiert.

1.9 Festlegung der Konformität

Sicherheitsvorgaben (Security Targets) oder Schutzprofile (Protection Profiles), die Konformität zu diesem Schutzprofil (Schutzprofil für KISA-Module) behaupten wollen, müssen

strict conformance

behaupten.

1.10 PP-Organisation

Der Aufbau dieses Schutzprofils folgt der Mustergliederung, die durch Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and General Model, Anhang A, vorgegeben wird.

1.11 Hinweise zur Anwendung des PPs auf unterschiedliche Ausprägungen des TOEs

Dieses Schutzprofil soll als Basis für Evaluierungen unterschiedlicher Bauformen des TOEs dienen. Sowohl Einboxlösungen als auch Mehrkomponentenlösungen sollen Konformität zu diesem PP behaupten können.

Der TOE kann als selbständiges Gerät (Einboxlösung) oder als Bestandteil eines umfassenderen Systems des Eisenbahnbetriebs (Mehrkomponentenlösung), implementiert werden. Somit fordert dieses Schutzprofil keine festgelegte Kombination von zusätzlicher Hardware, Software oder Firmware, die nicht zum TOE gehört, aber für dessen Betrieb erforderlich ist. Es bleibt daher dem ST-Autor überlassen, die genaue technische Plattform zu beschreiben, die für einen spezifischen TOE erforderlich ist. Zudem soll er erläutern, wie der TOE damit in die zukünftigen Systeme des Eisenbahnbetriebs integriert werden kann.

Um diese Allgemeingültigkeit des Schutzprofils zu erreichen, war es erforderlich, die verbindlichen Inhalte im Schutzprofil jeweils auf die Minimalanforderungen an den TOE zu beschränken. Jede spezielle Ausprägung des TOE kann zusätzliche Sicherheitsanforderungen nach sich ziehen.

2 TOE-Beschreibung

2.1 Einsatzumgebung des TOE

Als Einsatzumgebung werden Systeme des Eisenbahnbetriebs angegeben. Die eingesetzten Systeme müssen einem Lebenszyklus gemäß der normativen Regelungen der DIN EN 50126:2000 [DIN126] folgen. Es wird ein prozessuales Vorgehen beschrieben für das Definieren und Umsetzen von Anforderungen zum Erreichen von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (engl.: Reliability, Availability, Maintainability, Safety – kurz RAMS) bei der Systemspezifikation von Systemen im Eisenbahnbetrieb. Als Systeme des Eisenbahnbetriebs werden Bahnanwendungen, Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme bezeichnet. Mitgeltend sind die Normenwerke DIN EN 50128:2012 [DIN128] und DIN EN 50129:2003 [DIN129] für Software und Hardware. Und im Besonderen für die Übertragung von sicherheitsrelevanten Nachrichten gilt die Norm DIN EN 50159:2011 [DIN159].

Das normierte Vorgehen ermittelt und spezifiziert ein für einzelne Anwendungen ausreichendes Schutzniveau für die funktionale Sicherheit. Funktionale Sicherheit wird erreicht, wenn sicherheitsgerichtete Steuerungen ihre Sicherheitsfunktionen zuverlässig erbringen. Beeinträchtigungen von außen oder Wechselwirkungen zwischen verschiedenen sicherheitsrelevanten Anwendungen stellen eine Gefährdung der funktionalen Sicherheit dar und werden mit einer entsprechenden Fehleranalyse untersucht und anhand von statistischem Material abgeschätzt. Es werden Maßnahmen in den Systemen zur Risikominimierung angewandt.

Zur Aufrechterhaltung der angewandten Maßnahmen müssen die Systeme des Eisenbahnbetriebs in einer kontrollierten Umgebung (Kontrollbereich) ausgeführt werden. Zutritt und Zugang wird nur berechtigten Personen gewährt, ebenso werden die Umweltbedingungen kontrolliert. Mit verschiedenen Maßnahmen, wie das Betreiben von Gefahrenmeldeanlagen (GMA), Zutrittskontrollanlagen (ZKA), Videoüberwachungsanlagen (VÜA) und Einbruchsmeldeanlagen (EMA) wird der Kontrollbereich durchgesetzt. Der Umfang und die Stärke der Maßnahmen werden durch eine Schutzbedarfsfeststellung objektbezogen durch die Sicherheitsbeauftragten festgelegt. Bereiche gleicher Sicherheit bilden einen Integritätsbereich (IB).

Die Anforderungen an die sicherheitsrelevante Kommunikation zwischen Anwendungen wird durch die normativen Regelungen der DIN EN 50159:2011 definiert. Es werden drei Übertragungssysteme anhand der Kriterien von Garantien der Zuverlässigkeit und Verfügbarkeit, Beständigkeit der Leistungsmerkmale und ausgeübter Zugriffskontrolle unterschieden. Innerhalb des Integritätsbereichs werden die Kriterien für Kategorie-1- oder Kategorie-2-Übertragungssysteme erfüllt. Die identifizierten Bedrohungen auf diese kategorisierten Übertragungssysteme müssen durch die sicherheitsrelevante Anwendung beherrscht werden. Die zu beherrschenden Bedrohungen sind Nachrichtenfehler:

- Wiederholung
- Auslassung
- Einfügung
- Resequenzierung
- Verfälschung
- Verzögerung

Für ein Übertragungssystem der Kategorie-3 besteht ein Risiko des nicht autorisierten Zugriffs mit den resultierenden Bedrohungen durch nicht autorisierte Software-Modifikationen oder die Übertragung nicht autorisierter Nachrichten.

Für die Übertragung von sicherheitsrelevanten Nachrichten der Systeme der Leit- und Sicherungstechnik über offene Übertragungssysteme werden in der Norm DIN EN 50159:2011 allgemeine Anforderungen genannt, die in der Systemsicherheitsanforderungsspezifikation respektive dem vorliegenden Schutzprofil berücksichtigt werden.

Die Kommunikationsinfrastruktur für sicherheitsrelevante Anwendungen (KISA) liefert eine Architektur mit dem Ziel, wesentliche Aufgaben des IT-Sicherheitsmanagements für die Systeme des Eisenbahnbetriebs zu übernehmen. Die bloße Fähigkeit der Architektur, dieses Spektrum abzudecken bedeutet nicht, dass alle diese Anwendungsmöglichkeiten vom ersten Tag an genutzt werden.

Ein Bestandteil der Architektur ist das KISA-Modul mit der kryptografischen Teilfunktion als TOE zur Übertragung sicherheitsrelevanter Nachrichten zwischen LST-Anwendung mithilfe einer verschlüsselten Verbindung. Realisiert wird die verschlüsselte Verbindung zwischen zwei gleichen Integritätsbereichen. Der TOE ist immer Bestandteil desselben Integritätsbereichs wie die zu sichernde Anwendung - dessen Zutritt, Zugang und Umweltbedingungen kontrolliert werden. Diese Integritätsbereiche sind verortet in den Feldelementeanschlusskästen im Gleisfeld, Konzentratorstandorten, Einsatzbereichen des ETCS, Stellwerken, Bedienplätzen und Betriebszentralen. Allgemein können alle Betriebsstellen des Eisenbahnbetriebs Aufstellbereiche des TOE sein.

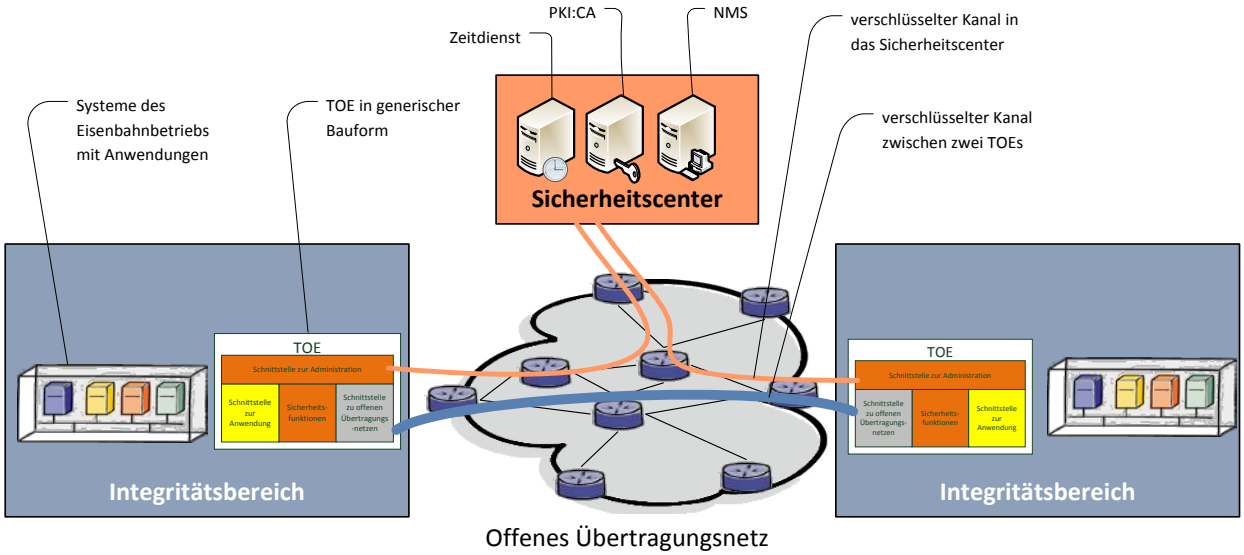

Abbildung 3: Einsatzumgebung des TOE, logische Kommunikationsbeziehungen

Der TOE wird durch eine Sicherheitsbetriebsführung im 24/7-Schichtbetrieb aus einem Sicherheitscenter (KISA-Sicherheitscenter) überwacht. Es bestehen Handlungsanweisungen für die Betriebsführung nach dem ITILv3-Rahmenwerk. Die Kommunikation mit dem TOE erfolgt über einen sicheren Kanal. Folgende Netzdienste werden durch das Sicherheitscenter erbracht:

1) **Netzwerkmanagementsystem (NMS):** Das System besteht aus verschiedenen Einzelkomponenten, die über Standardschnittstellen als Systemverbund alle Funktionen für ein Netzmanagement erfüllen. Dazu gehören folgende Funktionen:

   - Das Ereignismanagement erfasst alle Alarmmeldungen des TOEs und erstellt Störungsmeldungen, die durch den Operator weiter bearbeitet werden müssen. Alle Maßnahmen zur Störungsbeseitigung werden mit zeitlichen Verlauf und beteiligten Personen dokumentiert.
   - Das Konfigurationsmanagement verwaltet die Konfigurationen aller TOE und der konfigurierten Kommunikationsverbindungen. Es wird der Ist-Stand dokumentiert und liefert einen Überblick über die im Netz verteilten TOE. Über die Konfigurationsdaten unterstützt das Konfigurationsmanagement in der Datenwiederherstellung und Wiederanlauf. Das System unterstützt Administratoren und den Supervisor bei der Konfiguration der TOEs.
   - Das Accessmanagement verwaltet die Identitäten und Rollen, die Zugang auf den TOE haben. Es wird ein starkes Authentisierungsverfahren verwendet (2-Faktor-Authentisierung). Mit Benutzername, Passwort und Token meldet sich eine Identität an dem NMS an. Das NMS gewährt Zugang zu dem TOE. Der Fernzugriff auf den TOE kann nur nach erfolgreicher Authentisierung durch das

NMS erfolgen. Der Zugriff von einer Rolle auf konkrete Operationen und Daten wird durch den TOE verwaltet.

2) **Verzeichnisdienst für Zertifikate (PKI):** Das System generiert Zertifikate sowie verwaltet und bestätigt Zertifikate (PKI). Hierzu gehören auch die Rücknahme und die Erneuerung von Zertifikaten.

3) **Zeitdienst:** Das Sicherheitscenter stellt einen netzbasierten Dienst zur Zeitsynchronisation der TOEs bereit.

2.2 Schnittstellen des TOE

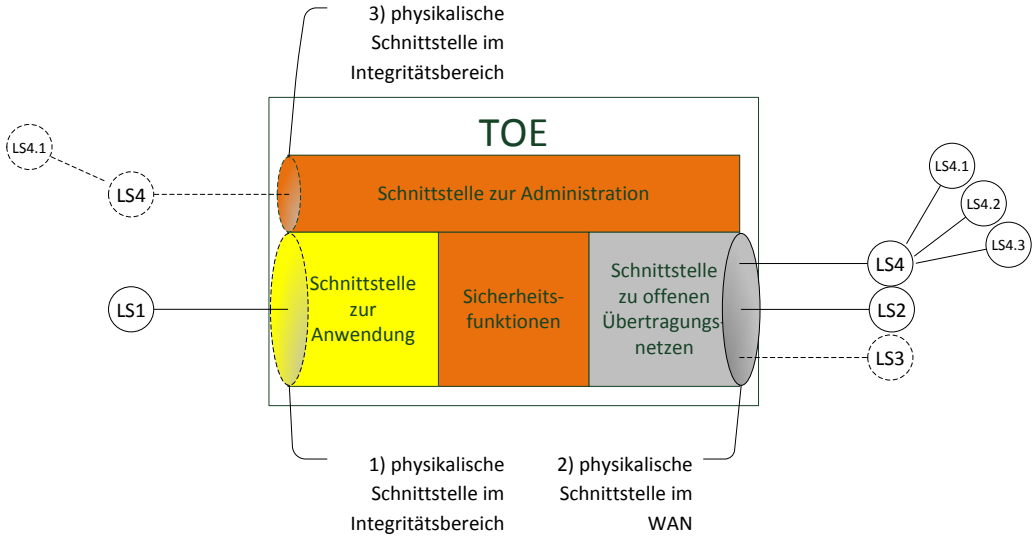

Abbildung 4: Übersicht zu den Schnittstellen des TOE

2.2.1 Physische Schnittstellen des TOEs

Application Note: Der ST-Autor muss die Beschreibung der physikalischen Schnittstellen abhängig von der konkreten Ausgestaltung der spezifischen Bauform anpassen. Es wird erwartet, dass der TOE über die im Folgenden aufgelisteten Schnittstellen verfügt. Wenn Abweichungen bestehen, so sind diese in dem Security Target zu erläutern.

Der TOE besitzt folgende (externe) physikalische Schnittstellen:

- Optional: eine physikalische Schnittstelle zur Anwendung. Diese Schnittstelle ist abhängig von der konkreten Bauform. Wenn die LST-Anwendung als Mehrkomponentenlösung realisiert wird, ist der TOE eine Teilfunktion und der Nutzdatenstrom wird nur über die logische Schnittstelle LS1 an den TOE geführt.
- Eine physikalische Schnittstelle zu offenen Übertragungsnetzen
- Optional: eine physikalische Schnittstelle zur lokalen Betriebsführung. Diese Schnittstelle ist abhängig von der konkreten Bauform. Es kann eine physische Schnittstelle für eine lokale Betriebsführung implementiert werden. Die Kommunikationsbeziehung über diese Schnittstelle ist identisch zu der logischen Schnittstelle LS4. Der Administrator greift über ein portables Netzmanagementsystem auf den TOE zu.

2.2.2 Logische Schnittstellen des TOEs

Application Note: Der ST-Autor muss die Beschreibung der logischen Schnittstellen abhängig von der konkreten Ausgestaltung der spezifischen Bauform anpassen.

Der TOE besitzt folgende (externe) logische Schnittstellen:

LS1 Eine Schnittstelle für den Nutzdatenstrom, der physisch über 1) angebunden wird.

LS2 Eine Schnittstelle als verschlüsselter Kanal (der verschlüsselte Nutzdatenstrom) mit einem vertrauenswürdigen System als Empfänger

LS3 Temporär: Eine Schnittstelle, für den Aufbau von Sicherheitsbeziehungen, die Schnittstelle wird mit dem Aufbau des verschlüsselten Kanals geschlossen.

LS4 Eine Schnittstelle als verschlüsselter Kanal zur Kommunikation mit dem Ziel Sicherheitscenter, unterteilt mit folgenden Zielen:

LS4.1 Netzmanagementsystem (NMS) zur Überwachung und Betriebsführung

LS4.2 Verzeichnisdienst für Zertifikate (PKI)

LS4.3 Zeitdienst

2.3 Aufbau und physische Abgrenzung des TOE

Der TOE kann in verschiedene Bauformen implementiert werden. In dem Referenzaufbau gemäß Lastenheft [KISA], bezeichnet als KISA-Modul, wird der TOE, als ein anwendungsspezifisch konfigurierbares System [DIN128], als Anwendung auf einem seriengefertigten Hardware- und Software-Produkt ausgeführt. Der TOE besitzt die o.g. Schnittstellen und die in dem Schutzprofil definierten Funktionen und Anforderungen. Diese minimale Bauform wird als Einboxlösung bezeichnet.

Weitere Bauformen ergeben sich als ein „kryptografisch gesichertes System des Eisenbahnbetriebs“ und „KISA-Modul 2.0“ (Arbeitstitel). Diese erweiterten Bauformen werden als Mehrkomponentenlösung bezeichnet und beinhalten den TOE als eine Teilfunktion. Ein kryptografisch gesichertes System des Eisenbahnbetriebs besteht aus dem TOE und einer LST-Anwendung.

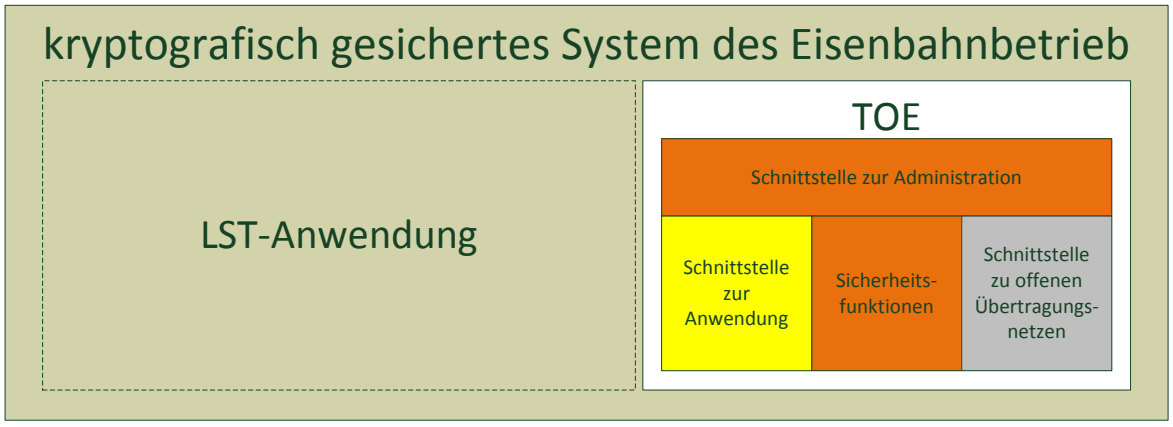

Abbildung 5: Mehrkomponentenlösung mit LST-Anwendung

Beide Anwendungen (TOE und LST-Anwendung) müssen als getrennte anwendungsspezifisch konfigurierbare Teilsysteme innerhalb einer sicherheitsrelevanten Einrichtung ausgeführt werden. Die Interaktion beider Teilsysteme erfolgt ausschließlich über die für den TOE definierten Schnittstellen. Für die Rückwirkungsfreiheit entsprechend der DIN EN 50129:2003 sind jeweils klare Aussagen (physikalische/funktionale interne und externe Einflüsse der einzelnen Teilsysteme) zu den aufgeführten Inhalten der Norm vorzulegen. Eine Bewertung dieser Aussagen, die Gegenstand des Sicherheitsnachweises bzw. einer Herstellererklärung zum Produkt bestehend aus seriengefertigter Hardware und Software sein können, erfolgt durch die Aufsichts-, Genehmigungs- und Sicherheitsbehörde und/oder der für die Produktfreigabe zuständigen Fachorganisation des Infrastrukturbetreibers. Konkrete LST-Anwendungen werden zukünftige Lastenhefte für kryptografisch gesicherte Systeme des Eisenbahnbetriebs definieren.

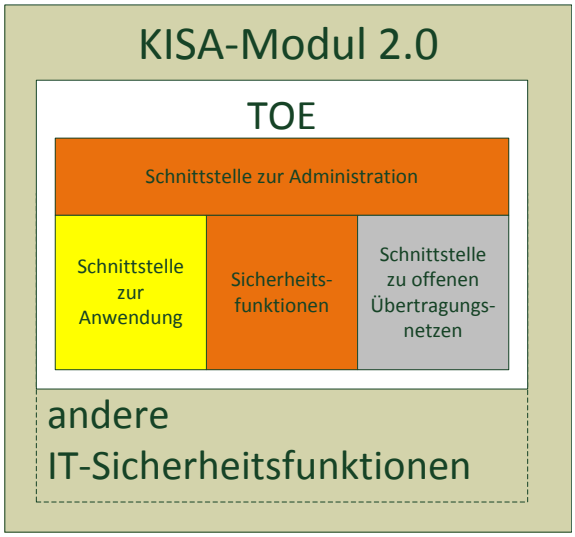

Abbildung 6: Mehrkomponentenlösung mit weiteren Sicherheitsfunktionen

Die Bauform KISA-Modul 2.0 besteht aus dem TOE und weiteren Sicherheitsfunktionen. Diese Sicherheitsfunktionen werden als separate Schutzprofile und separate TOEs festgelegt. Beide TOEs können dabei als getrennte anwendungsspezifisch konfigurierbare Systeme auf einem gemeinsamen seriengefertigten Hardware- und Software-Produkt ausgeführt werden. Die Interaktion beider Komponenten erfolgt ausschließlich über die für den TOE definierten Schnittstellen. Für die Rückwirkungsfreiheit entsprechend der DIN EN 50129:2003 sind jeweils klare Aussagen (physikalische/funktionale interne und externe Einflüsse der einzelnen Teilsysteme) zu den aufgeführten Inhalten der Norm vorzulegen. Eine Bewertung dieser Aussagen, die Gegenstand des Sicherheitsnachweises bzw. einer Herstellererklärung zum Produkt bestehend aus seriengefertigter Hardware und Software sein können, erfolgt durch die Aufsichts-, Genehmigungs- und Sicherheitsbehörde und/oder der für die Produktfreigabe zuständigen Fachorganisation des Infrastrukturbetreibers. Näheres werden zukünftige Lastenhefte für IT-Sicherheitssysteme des Eisenbahnbetriebes definieren.

2.4 Logische Abgrenzung: Vom TOE erbrachte Sicherheitsdienste

Der TOE erbringt seine Sicherheitsdienste über die in dem Lastenheft [KISA] definierten Schnittstellen weitgehend automatisch. Informationsflüsse werden grundsätzlich durch die Anwendung initiiert. Der TOE erlaubt ein **Management der Sicherheitsdienste** nach einer **Authentisierung** durch Benutzername und Passwort (oder einen gleich starken oder stärkeren Authentisierungsmechanismus) und die **Autorisierung** auf einzelne Objekte.

VPN-Client und Server (IPsec): Der TOE stellt einen **verschlüsselten Kanal** mithilfe von IPsec (Internet Protocol Security) zwischen zwei oder mehreren Standorten- gleicher Sicherheit für die Kommunikation zwischen sicherheitsrelevanten Anwendungen bereit. Für jede LST-Anwendung wird ein verschlüsselter Kanal initiiert. Der TOE prüft mittels Gültigkeit von Zertifikaten die **Authentizität** der Kommunikationspartner. Die Zertifikate werden mathematisch und gegen Sperrlisten geprüft. Für jede Sitzung wird ein Sitzungsschlüssel vereinbart. Der TOE löscht nicht mehr benötigte kryptographische Schlüssel nach ihrer Verwendung durch **aktives Überschreiben** aus seinem sicheren **Schlüsselspeicher**.

Der Nutzdatenstrom, welcher über den verschlüsselten Kanal übertragen wird, ist hinsichtlich seiner **Vertraulichkeit** und **Datenintegrität** geschützt. Zur Unterstützung des Ziels **Verfügbarkeit** wird innerhalb des TOEs wird der **Nutzdatenstrom priorisiert** weitergeleitet. Der TOE **protokolliert mit Zeitstempel und alarmiert** Ereignisse der Sicherheitsfunktionen. Zur Sicherstellung der Verfügbarkeit wird der TOE permanent überwacht und bei Beeinträchtigungen der Betriebsparameter operativ agiert. Der TOE setzt auch eine regelbasierte **Informationsflusskontrolle** um, d.h., regelbasiert müssen alle Informationsflüsse den etablierten verschlüsselten Kanal nutzen.

Paketfilter: Der TOE beschränkt den freien Zugang zum als unsicher angesehenen offenen Übertragungsnetz zum Schutz des lokalen Netz und der LST-Anwendungen. Dazu verfügt der

TOE über die Funktionalität eines Paketfilters, welcher entsprechende Regeln umsetzen kann. Er schränkt die Menge der zulässigen Quellen und Ziele, Protokolle, Datendurchsatzraten ein. **Der TOE schützt sich selbst** und das lokale Netz der LST-Anwendungen vor Angriffen aus dem offenen Übertragungsnetz und Angriffen aus dem lokalen Netz. Der TOE bietet **grundlegende Intrusion-Detektion-Funktionalität**, womit nicht wohlgeformte IP-Pakete und einfache Angriffsmuster erkannt werden können.

Systemaktualisierungen: Für eine Reaktion auf erkannte Schwachstellen in der kryptografischen Funktion, weiteren Sicherheitsfunktionen oder der Systemsoftware kann aktualisierter Programmcode eingespielt werden.

3 APE_SPD: Definition des Sicherheitsproblems

In diesem Abschnitt wird zunächst beschrieben, welche Werte der TOE schützen muss, welche externen Einheiten mit ihm interagieren und welche Objekte von Bedeutung sind. Auf dieser Basis wird danach beschrieben, welche Bedrohungen der TOE abwehren muss, welche organisatorischen Sicherheitspolitiken zu beachten sind und welche Annahmen an seine Einsatzumgebung getroffen werden können.

3.1 Zu schützende Werte

Werte sind durch Gegenmaßnahmen zu schützende Informationen oder Ressourcen. Der Schutz kann durch den TOE oder durch die Umgebung erfolgen.

Bei den zu schützenden Werten wird zwischen primären und sekundären Werten unterschieden:

Die zu schützenden primären Werte leiten sich direkt aus den Anforderungen an ein Übertragungssystem gemäß DIN EN50159:2011 sowie den allgemeinen Sachverhalten der IT-Sicherheit ab:

- Nachrichtenauthentizität
- Nachrichtenintegrität
- Rechtzeitigkeit der Nachrichten – entspricht Verfügbarkeit
- Nachrichtensequenz – entspricht Integrität
- Sicherstellung von Vertraulichkeit der sicherheitsrelevanten Information
- Verhinderung der Überlastung des Übertragungssystem – entspricht Verfügbarkeit

Die sekundären Werte sind solche Werte, die durch die Einführung des TOE erst entstehen, durch diesen bedingt werden oder von denen primäre Werte abgeleitet werden können.

3.1.1 Primäre Werte

Die primären Werte sind in der folgenden Tabelle aufgeführt.

Wert	zu schützende Eigenschaften des Wertes	Erläuterung
Nutzdatenstrom als zu schützende Daten	Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit	Austausch sicherheitsrelevanter Information der Anwendung in einer Ende-zu-Ende Beziehung zwischen zwei sicherheitsrelevanten Einrichtungen. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten unbemerkt manipulieren können. Der Absender von übertragenen Daten muss eindeutig bestimmbar sein.
LST-Anwendung	Integrität, Authentizität, Verfügbarkeit	Quelle und Ziel des Nutzdatenstromes. Die LST-Anwendung besteht aus verschiedenen Software-Komponenten die verteilt auf den Systemen der Leit- und Sicherungstechnik ausgeführt werden.
Systeme des Eisenbahnbetriebes	Integrität und Verfügbarkeit	Die Systeme des Eisenbahnbetriebes verarbeiten verschiedene Daten die für einen sicheren Eisenbahnbetrieb notwendig sind. Die Systeme des Bahnbetriebes befinden sich in demselben lokalen Integritätsbe-

		reich.
lokales Netzwerk	Integrität und Verfügbarkeit	Das lokale Netzwerk verbindet die Systeme des Bahnbetriebes innerhalb des lokalen Integritätsbereichs. Es ist ein geschlossenes Übertragungssystem.

Tabelle 1: Primäre Werte

3.1.2 Sekundäre Werte

Die sekundären Werte sind in der Tabelle aufgeführt.

Wert	zu schützende Eigenschaften des Wertes	Erläuterung
Authentisierungsgeheimnisse, Übertragung	Vertraulichkeit, Integrität und Authentizität	Die Vertraulichkeit, Integrität und Authentizität von Authentisierungsgeheimnissen bei der Übertragung zwischen TOE und dem Sicherheitscenter bzw. zwischen TOE‘s in Sicherheitsbeziehung sind zu schützen. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten unbemerkt manipulieren können. Der Absender und der Empfänger von übertragenen Daten müssen eindeutig bestimmbar sein.
Authentisierungsgeheimnisse, Speicherung im TOE	Vertraulichkeit und Integrität	Die Vertraulichkeit von Authentisierungsgeheimnissen
kryptographisches Schlüsselmaterial, Übertragung	Vertraulichkeit, Integrität und Authentizität	Gelingt es einem Angreifer, Kenntnis von Schlüsselmaterial zu erlangen oder dieses zu manipulieren, so ist nicht mehr sichergestellt, dass der TOE seine Sicherheitsleistungen korrekt erbringt. Werden Sitzungsschlüssel ausgetauscht, so ist vorher die Authentizität des Kommunikationspartners sicherzustellen.
kryptographisches Schlüsselmaterial, Speicherung im TOE als Geheimnis	Vertraulichkeit und Integrität	Gelingt es einem Angreifer, Kenntnis von Schlüsselmaterial zu erlangen oder dieses zu manipulieren, so ist nicht mehr sichergestellt, dass der TOE seine Sicherheitsleistungen korrekt erbringt.
Nutzdatenstrom Weiterleitung im TOE	Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit	Auch während der Weiterleitung durch den TOE müssen die Werte des Nutzdatenstrom geschützt werden
TOE (Hardware, Software, Konfiguration)	Integrität	Gelingt es einem Angreifer, die Integrität des TOE zu verletzen, so ist nicht mehr sichergestellt, dass der TOE seine Sicherheitsleistungen korrekt erbringt. Es ist zu befürchten, dass dann zu schützende Daten unbefugt zur Kenntnis genommen oder unbemerkt manipuliert werden können.
TOE-Systemaktualisierung	Integrität und Authentizität	Falls der TOE ein sicheres Update unterstützt, muss er Integrität und

		Authentizität der Software vor ihrer Aktivierung überprüfen. Andernfalls ist nicht mehr sichergestellt, dass der TOE seine Sicherheitsleistungen korrekt erbringt.
Protokolldaten, Übertragung	Vertraulichkeit, Integrität und Authentizität	Der TOE muss Protokolldaten bzw. daraus generierte Alarmmeldungen aller Funktionseinheiten des TOE an einen Empfänger (KSC:NMS) übertragen.
Protokolldaten, Speicherung im TOE	Integrität und Verfügbarkeit	Der TOE muss Protokolldaten erfassen, anhand derer Status und Veränderungen aller Funktionseinheiten des TOE bzw. Veränderungen an der Konfiguration des TOE nachvollzogen werden können. Diese Daten dürfen nicht modifiziert oder unautorisiert gelöscht werden.
Managementdaten, Übertragung	Vertraulichkeit, Integrität und Authentizität	Wenn der TOE administriert wird, dürfen die Managementdaten nicht eingesehen oder unbemerkt verändert werden können.
Managementdaten, Speicherung im TOE	Integrität und Verfügbarkeit	Konfigurationsdaten und Sicherheitsattribute des TOE dürfen nur von autorisierten Personen verändert werden. Für die korrekte Funktion müssen die Daten immer verfügbar sein.
Systeme im Sicherheitscenter	Integrität	Bei diesen Aspekten handelt es sich um Bedrohungen der Systeme im Sicherheitscenter und nicht um Bedrohungen des TOE. Das KISA-Modul (TOE) kann nicht für die Integrität der Systeme im Sicherheitscenter garantieren; daher wird die Integrität der Systeme im Sicherheitscenter nicht als Sicherheitsziel für das TOE formuliert.
Systemzeit im TOE	Verfügbarkeit und Integrität	Der TOE muss eine gültige Systemzeit vorhalten und diese regelmäßig mit Zeitservern im Sicherheitscenter synchronisieren. Für die korrekte Funktion muss die Zeit verfügbar sein.

Tabelle 2: Sekundäre Werte

3.2 Akteure und ihr Interesse am TOE

Eine ausführliche Beschreibung der organisatorischen Vorgaben rund um den TOE ist in dem Planungshandbuch und Betriebshandbuch für KISA beschrieben. Diese Anwendungsrichtlinien wurden durch das Eisenbahn-Bundesamt geprüft und zur Umsetzung freigegeben. Dies zusammenfassend wird kurz der Lebenszyklus des TOE beschrieben.

Die konkrete Systemdefinition, eine detaillierte Spezifikation der Anwendungsbedingungen und die Systemschnittstellen des TOE werden in einem Lastenheft beschrieben, durch einen Hersteller erfüllt und zur Zulassung durch das Eisenbahn-Bundesamt gebracht. Voraussetzung für

die Zulassung sind die normativen Regelungen der DIN EN 50126:2000. Diese Anforderungen stehen außerhalb des Schutzprofils und müssen durch die Besonderheiten der Einsatzumgebung erfüllt werden. Der dokumentierte Systemlebenszyklus und die Zulassung ist Voraussetzung für die Freigabe und den betrieblichen Einsatz.

Für die Planung, Konfiguration und Inbetriebnahme wurde durch den Infrastrukturbetreiber, dem Betreiber der KISA-Architektur und Anwender des TOE, den regulatorischen Vorgaben des Eisenbahn-Bundesamts folgend, ein verbindliches Regelwerk (Planungshandbuch) erstellt. Der Planungsablauf umfasst Festlegungen für die betroffenen Komponenten, deren Schnittstellen und Anbindung zu der LST-Anwendung sowie die versorgungstechnische und räumliche Planung. Abschluss bildet eine unabhängige Planprüfung, die als Ergebnis verifizierte Planungsdaten für die Schnittstellen und Funktionen des TOE enthält.

Die Beschaffung und Inbetriebnahme erfolgt durch die Rolle des KISA-Administrators. Vordem Einbringen der Konfiguration wird geprüft, ob die Lieferkette kompromittiert wurde und die Hardwareplattform und die Systemsoftware für die LST-Anwendung zugelassen und freigegeben wurde. Die initiale Konfiguration der Systemfunktionen und der Schnittstellenkonfiguration wird durch die Rolle des Administrators auf Basis der Planungsdaten in der Umgebung des KISA-Sicherheitscenters eingebracht. Die Sicherheitsfunktionen mit den kryptografischen Parametern werden im Vier-Augen-Prinzip durch die Rolle des KISA-Administrators und des KISA-Supervisors eingebracht.

Die Hardware wird durch Personen des TK- oder LST-Vor-Ort-Service an den Zielstandort verbracht (Integritätsbereich), eingebaut sowie an das Netzwerk und die Versorgungseinrichtungen angeschlossen. Nach dem Herstellen der Funktion erfolgt eine abschließende Funktionsprüfung durch eine unabhängige Abnahmeprüfung. Mit der Inbetriebnahme erfolgt eine ständige Überwachung und Protokollierung der Sicherheitsfunktion aus dem Sicherheitscenter heraus.

Für den Betrieb, die Wartung und Instandsetzung sowie Außerbetriebnahme wurde durch den Infrastrukturbetreiber, dem Betreiber der KISA-Architektur und Anwender des TOE, den regulatorischen Vorgaben des Eisenbahn-Bundesamts folgend, ein verbindliches Regelwerk (Betriebshandbuch) erstellt.

Die permanente Statusüberwachung (24/7 Stunden) und Erstreaktion im Ereignisfall, sowohl Sicherheitsereignisse als auch Betriebsereignisse, wird durch KISA-Operatoren sichergestellt. Sie haben minimale Berechtigungen, um im Rahmen der Erstreaktion per Fernzugriff eine qualifizierende Einschätzung des Ereignisses abzugeben und vordefinierte operative Aktionen auszuführen. KISA-Administratoren werden zu der Ereignisbearbeitung per Fernzugriff hinzugezogen, wenn die vordefinierten Aktionen zu keiner Lösung des Ereignisses führen oder eine weitergehende Ereignisqualifizierung notwendig ist. Der Austausch der Hardware im Störungsfall wird durch TK- oder LST-Vor-Ort-Service durchgeführt.

Die Wartung und Instandhaltung erfolgt durch KISA-Administratoren per Fernzugriff. Instandhaltungsaufgaben vor Ort, ohne Zugriff auf die Funktionen des TOEs, werden durch Personen des TK- oder LST-Vor-Ort-Service durchgeführt.

Die Außerbetriebnahme erfolgt durch Personen des TK- oder LST-Vor-Ort-Service, die die betroffene Hardware-Komponente ausbauen und in das KISA-Sicherheitscenter verbringen. Dort erfolgt durch die Rolle des KISA-Administrators und des KISA-Supervisors die Löschung der Sicherheitsfunktionen und der gespeicherten Daten.

3.3 Externe Einheiten

In der Einsatzumgebung des TOEs, dem Integritätsbereich, gibt es folgende externe Einheiten:

KISA-Architektur	Kommunikationspartner des TOE, zwischen denen eine logische Sicherheitsbeziehung aufgebaut wird
Redundanter TOE	Lokaler Kommunikationspartner des TOE
LST-Anwendung	Quelle und Ziel des Nutzdatenstromes
Lokales Netzwerk	Geschlossenes Übertragungsnetzwerk im

	Integritätsbereich
TK-Infrastruktur	Offenes Übertragungsnetz, Weitverkehrsnetz
KISA-Sicherheitscenter	Gesicherte Umgebung mit den Diensten PKI, Zeit, Überwachung und Betriebsführung.
KISA-Supervisor	Diese Rolle besitzt Zugang auf alle Funktionseinheiten des TOE. Mit Zugriff auf die kryptografischen Funktionen und der Berechtigung, neue Gerätezertifikate für die Herstellung der Funktion einzurichten.
KISA-Administrator	Diese Rolle besitzt Zugang auf alle Funktionseinheiten des TOE mit der eingeschränkten Berechtigung für die Aufgaben der Konfiguration der Funktionseinheiten: Schnittstelle zur Anwendung und Schnittstelle zu offenen Übertragungsnetzen
KISA-Operator	Diese Rolle besitzt Zugang auf die Funktionseinheit der Betriebsführung mit der einschränkenden Berechtigung des ausschließlich lesenden Zugriffs auf die Betriebsdaten des TOE
LST-Vor-Ort-Service	Diese Rolle besitzt Zutritt und Zugang in den Integritätsbereich des TOE. Es bestehen keine Berechtigungen für einen Zugriff auf die Daten des TOE.
TK-Vor-Ort-Service	Personen sind durch eine Zusatzausbildung berechtigt Zugang zu sicherheitsrelevanten Einrichtungen zu erhalten. Diese Rolle besitzt Zutritt und Zugang in den Integritätsbereich des TOE. Es bestehen keine Berechtigungen für einen Zugriff auf die Summe aller Daten des TOE.
Angreifer	Diese Rolle führt eine unerwünschte oder unberechtigte Handlung aus. Der Angreifer verfügt über Angriffspotential „High“ (siehe CEM, Anhang B.4 "Calculating attack potential").

Tabelle 3: Darstellung der externen Einheiten

3.4 Bedrohungen

3.4.1 Auswahl der betrachteten Bedrohungen

Der TOE muss solche Bedrohungen abwehren, die durch die Einführung der KISA-Architektur entstanden sind. Der Integritätsbereich, als Einsatzumgebung des TOE, schützt sich selbst gegen bestehende Bedrohungen. Für den Integritätsbereich, existieren organisatorische Sicherheitsrichtlinien dessen Durchsetzung als Annahme vorausgesetzt wird.

Den dargestellten Bedrohungen wird entweder durch den TOE, mit Maßnahmen in der Einsatzumgebung oder einer Kombination aus beidem entgegengewirkt. Angriffen, denen komplett durch Maßnahmen in der Umgebung entgegengewirkt wird, werden direkt auf die entsprechenden Annahmen abgebildet. Lediglich Angriffe, denen der TOE vollständig oder teilweise entgegenwirkt, werden in Abschnitt 3.4.2 auf Bedrohungen („threats“) abgebildet.

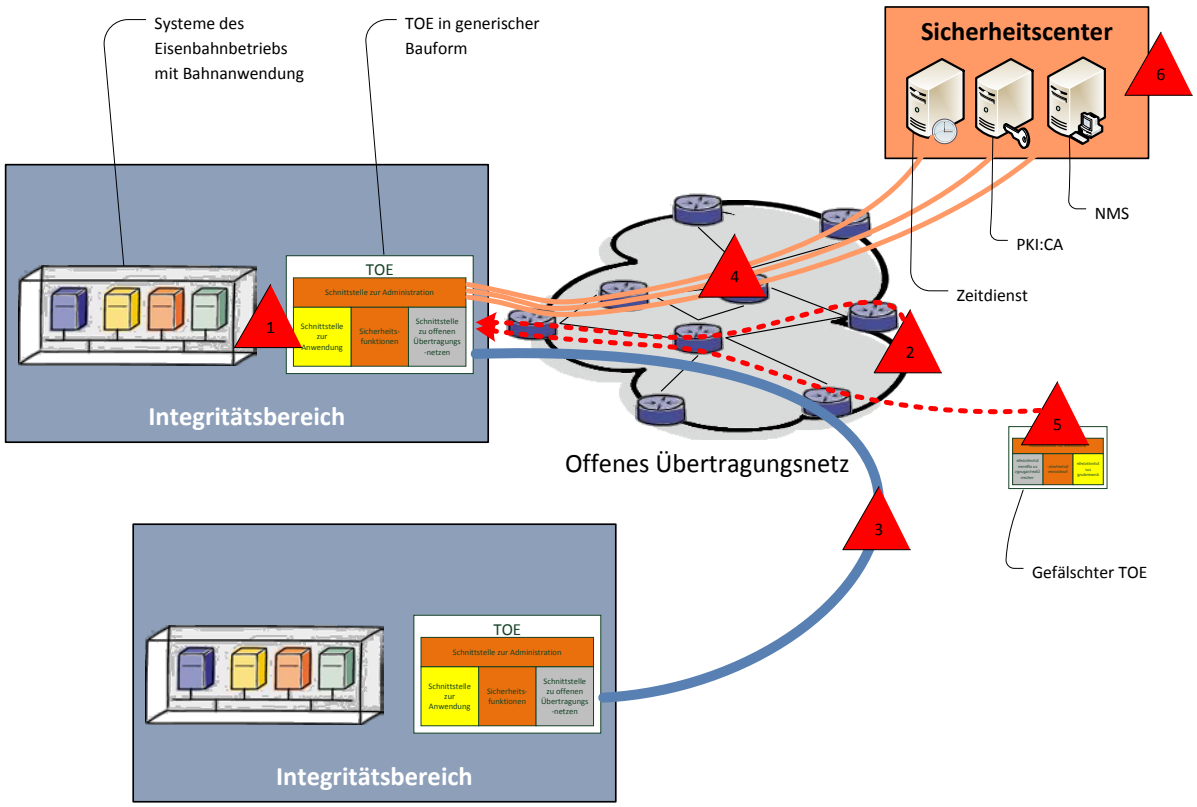

Abbildung 7: Bedrohungen gegen den TOE

Es wurden verschiedene Bedrohungsszenarien identifiziert, diese sind in der Abbildung 7 dargestellt. Die rot-eingefärbten nummerierten Dreiecke sind Ausgangspunkte für Bedrohungen gegen den TOE.

1) Der Aufstellbereich des TOE ist ein Integritätsbereich für Systeme des Bahnbetriebes. Dieser kann durch äußere und innere Umwelteinflüsse, Störungen in den Versorgungseinrichtungen und Totalverlust/Zerstörung eine Bedrohung für den TOE darstellen. Diese Bedrohungen können nur durch organisatorische Sicherheitspolitiken gemindert werden. Angriffe aus dem Integritätsbereich werden hier nicht betrachtet und müssen durch die Umgebung vollständig abgewehrt werden.

2) Der TOE stellt eine Verbindung zu einem offenen Übertragungssystem her. Das offene Übertragungssystem hat keinerlei bekannte Sicherheitsfunktionen und besitzt als Weitverkehrsnetz (WAN) eine Vielzahl unbekannter Bedrohungen und ein hohes Bedrohungspotential gegen den TOE. Der TOE mindert das Risiko von Bedrohungen, die als aktive Angriffe gegen den TOE und die primären Werte geführt werden.

3) Der sichere Kanal, sowohl während der Initialisierung als auch während der kryptografisch gesicherten Sitzung, wird über ein offenes Übertragungssystem geführt und ist dem sich daraus ergebenden Bedrohungspotential ausgesetzt. Der TOE mindert das Risiko von erfolgreichen Angriffen durch eine stetig aktuell-sichere Authentisierung und Verschlüsselung. Das eingesetzte Sicherheitsprotokoll (gemäß Lastenheft [KISA] IPsec) erkennt fehlende oder eingespielte Datenpakete.

4) Die Kommunikation mit dem Sicherheitscenter erfolgt über ein offenes Übertragungssystem und ist dem sich daraus ergebenden Bedrohungspotential ausgesetzt. Der TOE mindert Risiko von erfolgreichen Angriffen durch eine stetig aktuell-sichere Authentisierung und Verschlüsselung. Das eingesetzte Sicherheitsprotokoll (gemäß Lastenheft [KISA] IPsec) erkennt fehlende oder eingespielte Datenpakete.

5) Bedrohungen gehen auch von nicht autorisierten TOEs aus. Diese können autorisierten TOEs eine falsche Vertrauensbasis suggerieren, so dass ein verschlüsselter Kanal aufgebaut wird und Nutzdaten oder Managementdaten zu dem nicht autorisierten TOE übertragen werden.

6) Bedrohungen auf die Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit des KISA-Sicherheitscenters gefährden den Vertrauensanker der TOEs für die Authentisierung von vertrauenswürdigen Systemen sowie die Sicherheitsüberwachung der TOEs. Der TOE hat nur die Möglichkeit, auf Grundlage des Authentisierungsgeheimnisses die korrekte Identität des Sicherheitscenters zu prüfen.

3.4.2 Liste der Bedrohungen

3.4.2.1 T.counterfeit

Manipulierte TOE

Ein Angreifer bringt gefälschte TOE in Umlauf. Der Angriff kann durch den unbemerkten Austausch eines bereits im Einsatz befindlichen Geräts erfolgen – wozu in der Regel ein Eindringen in den Integritätsbereich erforderlich ist – oder bei der Erstauslieferung durchgeführt werden. Der Angreifer verfügt über hohes Angriffspotential. Ziel bzw. Motivation des Angriffs ist es, mit einem entfernten TOE eine Kommunikationsbeziehung aufzubauen und diesen im nächsten Schritt zu kompromittieren, um

- im TOE gespeicherte Geheimnisse und kryptographisches Schlüsselmaterial in Erfahrung zu bringen
- den TOE und dessen sicheren Kanal für einen Zugang auf entfernte vertrauenswürdige Systeme zu nutzen
- durch manipulierte Aufrufe den TOE in einen unsicheren Systemzustand bringt (u.a. DoS-Angriffe)
- den TOE und dessen Sicherheitsfunktionen zu manipulieren, um Angriffe aus dem T.remote_WAN auszuführen

.

3.4.2.2 T.remote_WAN

Angriffe gegen den TOE von außen

Ein Angreifer greift den TOE aus dem öffentlichen Übertragungsnetzwerk heraus an. Der Angreifer nutzt bislang noch nicht bekannte Implementierungsfehler des TOE aus. Der Angreifer verfügt über hohes Angriffspotential. Ziel bzw. Motivation des Angriffs ist es, den TOE zu kompromittieren, um

- im TOE gespeicherte Geheimnisse und kryptographisches Schlüsselmaterial in Erfahrung zu bringen
- den TOE so zu manipulieren, dass zukünftig übertragene Daten kompromittiert werden können
- den TOE und dessen sicheren Kanal für Zugang auf entfernte vertrauenswürdige Systeme nutzt
- die Protokollierungsfunktion des TOE zu deaktivieren
- durch manipulierte Aufrufe aus dem WAN den TOE in einen unsicheren Systemzustand zu bringen (u.a. DoS-Angriffe)

3.4.2.3 T.remote_VPN

man-in-the-middle-Angriff

Ein Angreifer aus dem öffentlichen Übertragungsnetz greift Daten ab oder manipuliert Daten unbemerkt, die zwischen den TOE und entfernten vertrauenswürdigen Systemen über den sicheren Kanal übertragen werden. Der Angreifer verfügt über hohes Angriffspotential. Ziel bzw. Motivation des Angriffs ist es, den sicheren Kanal zu kompromittieren, um

- unautorisierten Zugriff auf vom TOE übertragene Daten zu erhalten

- übertragene Daten zu manipulieren, um Zugang auf die Systeme des Eisenbahnbetriebs zu erhalten
- übertragene Daten zu manipulieren, um Zugang auf den TOE zu erhalten
- durch manipulierte Datenpakete des sicheren Kanals aus dem WAN den TOE in einen unsicheren Systemzustand zu bringen (u.a. DoS-Angriffe)

3.4.2.4 T.remote_Admin

Angriff mit gebrochenen Sicherheitsfunktionen

Ein Angreifer aus dem öffentlichen Übertragungsnetz oder dem Sicherheitscenter manipuliert sicherheitsrelevante Einstellungen des TOEs. Dies kann dem Angreifer einerseits dadurch gelingen, dass der TOE das Verändern von sicherheitsrelevanten Einstellungen nicht hinreichend schützt (im Sinne einer Zugriffskontrolle), sicherheitstechnische Funktionen umgeht oder dass sich ein Angreifer erfolgreich als zugriffsberechtigter Akteur ausgeben und mit dessen Berechtigungen agieren kann (im Sinne einer Authentisierung/Autorisierung). Der Angreifer verfügt über hohes Angriffspotential. Ziel bzw. Motivation des Angriffs ist es, den TOE zu kompromittieren, um

- im TOE gespeicherte Geheimnisse und kryptographisches Schlüsselmaterial in Erfahrung zu bringen
- den TOE so zu manipulieren, dass zukünftig übertragene Daten kompromittiert werden können
- den TOE und dessen sicheren Kanal für einen Zugang auf entfernte vertrauenswürdige Systeme zu nutzen
- durch manipulierte Funktionsaufrufe den TOE in einen unsicheren Systemzustand bringen (u.a. DoS-Angriffe)
- den TOE und dessen Sicherheitsfunktionen manipuliert, um Angriffe aus dem T.remote_WAN auszuführen
- die Protokollierungsfunktion des TOE zu deaktivieren

3.4.2.5 T.PKI

Angriff gegen das Authentisieren

Ein Angreifer manipuliert Sperrlisten, die im Rahmen der Gültigkeitsprüfung von Zertifikaten zwischen dem TOE und dem netzbasierten Verzeichnisdienst (siehe OE.PKI) ausgetauscht werden, um mit einem inzwischen gesperrten Zertifikat unautorisierten Zugriff auf vertrauenswürdige Systeme zu erhalten. Ein bereits gesperrtes Zertifikat wird dem TOE gegenüber als noch gültig ausgegeben, indem eine veraltete oder manipulierte Sperrliste verteilt wird. Dazu kann der Angreifer Nachrichten des Verzeichnisdienstes manipulieren oder sich selbst als Verzeichnisdienst ausgeben. Der Angreifer verfügt über hohes Angriffspotential.

3.4.2.6 T.TimeSync

Angriff gegen die Zeit

Ein Angreifer manipuliert Nachrichten, die im Rahmen der Zeitsynchronisation zwischen dem TOE und einem netzbasierten Dienst (OE.Time) ausgetauscht werden, um auf dem TOE die Einstellung einer falschen Echtzeit zu bewirken, oder gibt sich selbst als Zeitdienst aus. Der Angreifer verfügt über hohes Angriffspotential.

3.5 Organisatorische Sicherheitspolitiken

3.5.1 OSP.RAMS

Produktlebenszyklus

Alle eingesetzten Systeme im Eisenbahnbetrieb müssen zum Erreichen von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit durch das RAMS-Management auf Basis von Risikoanalysen und resultierenden Gefährdungsraten spezifiziert werden, so dass die Zuverlässigkeits- und Instandhaltbarkeitsanforderungen erfüllt werden. Die Ziele der Sicherheit und der Verfügbarkeit im Betrieb lassen sich nur dann verwirklichen, wenn die laufenden langfristigen Instandhaltungsarbeiten sowie das betriebliche Umfeld überwacht werden. Der RAMS-Prozess beschreibt den vollständigen Produktlebenszyklus und ist erst abgeschlossen, wenn ein Produkt außer Betrieb genommen und entsorgt worden ist.

3.5.2 OSP.ISMS

Managementsystem für Informationssicherheit

Der Infrastrukturbetreiber betreibt ein Managementsystem für Informationssicherheit. Es werden alle Überwachungsbereiche der ISO 27002:2013 kontrolliert. Es werden sich ableitende Maßnahmen umgesetzt und kontinuierlich auf ihre Wirksamkeit geprüft. Die Überwachungsbereiche werden insbesondere auf die Integritätsbereiche und die Systeme des Eisenbahnbetriebs angewandt.

3.5.3 OSP.Installation

Planung und Inbetriebnahme

Der Infrastrukturbetreiber ist von Grundsatz her verpflichtet, alle Baumaßnahmen an den Systemen des Eisenbahnbetriebes gegenüber den Aufsichts-, Genehmigungs- und Sicherheitsbehörde anzuzeigen. Alle Aspekte der Planung bis zu der Inbetriebnahme werden überwacht. Es sind für alle eingesetzten Komponenten Richtlinien definiert, mit folgenden Grundsätzen: Arbeitsgrundlage des Entwurfsverfassers bzw. Planerstellers ist eine betriebliche Aufgabenstellung bzw. Vorplanung. Bei der Erstellung von Planunterlagen sind die zugelassenen und freigegebenen Regelzeichnungen und Richtlinien zu beachten. Es dürfen nur Software und Hardware usw. vorgesehen werden, die eine Sicherheitszulassung erhalten haben. Vor einer Herstellung der Funktionsfähigkeit (HdF) ist die korrekte Planung durch eine Planprüfung zu bestätigen. Vor einer Inbetriebnahme erfolgte eine Abnahmeprüfung, die eine korrekte Funktion bestätigt.

3.5.4 OSP.Operation

sicherer Betrieb

Alle Maßnahmen an den Systemen des Eisenbahnbetriebs müssen darauf ausgerichtet sein, Sicherheit im Eisenbahnbetrieb zu gewährleisten und die Verfügbarkeit der Anlagen durch Vorsorge gegen Ausfälle zu erhalten und durch rasche Instandsetzung den Sollzustand wiederherzustellen. Dieser Grundsatz sowie die daraus resultierende Richtlinie wurden durch das Eisenbahn-Bundesamt bestätigt. Es wird der vollständige betriebliche Lebenszyklus ab den Zeitpunkt der Inbetriebnahme, Wartung und Instandsetzung bis zu den Außerbetriebnahmen beschrieben. Die aktuell gültige Richtlinie für das Montieren und Instandhalten von Anlagen wird durch den Infrastrukturbetreiber publiziert.

3.6 Annahmen

3.6.1 A.TrustedOSP

Verbindlichkeit der Sicherheitsrichtlinien

Es besteht das Vertrauen, dass die genannten organisatorischen Sicherheitspolitiken vollständig auf den Integritätsbereich als Einsatzumgebung des TOE mit den Systemen des Eisenbahnbetriebs, dem geschlossenen Übertragungsnetzwerk und der LST-Anwendung angewandt werden. Alle Bedrohungen, die gegen den Integritätsbereich und dessen Komponenten wirken können, werden durch Maßnahmen abgewehrt, die die Sicherheit im Eisenbahnbetrieb gewährleisten und die Verfügbarkeit der Anlagen aufrechterhalten.

3.6.2 A.TrustedKSC

Sicherheitscenter als Vertrauensanker

Das KISA-Sicherheitscenter mit den Diensten PKI, Zeit, Überwachung und Betriebsführung wird als vertrauenswürdig angesehen. Es ist als Kontrollbereich definiert und besitzt mindestens die gleiche Integritätsstufe wie die Einsatzumgebung des TOE.

Durch betriebliche und sicherheitstechnische Maßnahmen wird gewährleistet, dass die Bedrohung gegen den Kontrollbereich und gegen die versorgungstechnischen Einrichtungen sowie die IT-Systeme innerhalb des Kontrollbereichs abgewehrt werden.

Es wird angenommen, dass alle berechtigten Personen des Sicherheitscenters fachkundig und vertrauenswürdig sind. Die berechtigten Personen halten Authentisierungsinformationen und Token geheim bzw. geben diese nicht weiter (Passwort sowie Schlüssel-Token).

3.6.3 A.TrustedVendor

Geprüfte Systemtechnik

Es wird angenommen, dass der Lieferant und Hersteller und dessen Zulieferer vertrauenswürdig sind und die bereitgestellten Systeme gemäß dem RAMS-Management bei dem Systementwurf betrachtet wurden. Die Lieferkette zwischen Zulieferer und Hersteller sowie den Lieferanten in die Einsatzumgebung wurde durch geeignete Maßnahmen gesichert.

3.6.4 A.TrustedIB

Vertrauenswürdiger Integritätsbereich

Der Integritätsbereich stellt einen Kontrollbereich dar. Zutritt und Zugang wird nur berechtigten Personen gewährt, ebenso werden die Umweltbedingungen kontrolliert. Durch verschiedene Maßnahmen wie dem Betreiben von Gefahrenmeldeanlagen (GMA), Zutrittskontrollanlagen (ZKA), Videoüberwachungsanlagen (VÜA) und Einbruchsmeldeanlagen (EMA) werden diese Maßnahmen umgesetzt. Die dort verorteten Systeme des Eisenbahnbetriebs und die lokale geschlossene Netzwerkinfrastruktur wird als vertrauenswürdig angesehen.

4 APE_OBJ: Sicherheitsziele

In den nachfolgenden Abschnitten werden die Sicherheitsziele für den TOE und dessen Umgebung definiert.

4.1 Sicherheitsziele für den TOE

Der TOE muss die Nutzdaten (zu schützende Daten, siehe Abschnitt 3.1), die primären Werte und sich selbst schützen. Die Authentizität des Nutzdatenstromes kann der TOE nicht als Sicherheitsziel annehmen, gemäß DIN EN 50159:2011 kann dies nur durch die kommunizierenden sicherheitsrelevanten Anwendungen selbst erfolgen. Durch die bestehenden organisatorischen Sicherheitspolitiken in der Einsatzumgebung wird dies jedoch gewährleistet.

4.1.1 O.Integrity

Die Integrität des Nutzdatenstromes während der Weiterleitung durch den TOE darf nicht verändert werden. Dieses Schutzziel ergibt sich aus der DIN EN 50159:2011.

4.1.2 O.Confidentiality

Die Vertraulichkeit des Nutzdatenstromes während der Weiterleitung durch den TOE darf nichtverletzt werden. Dieses Schutzziel ergibt sich aus der DIN EN 50159:2011.

4.1.3 O.Availability

Die Verfügbarkeit im Sinne der Rechtzeitigkeit des Nutzdatenstromes während der Weiterleitung durch den TOE muss eine hohe Priorität besitzen. Dieses Schutzziel ergibt sich aus der DIN EN 50159:2011.

Application Note: Die Rechtzeitigkeit (Laufzeit eines Datenpaketes) des Nutzdatenstromes wird durch die konkrete Anwendung definiert. Die Laufzeit wird durch den gesamten Übertragungspfades negativ beeinflusst. Das Schutzziel wird neben der Priorisierung des Nutzdatenstromes auch über eine kurze Durchlaufzeit (Werte gemäß aktuellen Lastenheft) durch den TOE erreicht. Die Durchlaufzeit umfasst die Weiterleitung inklusive der Zeit für die angewendete kryptografische Funktion.

4.1.4 O.TOE_Protect

Der TOE schützt sich und seine sekundären Werte und die Sicherheitsfunktionen gegen Bedrohungen, die Integrität und Vertraulichkeit verletzen können. Der TOE beschränkt den freien Zugang zum als unsicher angesehenen offenen Übertragungsnetz zum Schutz des lokalen Netz und der LST-Anwendungen. Der TOE erkennt und verhindert manipulierte Aufrufe die einen unsicheren Systemzustand oder eine Überlastsituation provozieren können. Dazu verfügt der TOE über die Funktionalität eines Paketfilters, welcher entsprechende Regeln umsetzen kann. Er schränkt die Menge der zulässigen Quellen und Ziele, Protokolle und Datendurchsatzraten ein. Der TOE bietet grundlegende Intrusion Detektion-Funktionalität, womit nicht wohlgeformte IP-Pakete und einfache Angriffsmuster erkannt werden können.

Der TOE erkennt und verhindert unautorisierten Zugriff auf Objekte, im Besonderen auf gespeicherte Geheimnisse und kryptographische Schlüssel. Der TOE löscht nicht mehr benötigte kryptographische Schlüssel nach ihrer Verwendung durch aktives Überschreiben aus seinem sicheren Schlüsselspeicher. Der TOE erkennt unautorisierte Veränderungen an der sicherheitstechnischen Konfiguration. Unautorisierte Veränderungen stellen eine Gefährdung der Schutzziele dar.

4.1.5 O.TOE_AccessControl

Der TOE kontrolliert den Zugang den äußeren Schnittstellen. Nur authentifizierten und autorisierten Personen und Anwendungen wird Zugang gewährt. Der TOE kontrolliert den Zugriff auf Objekte und Dienste von autorisierten Personen und Anwendungen mit einer rollenbasierten Rechtevergabe.

4.1.6 O.TOE_Authenticity

Der TOE muss auf Anforderung einen Nachweis seiner Authentizität gegenüber dem Sicherheitscenter und anderen korrespondierenden TOEs ermöglichen. Diesen Nachweis erbringt der TOE durch entsprechend gesetzte Konfigurationsparameter und Zertifikate, die im Rahmen von der Herstellung der Funktion des TOE definiert werden und den TOE eindeutig identifizieren lassen.

4.1.7 O.TOE_TrustedChannel

Der TOE etabliert einen verschlüsselten Kanal mit einem vertrauenswürdigen entfernten IT-System. Der TOE erzwingt eine gegenseitige Authentifizierung. Der vertrauenswürdige Kanal ist eine kryptografisch gesicherte Verbindung. Die zugehörigen kryptographischen Parameter, Algorithmen, Schlüssel und Betriebsmodi für diese Verbindung müssen Der Kanal schützt die Vertraulichkeit und Integrität der zu übertragenen Daten.

Jeder LST-Anwendung wird ein Zielbezeichner des verschlüsselten Kanals zugeordnet. Die Weiterleitung des Nutzdatenstromes erfolgt als erzwungene Nutzung des verschlüsselten Kanals. Ohne erfolgreich etablierte Sicherheitsverbindung erfolgt keine Weiterleitung.

4.1.8 O.TOE_Repudiation

Der TOE protokolliert mit einem Zeitstempel sicherheitsrelevante Ereignisse aller Funktionseinheiten als Nachweis der korrekten Funktion. Die Protokollierung erfolgt auf dem TOE und wird zyklisch an das Sicherheitscenter für eine Auswertung über einen verschlüsselten Kanal übertragen.

4.1.9 O.TOE_Signaling

Der TOE überwacht die sicherheitsrelevanten Funktionen und generiert für definierte Ereignisse Alarmmeldungen, die über einen verschlüsselten Kanal an das Sicherheitscenter übertragen werden.

4.1.10 O.KeyManagement

Der TOE ermöglicht eine Gültigkeitsprüfung für die Zertifikate der vertrauenswürdigen entfernten IT-Systeme und des Sicherheitscenters, die zum Aufbau jedes einzelnen verschlüsselten Kanals verwendet werden. Die Zertifikate müssen mittels OCSP oder der vorliegenden CRL geprüft gegen eine zentrale PKI-Infrastruktur geprüft werden. Die Übertragung erfolgt über einen verschlüsselten Kanal.

4.1.11 O.TOE_Update

Softwareseitige Veränderungen des TOEs werden im Rahmen von Aktualisierungen (Software-Updates und Sicherheits-Patches) über den verschlüsselten Kanal übertragen.

4.1.12 O.TOE_Time

Der TOE verfügt über eine verlässliche Systemzeit, die in regelmäßigen Abständen über einen verschlüsselten Kanal mit einem vertrauenswürdigen Zeitserver synchronisiert wird (siehe OE.Time).

4.2 Sicherheitsziele für die Umgebung

Die Einsatzumgebung des TOE muss folgende Sicherheitsziele erfüllen:

4.2.1 OE.Integration

Herstellung der Funktionsfähigkeit und Inbetriebnahme

Das Auslieferungsverfahren und die Verfahren zur Herstellung der Funktion des TOEs stellen sicher, dass nur authentische und korrekt konfigurierte TOEs in Betrieb genommen werden können. Gefälschte TOEs müssen vom Sicherheitscenter und von anderen korrespondierenden TOEs sicher erkannt werden können.

4.2.2 OE.OperationalPhase

Überwachung und Betriebsführung

Die Überwachung und Betriebsführung in dem KISA-Sicherheitscenter folgt organisatorischen Regelungen des Bahnbetriebs und definierten operativen Abläufen des Informationssicherheitsmanagements. Es gibt ein abgestuftes Berechtigungskonzept für die Überwachung und Administration. Es werden regelmäßige Wartungen durchgeführt und die Maßnahmen zur Instandsetzung sind definiert. Die Außerbetriebnahme eines TOE wird durch einen verbindlichen Ablauf geregelt. Geheimnisse und Schlüsselmaterial sowie die eingebrachten Sicherheitsfunktionen des TOEs werden sicher gelöscht.

4.2.3 OE.PhysicalProtection

Schutz des Integritätsbereichs

Die Umgebung des TOE muss vor physischem Zugriff Unbefugter sowie vor Entwendung schützen. Der TOE darf nicht öffentlich zugänglich sein (z.B. Aufbewahrung in einem nicht öffentlich zugänglichen Raum). Die Umgebung muss sicherstellen, dass ein Diebstahl des TOEs und/oder Manipulationen am TOE rechtzeitig erkannt werden. Die Umweltbedingungen werden kontrolliert und vorbeugende Maßnahmen gegen Elementarschäden wurden angewandt.

4.2.4 OE.SecureKSC

Betrieb einer Public-Key-Infrastruktur und Bereitstellung der CRL

Das KISA-Sicherheitscenter wird in einer Umgebung mit gleicher oder höherer Integrität wie die zu schützenden Systemen des Eisenbahnbetriebes errichtet. Aus Gründen der Verfügbarkeit ist das KISA-Sicherheitscenter disloziert aufgebaut. Aus beiden KISA-Sicherheitscentern wird im Schichtbetrieb die KISA-Architektur überwacht und betriebsgeführt. Es stellt einen eigenständigen Kontrollbereich dar, in den nur autorisiertes Personal Zutritt haben.

Das KISA-Sicherheitscenter stellt einen vertrauenswürdigen Verzeichnisdienst für die Zertifikate bereit. Diese Public-Key-Infrastruktur besteht aus Zertifizierungsstelle (Certificate Authority, CA), die das CA-Zertifikat bereitstellt und die Signatur von Zertifikatsanträgen übernimmt. Registrierungsstelle (Registration Authority, RA) als Vergabestelle für Zertifikate, auch an untergeordnete Zertifizierungsstellen Zertifikate beantragen können. Zertifikatsperrliste (Certificate Revocation List, CRL) mit einer Liste mit Zertifikaten, die vor Ablauf der Gültigkeit zurückgezogen wurden.

Es wird ein Netzmanagementsystem zur Überwachung und Betriebsführung bereitgestellt. Der Systemverbund übernimmt die Aufgaben zur Überwachung und Analyse von Ereignissen der TOEs, stellt Funktionen zur Konfiguration und Funktionswiederherstellung der TOEs bereit, beherbergt die Rechte- und Rolle-verwaltung für die Systeme der KISA-Architektur.

Es wird ein netzweiter Echtzeitdienst bereitgestellt, der alle Uhren der KISA-Architektur auf ein gemeinsames Zeitnormal synchronisiert.

4.2.5 OE.Update

Software-Aktualisierung und Fehlerbehebung

Durch etablierte Prozesse wird dafür gesorgt, dass wenn Software-Updates und Sicherheits-Patches zu installieren sind, diese nur dann signiert und ausgeliefert werden, wenn der Code von einer dazu autorisierten Stelle geprüft wurde.

Der TOE und dessen grundlegendes Betriebssystem muss vor seiner Auslieferung (d.h. üblicherweise während der Produktion) mit einem Prüfschlüssel versehen werden, so dass zur Inbetriebnahme die Integrität und Authentizität geprüften werden kann. Das Schlüsselpaar muss von geeigneter kryptographischer Qualität sein.

4.2.6 OE.ISMS

Zentrales Informationssicherheitsmanagement des Infrastrukturbetreibers

Es sind Verfahren und Regeln innerhalb des Unternehmens für alle Organisationseinheiten und eingesetzten Technologien etabliert, die Informationssicherheit definieren, steuern und kontrollieren.

4.2.7 OE.RAMS

Einsatz von zuverlässigen und vertrauenswürdigen Komponenten

Die eingesetzten Systeme folgen einem Lebenszyklus gemäß der normativen Regelungen der DIN EN 50126:2000. Es wird für alle eingesetzten Systeme im Eisenbahnbetrieb ein prozessuales Vorgehen angewandt, das Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit für die Komponenten gewährleistet.

5 APE_REQ: Sicherheitsanforderungen

5.1 TOE-Sicherheitsanforderungen

In CC werden aktive Entitäten im TOE, die Operationen auf Objekten ausführen, als Subjekte bezeichnet. Als Objekte werden passive Entitäten bezeichnet, die Informationen beinhalten oder empfangen. Benutzer, Subjekte, Objekte, Informationen, Sitzungen oder Ressourcen können Attribute besitzen, die Informationen beinhalten, die der TOE für die korrekte Funktion benötigt. Attribute, die speziell für die Durchsetzung der IT-Sicherheitsanforderungen benötigt werden, werden als IT-Sicherheitsattribute bezeichnet.

Bei Daten wird nach CC zwischen Benutzerdaten und Funktionsdaten (TSF-Daten) unterschieden, wobei letztere für die Durchsetzung der IT-Sicherheitsanforderungen benötigt werden. Eine wichtige Rolle kommt dabei den sog. Authentikationsdaten, die zur Authentifizierung von Benutzern benötigt werden und den sog. Geheimnissen, z. B. kryptographischen Schlüsseln zu.

Die funktionalen Sicherheitsanforderungen der aus CC Teil 2 Version 3.1 R4 entnommenen Komponenten sind entsprechend den in CC Teil 1 Version 3.1 R4 definierten Anweisungen formatiert.

5.2 SFR: Funktionale TOE-Sicherheitsanforderungen

Die funktionalen Sicherheitsanforderungen nach funktionalen Gruppen gegliedert. Die funktionalen Gruppen orientieren sich an den im Abschnitt 2.4 beschriebenen Sicherheitsdiensten:

- VPN-Client/Server: gegenseitige Authentisierung, Vertraulichkeit, Datenintegrität, Informationsflusskontrolle (erzwungene VPN-Nutzung für sensitive Daten);
- Paketfilter: sowohl für WAN als auch für LAN, Separation von Anwendungen, grundlegende Intrusion Prävention;
- Netzdienste: Echtzeituhr und Zeitsynchronisation, Zertifikatsprüfung mittels Sperrlisten
- Selbstschutz: Speicheraufbereitung, Selbsttests, sicherer Schlüsselspeicher, Schutz von Geheimnissen, Ereignisprotokollierung (Sicherheits-Log, Security Log);
- Administration: Möglichkeit zur Wartung, erzwungene Authentisierung des Administrators, sicheres Software-Update.

5.2.1 Class FAU: Security Audit

5.2.1.1 FAU_ARP.1 Security alarms

Hierarchical to:	No other components.
Dependencies:	FAU_SAA.1 Potential violation analysis
FAU_ARP.1.1	The TSF shall take [assignment: *list of actions*] upon detection of a potential security violation.
Application Note:	Der Alarm muss gemäß Lastenheft [KISA] als SNMPv3 Trap-Nachricht an ein konfigurierbares Ziel gesandt werden. Die auslösenden Ereignisse (FAU_SAA.1) müssen durch den Supervisor (FMT_MSA.3) definierbar sein.

5.2.1.2 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [selection, choose one of: *minimum,*

basic, detailed, not specified] level of audit; and
c) [assignment: *other specifically defined auditable events*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

Application Note: Der ST-Autor soll die Liste der zu protokollierenden Ereignisse unter FAU_GEN.1.1 Punkt c) mit der jeweils aktuellen Version des KISA-Lastenheft [KISA] abgleichen und die funktionale Anforderung FAU_GEN.1 anpassen. Die Auswertung des Ereignisprotokolls erfolgt durch die Umgebung. Der Administrator darf die Protokolleinträge nicht löschen können (FAU_STG.1).

5.2.1.3 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Note: Der TOE muss bei Konfigurationsänderungen durch authentisierte Administratoren die Identität des ändernden Administrators in das Ereignisprotokoll aufnehmen.

5.2.1.4 FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;
b) [assignment: *any other rules*].

Application Note: Als Mindestanforderung wird das durch FAU_GEN.1 generierte Protokoll dazu verwendet, sicherheitsrelevante Ereignisse regelbasiert zu erkennen und damit grundlegende Einbruchsdetektion durchzuführen (FAU_SAA.1). Der ST-Autor soll durch die Operationen in FAU_SAA.1.2 präzisieren, welche Funktionalität genau der TOE bietet. Regelverletzungen sollen signalisiert werden.

5.2.1.5 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [selection, choose one of: *prevent, detect*] unauthorised modifications to the stored audit records in the audit trail.

Application Note: Niemand darf die durch FAU_GEN.1 erzeugten Audit-Daten verändern oder löschen – die Daten werden automatisch vom TOE selbst zyklisch überschrieben. Nur der TOE ist autorisiert, die Daten zyklisch zu überschreiben, gibt es ein Löschen von Daten – aber unautorisiertes Überschreiben soll verhindert werden.

5.2.1.6 FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *predefined limit*].

Application Note: Wenn der für die Protokolleinträge vorgesehene Speicherbereich verbraucht ist, muss der TOE alte Einträge zyklisch überschreiben. Die Größe des Speicherbereichs wird durch den Supervisor eingestellt. (FMT_MSA.3)

5.2.2 Class FCS: Cryptographic Support

5.2.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment*: cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note: Gemäß dem Systemkonzept [KISA] wird einzig IPsec verwendet. Es müssen die aktuell gültigen technischen Richtlinien des BSI für den Einsatz von IPsec angewandt werden. Die aus diesen Vorgaben einzusetzen Parameter werden durch den Supervisor bestimmt und initial konfiguriert (FMT_MSA.3).

5.2.2.2 FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*].

Application Note: Gemäß dem Systemkonzept [KISA] wird einzig IPsec verwendet. Es müssen die aktuell gültigen technischen Richtlinien des BSI für den Einsatz von IPsec gemäß angewandt werden). Die aus diesen Vor-

gaben einzusetzen Parameter werden durch den Supervisor bestimmt und initial konfiguriert (FMT_MSA.3).

5.2.2.3 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Application Note: Die Authentisierungsgeheimnisse und die kryptografischen Schlüssel werden in einem flüchtigen Speicher abgelegt. Der TOE soll kryptografische Schlüssel einer Sitzung (verschlüsselter Kanal) nach Beendigung oder Unterbrechung löschen. Der Speicherbereich soll danach überschrieben werden. Die lokale Haltedauer der Authentisierungsgeheimnisse wird durch den Supervisor bestimmt und initial konfiguriert (FMT_MSA.3).

Die Gültigkeit der Authentisierungsgeheimnisse wird durch die Speerliste des PKI-Verzeichnisdiensts bestimmt. Ungültige oder abgelaufene Authentisierungsgeheimnisse sind automatisch zu löschen.

5.2.2.4 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note: Gemäß dem Systemkonzept [KISA] wird einzig IPsec verwendet. Es müssen die aktuell gültigen technischen Richtlinien des BSI für den Einsatz von IPsec gemäß angewandt werden. Die aus diesen Vorgaben einzusetzen Parameter werden durch den Supervisor bestimmt und initial konfiguriert (FMT_MSA.3).

5.2.3 Class FDP: User Data Protection

5.2.3.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

Application Note: Abhängig von der konkreten Implementierung soll der ST-Autor beschreiben, welche Zugriffsrechte es gibt und wie diese für Objekte und Funktionen zu vergeben sind.

5.2.3.2 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1	The TSF shall enforce *the* [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].
Application Note:	Abhängig von der konkreten Implementierung soll der ST-Autor beschreiben, welche Zugriffsrechte es gibt und wie diese für Objekte und Funktionen zu vergeben sind. Die Authentisierungsgeheimnisse und die kryptografischen Schlüssel, die Protokolldaten und der Nutzdatenstrom sind explizit vor lesenden und schreibenden Zugriff von nicht-autorisierten Subjekten zu schützen.

5.2.3.3 FDP_IFC.2 Complete information flow control

Hierarchical to:	FDP_IFC.1 Subset information flow control
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.2.1	The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects and information*] and all operations that cause that information to flow to and from subjects covered by the SFP.
FDP_IFC.2.2	The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.
Application Note:	Die Paketfilter (LAN-seitig und WAN-seitig) sollen sowohl den TOE als auch die Informationsflüsse zwischen LAN und WAN bzw. zwischen WAN und LAN kontrollieren. Der TOE sendet und empfängt sicherheitsrelevante Nachrichten WAN-seitig ausschließlich über den verschlüsselten Kanal (FTP_ITC.1). Im Fall einer Modullösung kann dieser Schutz auch nur WAN-seitig implementiert werden. Der ST-Autor muss das Security Target entsprechend anpassen. Systembedingt bietet IPv4 (Internet Protocol, Version 4) nur eine Identifikation der Informationsflüsse, aber keine Authentisierung. Aus Mangel an besseren Mechanismen müssen dennoch auf dieser Basis die Entscheidungen über die Zulässigkeit von Informationsflüssen getroffen werden.

5.2.3.4 FDP_IFF.1 Simple security attributes

Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1	The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*].
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].
FDP_IFF.1.3	The TSF shall enforce the [assignment: *additional information flow control SFP rules*].
FDP_IFF.1.4	The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorise information flows*].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].
Application Note:	Der Nutzdatenstrom darf nicht unverschlüsselt über die WAN-verbindung übertragen werden. Die Quelle und das Ziel des verschlüsselten Kanals müssen eindeutig einer LAN-seitigen Schnittstelle zugeordnet sein. Es darf nur die vorher definierte maximal zulässige Datendurchsatzrate und die festgelegten Anwendungsschnittstellen übertragen werden. Die von FDP_IFF.1.2 geforderten Filterregeln (packet filtering rules) sind mit geeigneten Default-Werten vorbelegt (FMT_MSA.3) und können vom Administrator verwaltet werden (FMT_MSA.1). Die WAN-Schnittstelle kann eine zustandsgesteuerte Filterung umsetzten. Dies bedeutet in diesem Zusammenhang, dass der TOE zur Entscheidungsfindung, ob ein Informationsfluss zulässig ist oder nicht, auch den Status einer Verbindung mit in diese Entscheidung einbezieht.

5.2.3.5 FDP_ITC.1 Import of user data without security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
FDP_ITC.1.1	The TSF shall enforce the [assignment*: access control SFP(s) and/or information flow control SFP(s)*] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].
Application Note:	Für den Aufbau des verschlüsselten Kanals wird ein Schlüssel zwischen dem TOE und dem korrespondierenden TOE ausgetauscht,

was einen Schlüsselimport als häufigste Lösung die SFR FDP_ITC1 erfordert (das Zertifikat mit dem Public Key des vertrauenswürdigen Systems wird in den TOE importiert, damit der TOE das vertrauenswürdige System authentisieren kann). Der TOE darf auch selbst geeignete Schlüssel generieren. Die Schlüsselgenerierung kann sich auf einen, einige oder alle kryptographischen Algorithmen (FCS_COP.1) beziehen. Für jeden Schlüssel, den der TOE selbst generieren soll, muss der ST-Autor eine Anforderung FCS_CKM.1 (Cryptographic key generation) in das Security Target aufnehmen; bei Bedarf ist diese Funktion zu iterieren.

5.2.3.6 FDP_RIP.1 Subset residual information protection

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: [assignment: *list of objects*].

5.2.3.7 FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_UCT.1.1	The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to [selection: *transmit, receive*] user data in a manner protected from unauthorised disclosure.

5.2.3.8 FDP_UIT.1 Data exchange integrity

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
FDP_UIT.1.1	The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to [selection: *transmit, receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether [selection: *modification, deletion, insertion, replay*] has occurred.

5.2.4 Class FIA: Identification and Authentication

5.2.4.1 FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when [selection*: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].

5.2.4.2 FIA_UAU.1 Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.4.3 FIA_UID.1 Timing of identification

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before-allowing any other TSF-mediated actions on behalf of that user.

5.2.5 Class FMT: Security Management

5.2.5.1 FMT_MOF.1 Management of security functions behavior

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1	The TSF shall restrict the ability to [selection: *determine the behavior of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

5.2.5.2 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1	The TSF shall enforce the [assignment: *access control SFP(s), information flow control SFP(s*)] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

5.2.5.3 FMT_MSA.2 Secure security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for [assignment: *list of security attributes*].

5.2.5.4 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

5.2.5.5 FMT_MTD.1 Management of TSF data

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1	The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

5.2.5.6 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: *[assignment: list of management functions to be provided by the TSF]*.

5.2.5.7 FMT_SMR.2 Restrictions on security roles

Hierarchical to:	FMT_SMR.1 Security roles
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.2.1	The TSF shall maintain the roles: [assignment: *authorised identified roles*].
FMT_SMR.2.2	The TSF shall be able to associate users with roles.
FMT_SMR.2.3	The TSF shall ensure that the conditions [assignment: *conditions for the different roles*] are satisfied.

5.2.6 Class FPT: Protection of the TSF

5.2.6.1 FPT_ITI.1 Inter-TSF detection of modification

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_ITI.1.1	The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT-product within the following metric: [assignment: *a defined modification metric*].
FPT_ITI.1.2	The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [assignment: *action to be taken*] if modifications are detected.

5.2.6.2 FPT_RCV.4 Function recovery

Hierarchical to:	No other components.
Dependencies:	AGD_OPE.1 Operational user guidance
FPT_RCV.1.1	After [assignment: *list of failures/service discontinuities*] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

5.2.6.3 FPT_RPL.1 Replay detection

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_RPL.1.1	The TSF shall detect replay for the following entities: [assignment: *list of identified entities*].
FPT_RPL.1.2	The TSF shall perform [assignment: *list of specific actions*] when replay is detected.

5.2.6.4 FPT_STM.1 Reliable time stamps

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.
Refinement:	Die Echtzeituhr des TOE hält eine Freilaufgenauigkeit von [assigment: *Angabe der Freilaufgenauigkeit*] ein.
Application Note:	Der ST-Autor soll die vom TOE eingehaltene Freilaufgenauigkeit spezifizieren (z.B. in Sekunden pro Tag oder Sekunden pro Jahr). Vorgaben diesbezüglich ergeben sich aus der Lastenheft [KISA].

5.2.6.5 FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret [assignment: *list of TSF data types*] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.

5.2.6.6 FPT_TEE.1 Testing of external entities

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TEE.1.1	The TSF shall run a suite of tests [selection: *during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*] to check the fulfillment of [assignment: *list of properties of the external entities*].
FPT_TEE.1.2	If the test fails, the TSF shall [assignment: *action(s)*].
Application Notes:	Der ST-Autor muss in Abhängigkeit von den Vorgaben im Lastenheft [KISA] Testroutinen für die Übertragungsgüte des verschlüsselten Kanals über das offene Übertragungsnetz, anderen TOEs im selben Integritätsbereich und die Verfügbarkeit der Anwendung implementieren. Diese Testroutinen sind durch den Administrator konfigurierbar. Die Ergebnisse werden protokolliert und bei Überschreiten von Schwellwerten signalisiert.

5.2.6.7 FPT_TST.1 TSF testing

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions[assignment: conditions under which self test should occur]*] to demonstrate the correct operation of [selection: *[assignment: parts of TSF], the TSF*].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of [selection: *[assignment: parts of TSF data], TSF data*].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of [selection: *[assignment: parts of TSF], TSF*].
Application Note:	Der ST-Autor muss Methoden beschreiben wie während des Startvorgangs des TOEs (auch nach einem Neustart) Funktionen die Sicherheitsziele erfüllen auf korrekte Funktion getestet werden. Ausgewählte Testroutinen sollen als periodischer Selbsttest oder manuell von Operatoren während des Betriebes ausgeführt werden. Diese Testroutinen sind durch den Administrator konfigurierbar und dürfen den TOE in seiner Leistungsfähigkeit nicht beeinträchtigen.

5.2.7 Class FRU: Resource Utilisation

5.2.7.1 FRU_PRS.2 Full priority of service

Hierarchical to:	FRU_PRS.1 Limited priority of service
Dependencies:	No dependencies.
FRU_PRS.2.1	The TSF shall assign a priority to each subject in the TSF.
FRU_PRS.2.2	The TSF shall ensure that each access to all shareable resources shall be mediated on the basis of the subjects assigned priority.
Application Note:	Datenpakete des Nutzdatenstromes können durch das TOS-Feld mit einer Prioritätskennzahl markiert sein. Der TOE muss in der Lage sein, diese Prioritätskennzahl auszuwerten und nach unterschiedlichen Bedienmechanismen weiterzuleiten.

5.2.7.2 FRU_RSA.2 Minimum and maximum quotas

Hierarchical to:	FRU_RSA.1 Maximum quotas
Dependencies:	No dependencies.
FRU_RSA.2.1	The TSF shall enforce maximum quotas of the following resources *[assignment: controlled resources*] that [selection: *individual user, defined group of users, subjects*] can use [selection: *simultaneously, over a specified period of time*].
FRU_RSA.2.2	The TSF shall ensure the provision of minimum quantity of each [assignment: *controlled resource*] that is available for [selection: *an individual user, defined group of users, subjects*] to use [selection: *simultaneously, over a specified period of time*].
Application Note:	Der ST-Autor muss in Abhängigkeit von der konkreten Implementierung sinnvolle Vorgaben für die zugeteilten Ressourcen vorgeben. Die verbindliche Zuteilung wird durch den Administrator während des Konfigurationsvorgangs definiert.

5.2.8 Class FTP: Trusted path/channels

5.2.8.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to:	No other components
Dependencies:	No dependencies.
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.
FTP_ITC.1.2	The TSF shall permit the TSF and the remote trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for, [assignment: *list of functions for which a trusted channel is required (may be empty)*].
Refinement:	Der Trusted Channel muss auf Basis des **IPsec-Protokolls mit IKEv2** aufgebaut werden (siehe Lastenheft [KISA]).

5.3 SAR: Anforderungen an die Vertrauenswürdigkeit des TOE

Die Anforderungen an die Vertrauenswürdigkeit des TOE sind primär durch die spezielle Einsatzumgebung definiert. Für die Evaluierung des ST hinsichtlich Schwachstellenanalyse wird AVA_VAN.5 gefordert.

Assurance Class	Assurance components
ADV: Development	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
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	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
ASE: Security Target evaluation	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
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.5 Focused vulnerability analysis

6 Erklärungsteil (Rationale)

6.1 Erklärung der Sicherheitsziele (Security Objectives Rationale)

6.1.1 Abbildung der Bedrohungen, der Annahmen und der Sicherheitspolitiken auf Ziele

Die folgende Tabelle bildet die Bedrohungen, die Annahmen und die Sicherheitspolitiken für den TOE und die Umgebung ab.

Bedrohungen (T. …), OSPs (OSP. …), Annahmen (A. …)	**Sicherheitsziele für den TOE**												**Sicherheitsziele für die Einsatzumgebung**						
	O.Integrity	**O.Confidentiality**	**O.Availability**	**O.TOE_Protect**	**O.TOE_AccessControl**	**O.TOE_Authenticity**	**O.TOE_TrustedChannel**	**O.TOE_Repdudiation**	**O.TOE_Signaling**	**O.KeyManagement**	**O.TOE_Time**	**O.TOE_Update**	**OE.Integration**	**OE.OperationalPhase**	**OE.PhysicalProtection**	**OE.SecureKSC**	**OE.Update**	**OE.ISMS**	**OE.RAMS**
T.counterfeit				X		X		X	X	X				X	X			X	X
T.remote_WAN				X	X		X	X	X			X	X	X	X			X	
T.remote_VPN	X	X		X	X	X	X	X	X	X	X	X		X		X		X	
T.remote_Admin	X	X	X	X	X			X	X			X		X		X		X	
T.PKI							X			X						X			
T.TimeSync							X				X					X			
OSP.RAMS	X		X										X	X	X		X		X
OSP.ISMS					X		X	X	X					X	X	X		X	
OSP.Operation								X	X					X				X	X
OSP.Installation	X	X	X			X	X					X	X		X		X		X
A.TrustedOSP													X	X	X			X	X
A.TrustedKSC														X	X	X		X	
A.TrustedVendor													X				X	X	X
A.TrustedIB													X	X				X	X

Tabelle 4: Abbildung der Sicherheitsziele auf Bedrohungen, Sicherheitspolitiken, Annahmen

Ein Kreuz „X“ in einer Zelle bedeutet, dass die in der Zeile des Kreuzes stehende Bedrohung, Sicherheitspolitik oder Annahme durch das in der Spalte des Kreuzes stehende Sicherheitsziel (für den TOE oder für die Umgebung) abgewehrt bzw. abgebildet wird.

6.1.2 Abwehr der Bedrohungen durch die Sicherheitsziele

6.1.2.1 T.remote_VPN

Der TOE verschlüsselt die Daten für die Übertragung über das offene Übertragungsnetz mit einer kryptografischen Funktion. Der Angreifer kann daher ohne Kenntnis der Schlüssel die verschlüsselten Nachrichten nicht entschlüsseln (O.TrustedChannel). Durch diese Funktion wird auch die Integrität (O.Integrity), Vertraulichkeit (O.Confidentiality) des Nutzdatenstroms, und den Diensten (O.KeyManagement, O.TOE_Time) des KISA-Sicherheitscenters während der Übertragung über unsichere Umgebung durch den TOE gewährleistet.

Der TOE legt das für den verschlüsselten Kanal erforderliche Schlüsselmaterial (O.TOE_Protect) sicher ab und kontrolliert den Zugriff auf das Schlüsselmaterial. Mit der im Sicherheitsprotokoll (IPsec) integrierten Funktion der Authentisierung des Kommunikationspartners wird die Vertrauenswürdigkeit des Ziels (O.Authenticity) sichergestellt. Die Gültigkeitsprüfung erfordert das Mitwirken eines vertrauenswürdigen KISA-Sicherheitscenters mit den Diensten PKI und Zeit (OE.SecureKSC). Mit Sitzungsende des verschlüsselten Kanals wird das Schlüsselmaterial gelöscht.

Die dem TOE zugehörigen Schutzfunktionen (O.TOE_Protect, O.TOE_AccessControl) sichern durch eine Informationsflusskontrolle, dass zu schützende Daten nur über einen verschlüsselten Kanal zu einem vertrauenswürdigen System übertragen werden.

Es werden alle sicherheitsrelevanten Ereignisse protokolliert (O.TOE_Repudiation) und kritische Ereignisse erkannt und signalisiert (O.TOE_Signaling). Mit der Alarmierung und Auswertung sicher-heitsrelevanter Ereignisse werden durch die Betriebsführung (OE.OperationalPhase) gemäß den organisatorischen Richtlinien des Sicherheitsmanagements (OE.ISMS) Gegenmaßnahmen getroffen. Nach operativer Abwehr der Bedrohung und Analyse des Angriffs werden die genutzten Schwachstellen geschlossen (O.TOE-Update).

6.1.2.2 T.remote_WAN

Beschreibt einen Angriff aus dem offenen Übertragungsnetz, bei dem der TOE bzw. dessen Integrität bedroht wird. Angriffe aus dem offenen Übertragungsnetz werden durch den verschlüsselten Kanal (O.TrustedChannel) und den Paketfilter (mit grundlegender Intrusion Detektion-Funktionalität) abgewehrt. Die Inhalte, die durch den verschlüsselten Kanal übertragen werden, sind nicht bösartig (OE.Integration, OE.PhysicalProtection). Anfragen außerhalb des verschlüsselten Kanals werden durch den Paketfilter gefiltert (O.TOE_AccessControl) – der TOE schützt sich selbst mittels des WAN-seitigen Paketfilters. Der Paketfilter wird dabei unterstützt von O.TOE_Repudiation, O.TOE_Signaling, indem sicherheitsrelevante Ereignisse protokolliert und alarmiert werden, und von O.TOE_Protect, indem Selbsttests durchgeführt werden, die Veränderungen der Integrität des TOE erkennen. Mit der Alarmierung und Auswertung sicherheitsrelevanter Ereignisse werden durch die Betriebsführung (OE.OperationalPhase) gemäß den organisatorischen Richtlinien des Sicherheitsmanagements (OE.ISMS) Gegenmaßnahmen getroffen. Nach operativer Abwehr der Bedrohung und Analyse des Angriffs werden die Regelwerke des Paketfilters und Intrusion Detektion angepasst und genutzten Schwachstellen geschlossen (O.TOE-Update).

6.1.2.3 T.remote_Admin

Die administrativen Rechte für den Zugang und Zugriff auf den TOE werden durch OE.SecureKSC und durch O.TOE_AccessControl autorisiert. Wenn der Angriff über eine gebrochene Sicherheitsfunktion erfolgt, schützt der TOE sich selbst (O.TOE_Protect) durch Erkennen von Regelverstößen und bekannten einfachen Angriffsmustern sowie dem Ausführen von regelmäßigen Selbsttests. Durch diese Funktion wird auch die Integrität (O.Integrity), Vertraulichkeit (O.Confidentiality) und Verfügbarkeit (O.Availability) des Nutzdatenstroms während der Weiterleitung durch den TOE gewährleistet.

Es werden alle sicherheitsrelevanten Ereignisse protokolliert (O.TOE_Repudiation) und kritische Ereignisse erkannt und signalisiert (O.TOE_Signaling). Mit der Alarmierung und Auswertung sicherheitsrelevanter Ereignisse werden durch die Betriebsführung (OE.OperationalPhase) gemäß den organisatorischen Richtlinien des Sicherheitsmanagements (OE.ISMS) Gegenmaßnahmen getroffen. Nach operativer Abwehr der Bedrohung und Analyse des Angriffs werden die genutzten Schwachstellen geschlossen (O.TOE-Update).

6.1.2.4 T.counterfeit

Bei der Bedrohung T.counterfeit bringt ein Angreifer unbemerkt gefälschte TOEs in Umlauf. Der Lebenszyklus ALC_DEL gewährleistet ein sicheres Auslieferungsverfahren und ein sicheres Verfahren zur Inbetriebnahme. Das Auslieferungsverfahren wird durch OE.ISMS und OE.RAMS definiert, kontrolliert und gesteuert. Im laufenden Betrieb ermöglich der TOE auf Anforderung einen Nachweis seiner Authentizität (O.TOE_Authenticity, O.TOE_KeyManagement),

der durch die kryptographische Identität unterstützt wird. Der TOE nutzt Funktionen zur automatischen permanenten Überwachung entfernter korrespondierender TOEs, um dessen Verfügbarkeit zu überwachen (O.TOE_Protect), dessen kurzzeitiger Verlust einen potentiellen Angriff darstellt, der protokolliert und signalisiert (O.TOE_Repudiation, O.TOE_Signaling) wird. Der TOE wird an einem zutrittsgeschützten Ort betrieben (OE.physicalProtection), wodurch ein Entwenden erschwert wird. Der operative Betrieb (OE.OperationalPhase und OE.ISMS) unterstützen bei der Abwehr aller Angriffe, die sich gegen Schwächen in kryptographischen Algorithmen und Protokollen richten, also auch bei Schwächen, die sich auf die kryptographische Identität beziehen.

6.1.2.5 T.PKI

Bei der Bedrohung T.PKI manipuliert ein Angreifer Sperrlisten, die zum Zwecke der Gültigkeitsprüfung von Zertifikaten von einem netzbasierten Dienst verteilt werden. Dieser Angriff wird durch das Ziel O.KeyManagement mehrstufig abgewehrt. OE.SecureKSC unterstützt, indem die Gegenseite die Anfragen signiert zurücksendet. Wenn der TOE sich gegenüber dem Sicherheitscenter erfolgreich authentisiert hat, wird ein verschlüsselter Kanal (O.TrustedChannel) etabliert über den die Authentisierungsanfragen und Sperrlisten der Schlüsselverwaltung übertragen werden.

6.1.2.6 T.TimeSync

T.TimeSync beschreibt den Angriff, dass Nachrichten manipuliert werden, die im Rahmen einer Zeitsynchronisation mit dem netzbasierten Dienst ausgetauscht werden, um auf dem TOE die Einstellung einer falschen Echtzeit zu bewirken. Dieser Angriff wird durch O.TOE_Time abgewehrt, weil der TOE die Synchronisation über einen verschlüsselten Kanal (O.TrustedChannel) fordert. Die Zeit selbst wird durch die Umgebung (OE.SecureKSC) bereitgestellt, ebenso wie die Gegenseite des verschlüsselten Kanals.

6.1.3 Abbildung der Sicherheitspolitiken auf Sicherheitsziele für den TOE und die Umgebung

Die Sicherheitspolitiken sind allgemein für alle im deutschen Rechtsraum tätigen Bahnunternehmen gültig und stellen Anforderungen an den TOE und dessen Umgebung. Anderseits mindern die verbindlichen Sicherheitspolitiken die Bedrohungen gegen den TOE, die von der Umgebung und kommunizierenden vertrauenswürdigen Systemen (sicherheitsrelevante Anwendungen und Systemen des Bahnbetriebes) ausgehen.

6.1.3.1 OSP.RAMS

Alle eingesetzten Systeme im Eisenbahnbetrieb müssen zum Erreichen von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit durch das RAMS-Management (OE.RAMS) auf Basis von Risikoanalysen und resultierenden Gefährdungsraten spezifiziert werden. Diese Sicherheitspolitik wird durch die Sicherheitsziele O.Integrity und O.Availability von dem TOE mit unterstützt. Der sichere Entwurf des TOE sowie die Integration in eine sichere Umgebung (OE.Integration, OE.PhysicalProtection), den Integritätsbereich, ist ein Ziel, welches umgesetzt sein muss. Ebenso müssen die betrieblichen Aspekte (OE.OperationalPhase) wie auch die Instandhaltung (OE.Update) des TOE durch die Umgebung gewährleistet sein.

6.1.3.2 OSP.ISMS

Der Infrastrukturbetreiber betreibt ein Managementsystem für Informationssicherheit. Es werden alle Überwachungsbereiche der ISO 27002:2013 durch OE.ISMS kontrolliert. Der TOE unterstützt das ISMS durch seine Protokollierung und Alarmierung von sicherheitsrelevanten Ereignissen (O.TOE_Repudiation, O.TOE_Signaling) das Informationsmanagement operativ. Die geforderte Zugriffskontrolle, Überwachung und Betriebsführung in einer kontrollierten Umgebung wird ebenfalls durch den TOE und die Umgebung realisiert: O.TOE_TrustedChannel, O.TOE_AccessControl, OE.SecureKSC mit OE.OperationalPhase und OE.PhysicalProtect.

6.1.3.3 OSP.Installation

Es dürfen nur Software und Hardware usw. vorgesehen werden, die eine Zulassung durch die Aufsichts-, Genehmigungs- und Sicherheitsbehörde und eine Produktfreigabe der zuständigen Fachorganisation des Infrastrukturbetreibers erhalten haben. Diese Forderungen sind einerseits durch die Umgebung, vor der Betriebsphase durch OE.Integration, OE.PhysicalProtection, OE.RAMS als auch durch den TOE mit seinen Schutzzielen (O.Integrity, O.Confidentiality, O.Availability) sicherzustellen. Im laufenden Betrieb sind von dieser Vorgabe auch die Aktualisierungen von Hard- und Software betroffen die als Schutzziel an den TOE (O.TOE_Update) und die Umgebung formuliert sind (OE.Update). Vor der bahntechnischen Inbetriebnahme erfolgte eine Plan- und Abnahmeprüfung, die eine korrekte Planung und Funktion bestätigen, dazu werden die Schutzziele O.Authenticity und O.TOE_TrustedChannel geprüft und bestätigt.

6.1.3.4 OSP.Operation

Alle Maßnahmen (OE.RAMS und OE.ISMS) an den Systemen des Eisenbahnbetriebs müssen darauf ausgerichtet sein, Sicherheit im Eisenbahnbetrieb zu gewährleisten und die Verfügbarkeit der Anlagen durch Vorsorge gegen Ausfälle zu erhalten und durch rasche Instandsetzung den Sollzustand wiederherzustellen. Die Anforderungen werden durch O.TOE_Signaling und O.TOE_Repudiation erfüllt. Durch die Reaktion der Umgebung, konkret durch betriebliche Maßnahmen OE.OperationalPhase wird auch diese Sicherheitsrichtlinie durch den TOE und seine Umgebung erfüllt.

6.1.4 Abbildung der Annahmen auf Sicherheitsziele für die Umgebung

Bei den inhaltlich lediglich umformulierten Annahmen (A. ...) bzw. Umgebungszielen (OE. ...) bestehen direkte Beziehungen.

6.1.4.1 A.TrustedOSP

Die Einhaltung von organisatorischen Verfahrensweisen (OE.RAMS gemäß OSP.RAMS und OE.ISMS nach OSP.ISMS) ist die Voraussetzung für einen sicheren Aufbau (OE.Integration mit OSP.Installation) in einer kontrollierten Umgebung (OE.PhysicalProtection definiert nach OSP.ISMS) und eines sicheren Betriebs (OE.OperationalPhase nach OSP.Operation) für die Umgebung im Aufstellbereich des TOE.

6.1.4.2 A.TrustedKSC

Für den Zugriff auf den TOE ist ein sicheres KISA-Sicherheitscenter (OE.SecureKSC) notwendig. Das Erfassen von Bedrohungen, die Bewertung der Risiken und die resultierende Maßnahmen zur Gewährleistung des erforderlichen Sicherheitsniveaus werden durch OE.ISMS auf Basis von OSP.ISMS umgesetzt. Das KISA-Sicherheitscenter befindet sich in einen Kontrollbereich (OE.PhysicalProtection mit OSP.ISMS). Für die Komponenten des KISA-Sicherheitscenters sind organisatorischen Regelungen definiert. Es gibt ein abgestuftes Berechtigungskonzept für die Überwachung und Administration. Es werden regelmäßige Wartungen durchgeführt und die Maßnahmen zur Instandsetzung sind definiert (OE.OperationalPhase mit OSP.Operation).

6.1.4.3 A.TrustedVendor

Der Hersteller des Serienprodukts Hardware und Software (OE.Integration) stellt Aktualisierungen bereit (OE.Update), um neu erkannte Schwachstellen als Ergebnis von OE.ISMS zu beheben. Die Änderungen an den bestehenden Komponenten werden durch OE.RAMS gemäß OSP.RAMS bewertet, diese Forderung ergibt sich aus OSP.Installation. Der Hersteller ist in das OE.ISMS nach OSP.ISMS eingebunden.

6.1.4.4 A.TrustedIB

In dem Integritätsbereich werden nur Komponenten eingesetzt, die von einem Lebenszyklus-Management nach RAMS (OE.RAMS) betreut werden. Es findet das Informationssicherheitsmanagement (OE.ISMS) Anwendung, welches die geeigneten Maßnahmen auswählt, um Zuritt, Zugang in einen Integritätsbereich und Zugriff auf Daten und Funktionen der Anwendung zu kontrollieren und zu steuern. Alle Maßnahmen an Komponenten (OE.Integration) in dem Integritätsbereichen werden gemäß den geltenden organisatorischen Verfahrensweisen

(OSP.Installation) durchgeführt und mit Beginn der Inbetriebnahme überwacht (OE.OperationalPhase mit OSP.Operation).

6.2 Erklärung der Sicherheitsanforderungen

6.2.1 Abbildung der Anforderungen auf die Sicherheitsziele des TOEs

Die folgende Tabelle bildet die zu erbringenden Sicherheitsdienste auf die Sicherheitsziele des TOEs ab.

Sicherheitsdienste	Sicherheitsziele
Der TOE erlaubt ein Management der Sicherheitsdienste nach einer Authentisierung durch Benutzername und Passwort (oder einen gleich starken oder stärkeren Authentisierungsmechanismus) und die Autorisierung auf einzelne Objekte.	O.TOE_AccessControl O.TOE_Authenticity
Der TOE stellt einen verschlüsselten Kanal mithilfe von IPsec (Internet Protocol Security) zwischen zwei oder mehreren Integritätsbereichen gleicher Sicherheit für die Kommunikation zwischen sicherheitsrelevanten Anwendungen bereit. Für jede Anwendung wird ein verschlüsselter Kanal initiiert. Der TOE prüft mittels Gültigkeit von Zertifikaten die Authentizität der Kommunikationspartner. Die Zertifikate werden mathematisch und gegen Sperrlisten geprüft. Für jede Sitzung wird ein Sitzungsschlüssel vereinbart.	O.TOE_Authenticity O.TOE_TrustedChannel O.KeyManagement
Der Nutzdatenstrom, welcher über den gesicherten Kanal übertragen wird, ist hinsichtlich seiner Vertraulichkeit und Datenintegrität geschützt. Zur Unterstützung des Ziels Verfügbarkeit wird innerhalb des TOEs der Nutzdatenstrom priorisiert weitergeleitet.	O.Integrity O.Confidentiality O.Availability
Der TOE protokolliert, mit Zeitstempel, und alarmiert Ereignisse der Sicherheitsfunktionen. Zur Sicherstellung der Verfügbarkeit wird der TOE permanent überwacht und bei Beeinträchtigungen der Betriebsparameter operativ agiert.	O.TOE_Repdudiation O.TOE_Signaling O.TOE_Time
Für eine Reaktion auf erkannte Schwachstellen in der kryptografischen Funktion, weiteren Sicherheitsfunktionen oder der Systemsoftware kann aktualisierter Programmcode auf den TOE eingespielt werden. Der TOE schützt sich selbst und das lokale Netz der LST-Anwendung vor Angriffen aus dem offenen Übertragungsnetz und Angriffen aus dem lokalen Netz. Der TOE beschränkt den freien Zugang zum als unsicher angesehenen offenen Übertragungsnetz zum Schutz des lokalen Netzes und der LST-Anwendung.	O.TOE_Update O.TOE_Protect
Der TOE bietet grundlegende Intrusion-Detektion-Funktionalität, womit nicht wohlgeformte IP-Pakete und einfache Angriffsmuster erkannt werden können. Der TOE setzt auch eine regelbasierte Informationsflusskontrolle um, d.h., regelbasiert müssen alle Informationsflüsse den etablierten verschlüsselten Kanal nutzen. Der TOE verfügt über die Funktionalität eines Paketfilters, welcher entsprechende Regeln umsetzen kann. Er schränkt die Menge der zulässigen Quellen und Ziele, Protokolle, Datendurchsatzraten ein. Der TOE löscht nicht mehr benötigte kryptographische Schlüssel	O.TOE_AccessControl O.TOE_Protect O.TOE_TrustedChannel O.TOE_Authenticity

nach ihrer Verwendung durch aktives Überschreiben aus seinem gesicherten Schlüsselspeicher.	

Tabelle 5: Sicherheitsdienste und Sicherheitsziele

6.2.2 Abbildung der Sicherheitsfunktionen auf die Sicherheitsziele

Die folgende Tabelle bildet die ausgewählten Sicherheitsfunktionen der CC auf die Sicherheitsziele des TOE ab.

Ein Kreuz „X“ in einer Zelle bedeutet, dass die in der Zeile des Kreuzes stehende Sicherheitsfunktion durch das in der Spalte des Kreuzes stehende Sicherheitsziel abgebildet wird.

SFRs	**Sicherheitsziele für den TOE**											
	O.Integrity	**O.Confidentiality**	**O.Availability**	**O.TOE_Protect**	**O.TOE_AccessControl**	**O.TOE_Authenticity**	**O.TOE_TrustedChannel**	**O.TOE_Repdudiation**	**O.TOE_Signaling**	**O.KeyManagement**	**O.TOE_Time**	**O.TOE_Update**
FAU_ARP.1				X					X			
FAU_GEN.1								X	X			
FAU_GEN.2								X				
FAU_SAA.1									X			
FAU_STG.1								X				
FAU_STG.3								X				
FCS_CKM.1							X			X		
FCS_CKM.2						X						
FCS_CKM.4						X	X					
FCS_COP.1							X					X
FDP_ACC.1	X	X			X							
FDP_ACF.1					X							
FDP_IFC.2	X	X		X	X							
FDP_IFF.1	X	X		X	X							
FDP_ITC.1						X				X		
FDP_RIP.1						X	X			X		
FDP_UCT.1		X										
FDP_UIT.1	X											
FIA_AFL.1				X								
FIA_UAU.1					X							
FIA_UID.1					X							
FMT_MOF.1					X			X				
FMT_MSA.1					X							
FMT_MSA.2					X							
FMT_MSA.3					X	X	X	X	X			
FMT_MTD.1					X							
FMT_SMF.1					X							
FMT_SMR.2					X							
FPT_ITI.1				X								X
FPT_RCV.4				X								X
FPT_RPL.1				X								
FPT_STM.1								X		X	X	
FPT_TDC.1										X	X	

FPT_TEE.1				X								
FPT_TST.1				X								
FRU_PRS.2			X									
FRU_RSA.2			X									
FTP_ITC.1	X	X				X	X	X	X	X	X	X

Tabelle 6: Abbildung der Sicherheitsziele auf Sicherheitsfunktionen

6.2.3 Erfüllung der Sicherheitsziele durch die Anforderungen

6.2.3.1 O.Integrity

Um die Integrität des Nutzdatenstromes während der Weiterleitung innerhalb des TOE zu gewährleisten, wird FDP_UIT.1 gefordert. Mit FDP_ACC.1 soll der Zugriff, für Subjekte mit Zugang zum TOE eingeschränkt werden. Die Weiterleitung des Nutzdatenstromes innerhalb des TOE unterliegt der Informationsflusskontrolle (FDP_IFC.2 und FDP_IFF.1). Der eingehende Nutzdatenstrom des verschlüsselten Kanals (FTP_ITC.1) wird durch Prüfsummen auf seine korrekte Reihenfolge geprüft.

6.2.3.2 O.Confidentiality

Um die Vertraulichkeit des Nutzdatenstromes während der Weiterleitung durch den TOE zu gewährleisten, wird FDP_UCT.1 gefordert. Mit FDP_ACC.1 soll der Zugriff, für Subjekte mit Zugang zum TOE eingeschränkt werden. Der ausgehende Nutzdatenstrom wird durch Informationsflusskontrolle (FDP_IFC.2, FDP_IFF.1) in einen verschlüsselten Kanal (FTP_ITC.1) gezwungen.

6.2.3.3 O.Availability

Die Verfügbarkeit im Sinne der Rechtzeitigkeit des Nutzdatenstromes während der Weiterleitung durch den TOE muss eine hohe Priorität besitzen. Dieses Schutzziel wird durch FRU_PRS.2 und FRU_RSA.2 erreicht.

6.2.3.4 O.TOE_Protect

Der TOE erkennt unautorisierte Veränderungen an der sicherheitstechnischen Konfiguration (FPT_ITI.1). Unautorisierte Veränderungen stellen eine Gefährdung der Schutzziele dar.

Der TOE verfügt über die Funktionalität eines Paketfilters (FDP_IFC.2, FDP_IFF.1), um den Zugang an den Schnittstellen auf die zulässigen Quellen und Ziele, Protokolle, Datendurchsatzraten einzuschränken. Der Paketfilter schützt den TOE und die kryptografische Funktion vor manipulierten Aufrufen, die einen unsicheren Systemzustand oder eine Überlastsituation (u.a. DoS-Angriffe) provozieren könnten. Nicht wohlgeformte IP-Pakete und einfache Angriffsmuster werden durch grundlegende Intrusion Detektion-Funktionalität erkannt, protokolliert und signalisiert.

Beim Hochlauf muss mit der Funktion FPT_TST.1 ein Eigentest des gesamten Systems durchgeführt werden. Die Komponenten FIA_AFL.1 und FPT_RCV.4 stellen sicher, dass das technische System und seine Funktionen, bei Ausfällen und Unterbrechungen in einen sicheren Zustand gehen und falls möglich, wieder in einen betriebsfähigen Zustand versetzt werden. Korrespondierende entfernte TOEs werden mit der Funktion FPT_TEE.1 durch Korrelation ihrer Leistungswerte für die Verfügbarkeit überwacht. Der sichere Kanal wird durch die Funktion FPT_RPL.1, vor dem Einspielen von gefälschten Datendubletten geschützt. Abweichungen von Standardwerten in der kontrollierten Netzwerkumgebung werden protokolliert und stellen eine Gefährdung der Schutzziele dar.

Die Funktion FAU_ARP.1 generiert einen AlarmÜ wenn Hinweise auf potenzielle Sicherheitsverletzungen bestehen.

6.2.3.5 O.TOE_AccessControl

Der TOE kontrolliert den Zugang an den äußeren Schnittstellen. Nur authentifizierten und autorisierten Personen und Anwendungen wird Zugang gewährt. (FDP_ACC.1, FDP_ACF.1) Der

TOE kontrolliert (FIA_UAU.1, FIA_UID.1) die Zugriffsversuche auf Objekte und Dienste von autorisierten Personen und Anwendungen mit einer rollenbasierten Rechtevergabe.

Der TOE verbindet sicherheitsrelevante Anwendungen mit einer kryptografischen Übertragungsfunktion über offene Übertragungsnetze. Die Informationsflusskontrolle (FDP_IFC.2, FDP_IFF.1) erzwingt die Nutzung des verschlüsselten Kanals. Ohne erfolgreich etablierte Sicherheitsverbindung erfolgt keine Weiterleitung
Die Möglichkeit zur Verwaltung der Sicherheitsdienste wird durch die Funktionen der Klasse FMT bereitgestellt (FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1 und FMT_SMR.2). Es liegt ein Rollen- und Berechtigungskonzept vor, das Zugriff auf einzelne Objekte verweigert oder autorisiert. Dadurch wird auch die Verwaltung auf berechtigte Benutzer eingeschränkt.

6.2.3.6 O.TOE_Authenticity

Der TOE muss auf Anforderung einen Nachweis seiner Authentizität ermöglichen. Das Authentisierungsgeheimnis wurde initial auf den TOE eingebracht (FCS_CKM.2 mit FDP_ITC.1) und wird zyklisch aktualisiert (O.KeyManagement). Vor dem Aufbau einer Sicherheitsbeziehung zwischen einem Quell-TOE und einem Ziel-TOE wird eine zertifikatsbasierte Authentisierung und Etablierung eines verschlüsselten Kanals, durch die Protokoll-Implementierung IPsec ermöglicht (FTP_ITC.1). Nicht mehr benötigte Geheimnisse werden durch Überschreiben (FDP_RIP.1) zur Erfüllung von FCS_CKM.4 auf dem TOE gelöscht. Die auswählbaren Parameter für die Art des kryptografischen Schlüssels, der Verteilungsfunktion, Gültigkeitsdauer und Löschfunktion wird durch die Rolle des Supervisors festgelegt (FMT_MSA.3).

6.2.3.7 O.TOE_TrustedChannel

Der TOE etabliert einen verschlüsselten Kanal (FTP_ITC.1) mit einem vertrauenswürdigen entfernten IT-System. Der Kanal schützt die Vertraulichkeit und Integrität der zu übertragenen Daten durch eine kryptografische Funktion (FCS_COP.1), dessen Sitzungsschlüssel durch den TOE generiert wird (FCS_CKM.1). Nicht mehr benötigte Geheimnisse werden durch Überschreiben (FDP_RIP.1) zur Erfüllung von FCS_CKM.4 auf dem TOE gelöscht. Die auswählbaren Parameter für die Art des kryptografischen Schlüssels werden durch die Rolle des Supervisors festgelegt (FMT_MSA.3).

6.2.3.8 O.TOE_Repudiation

Der TOE protokolliert (FAU_GEN.1) mit einem Zeitstempel (FPT_STM.1) und Benutzer-ID (FAU_GEN.2), sicherheitsrelevante Ereignisse aller Funktionseinheiten als Nachweis der korrekten Funktion. Die Protokollierung erfolgt auf dem TOE, wird vor Zugriffen geschützt (FAU_STG.1) und wird zyklisch an das Sicherheitscenter (konfiguriert über FMT_MOF.1) für eine Auswertung über einen verschlüsselten Kanal (FTP_ITC.1) übertragen. Bei Überschreiten eines definierten Speicherbereichs (FMT_MSA.3) werden Protokolldaten (FAU_STG.3) gelöscht.

6.2.3.9 O.TOE_Signaling

Der TOE generiert (FAU_SAA.1) für definierte Ereignisse (konfiguriert über FMT_MSA.3) der Protokollaufzeichnungen (FAU.GEN.1); Alarmmeldungen (FAU.ARP.1) werden über einen verschlüsselten Kanal (FTP_ITC.1) an das Sicherheitscenter übertragen.

6.2.3.10 O.KeyManagement

Der TOE ermöglicht eine Gültigkeitsprüfung für die Zertifikate (FCS_CKM.1) der vertrauenswürdigen entfernten IT-Systeme und des Sicherheitscenters. Die Überprüfung ist integraler Bestandteil während des Aufbaus eines verschlüsselten Kanals (siehe FTP_ITC.1 refinement). Die Zertifikate müssen mittels OCSP (FPT_TDC.1, FDP_ITC.1) oder der vorliegenden zeitlich gültigen CRL (FPT_STM.1, FDP_RIP.1) gegen eine zentrale PKI-Infrastruktur geprüft werden. Die Übertragung erfolgt über einen verschlüsselten Kanal (FTP_ITC.1).

6.2.3.11 O.TOE_Update

Softwareseitige Veränderungen des TOEs, für eine Funktionswiederherstellung (FPT_RCV.4) durch Schwachstellenbehebung oder präventive Maßnahmen zur Stärkung der Sicherheitsfunktion (FCS_COP.1) werden im Rahmen von Aktualisierungen (diese werden durch eine Prüfsumme validiert, FPT_ITI.1) über den verschlüsselten Kanal FTP_ITC.1) übertragen.

6.2.3.12 O.TOE_Time

Der TOE verfügt über eine verlässliche Systemzeit (FPT_STM.1), die in regelmäßigen Abständen über einen verschlüsselten Kanal (FTP_ITC.1) mit einem vertrauenswürdigen Zeitserver synchronisiert (FPT_TDC.1) wird (siehe OE.Time).

6.2.4 Erfüllung der Abhängigkeiten

Die Abhängigkeiten zwischen Funktionen im Sinne der Common Criteria sind in diesem Abschnitt tabellarisch dargestellt. Die Darstellung beginnt bei der Funktion, die eine Abhängigkeit besitzt und zeigt durch Auswahl bzw. Referenzierung, wodurch die Abhängigkeit abgedeckt wird. Dadurch wird gezeigt, dass alle nach CC zu bestehenden Abhängigkeiten berücksichtigt wurden und die IT-Sicherheitsfunktionen in sich formal vollständig bzw. konsistent sind.

Funktion	Abhängigkeiten erfüllt durch
FAU_ARP.1	FAU_SAA.1
FAU_GEN.1	FAU_STM.1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1
FAU_SAA.1	FAU_GEN.1
FAU_STG.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1
FCS_CKM.1	FCS_CKM.2 für O.TOE_Authenticity FCS_COP.1 für O.TOE_TrustedChannel FCS_CKM.4
FCS_CKM.2	FCS_CKM.4, FDP_ITC.2
FCS_CKM.4	FDP_ITC.1
FCS_COP.1	FDP_ITC.1, FCS_CKM.4
FDP_ACC.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
FDP_IFC.2	FDP_IFF.1
FDP_IFF.1	FDP_IFC.2, FMT_MSA.3
FDP_ITC.1	FDP_ACC.1, FMT_MSA.3
FDP_UCT.1	FTP_ITC.1, FDP_ACC.1
FDP_UIT.1	FDP_ACC.1, FTP_ITC.1
FIA_AFL.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.2, FMT_SMT.1
FMT_MSA.1	FDP_ACC.1, FMT_SMR.2, FMT_SMT.1
FMT_MSA.2	FDP_ACC.1, FMT_SMR.2, FMT_SMT.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.2
FMT_MTD.1	FMT_SMR.2, FMT_SMF.1
FMT_SMR.2	FIA_UID.1
FPT_RCV.4	AGD_OPE.1

Tabelle 7: Erfüllung der Abhängigkeiten der SFRs

6.3 Erklärung für die gewählte EAL-Stufe

Der TOE stellt eine sichere Verbindung zwischen den Systemen des Bahnbetriebes her. Diese Verbindung wird unter Nutzung potentiell unsicherer offener Übertragungsnetze hergestellt. Der TOE soll das geschlossene Netz der Systeme für den Eisenbahnbetrieb von dem offenen Übertragungsnetz separieren. Da es sich bei den Systemen für den Eisenbahnbetrieb um kritische Infrastruktur handelt, dessen Versagen einen volkswirtschaftlichen Schaden darstellt muss davon ausgegangen werden, dass aus dem offenen Übertragungsnetz Angriffe gegen den TOE mit hohem Angriffspotential durchgeführt werden.

Damit die Evaluierung nachweisen kann, dass der TOE diese Angriffe erfolgreich abwehrt, muss eine Schwachstellenanalyse durchgeführt werden, die genau dieses hohe Angriffspotential berücksichtigt, deshalb wurde AVA_VAN.5 ausgewählt.

Um Ergebnisse zu erhalten nachdem dieses Schutzprofil für kommerziell Serienprodukte verwendet werden kann wurde EAL 4 als Qualitätsstufe gewählt, da dies der niedrigste Stand ist, dass die Voraussetzungen für den Einsatz von AVA_VAN.5 bietet.

6.4 Erfüllung der Abhängigkeiten der SARs

Die Abhängigkeiten der Sicherungsanforderungen entnommen aus EAL 4 werden automatisch erfüllt. Die Erhöhung auf AVA_VAN.5 führt keine zusätzlichen Funktionalitäten, die in EAL 4 nicht enthalten sind.