

Nachweis der Zulassung von Produkten mit Sicherheitsfunktionen nach VSA

BSI-VSA-10624

Zulassung für den Geheimhaltungsgrad:

Separation Kernel

GEHEIM

L4Re Secure Separation Kernel VS,

Version 1.0.0

Hersteller: Kernkonzept GmbH

Für das IT-Sicherheitsprodukt L4Re Secure Separation Kernel VS, Version 1.0.0 der Kernkonzept GmbH wurde initial mit Datum vom 01.01.2024 die Zulassung BSI-VSA-10624 erteilt. Die Zulassung ermöglicht die Verarbeitung und Übertragung von GEHEIM eingestuft Informationen. Zur Definition von GEHEIM siehe § 4 Abs 2 Nr. 2 SÜG (§ 2 Abs 2 Nr. 2 VSA).

L4Re Secure Separation Kernel VS, Version 1.0.0 ist mit heutigem Datum für den Schutz von NATO-Informationen bis zum Geheimhaltungsgrad NATO SECRET zugelassen.

Diese Zulassung ist befristet bis zum 31.12.2026.

Diese Zulassung gilt nur

- für die in Annex A aufgeführten oder referenzierten Konstruktionsstände.
- für VS-Produkte, die gemäß der beigefügten SecOPs installiert und betrieben werden.
- in Verbindung mit dem Annex I (NfD), welcher die Integration des Produktes beschreibt.

Das BSI übernimmt keine Gewährleistung für das IT-Sicherheitsprodukt.

Bonn, 19.03.2025

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

elektronisch gez.

Dr. Günther Welsch
Abteilungsleiter





Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

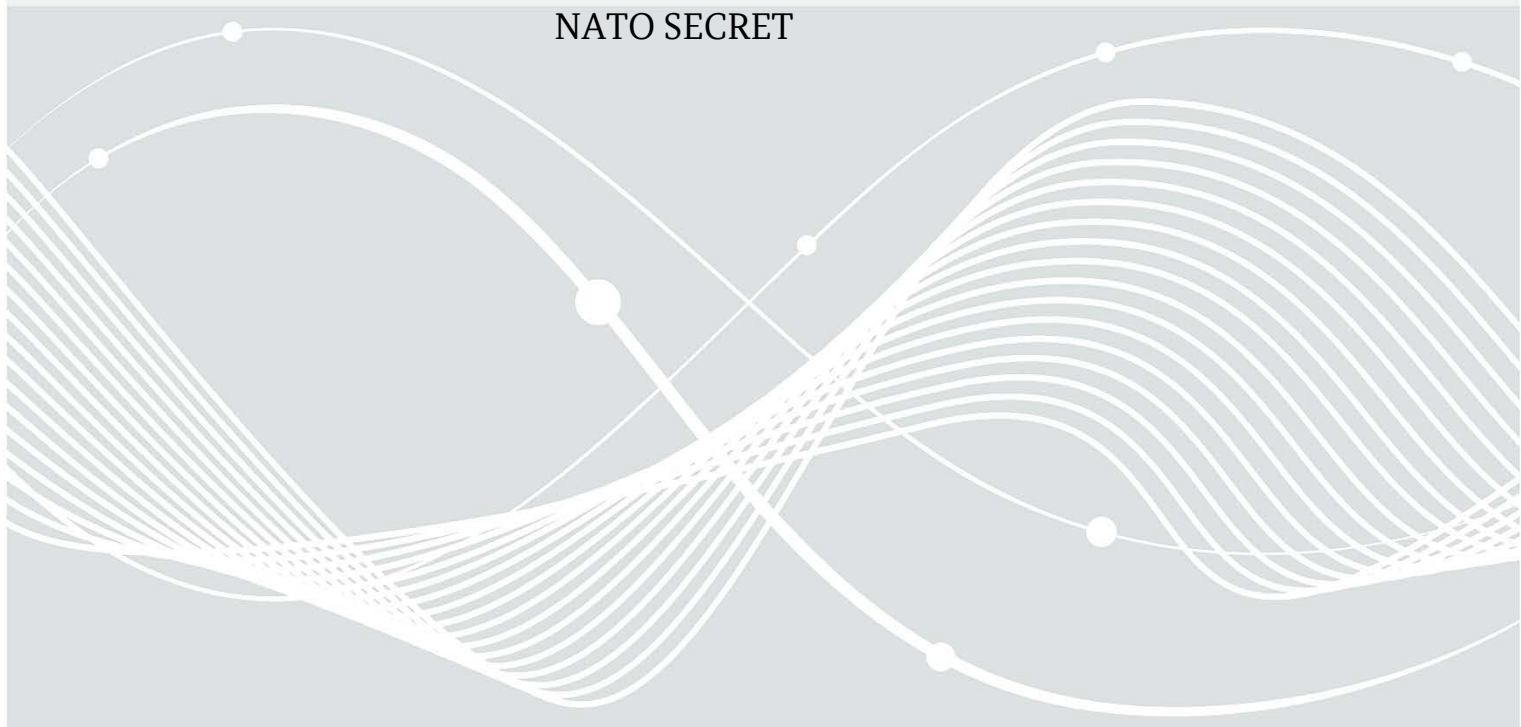
REPORT
zur Zulassung
BSI-VSA-10624

für das IT-Sicherheitsprodukt
L4Re Secure Separation Kernel VS 1.0.0

Stand: 19.03.2025

Geeignet zum Schutz von: GEHEIM

NATO SECRET



Änderungshistorie

Version	Datum	Geändert von	Bemerkungen/Gründe für Änderung
1.0	01.01.2024	BSI / V12	Ersterstellung
1.1	19.03.2025	BSI / V12	NATO-Zulassung eingearbeitet, redaktionelle Verbesserungen

Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSI-Gesetz und VSA die Aufgabe, für Zulassungsverfahren für IT-Sicherheitsprodukte (Systeme oder Komponenten) durchzuführen und Zulassungsaussagen zu erteilen. Ein IT-Sicherheitsprodukt, das über eine Zulassungsaussage des BSI verfügt, wird auch als VS-Produkt bezeichnet.

Diese Zulassungsverfahren werden auf Veranlassung eines behördlichen Antragstellers, nach einer begründeten Bedarfsmeldung und im Einvernehmen mit dem Hersteller durchgeführt.

Aus Gründen der besseren Lesbarkeit wird für die einzelnen Parteien und Instanzen auf die gleichzeitige Verwendung weiblicher, männlicher oder weiterer Sprachformen verzichtet und das generische Maskulinum verwendet. Sämtliche Personen- bzw. Rollenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Bestandteil des Verfahrens ist die technische Prüfung (Evaluierung) des IT Sicherheitsproduktes gemäß den Richtlinien des BSI.

Die Prüfung wird in der Regel vom BSI durchgeführt.

Das Ergebnis des Verfahrens ist im hier vorliegenden Report zusammengefasst. Hierin als Anhang enthalten sind die für diese Zulassung gültigen SecOPs einschließlich mindestens Annex A (Konstruktionsstände) und Annex B (Einstufungsliste) sowie evtl. weiterer Annexe.

Inhaltsverzeichnis

Änderungshistorie.....	2
Vorwort.....	3
1 Grundlagen des Zulassungsverfahrens.....	5
2 Prüfgegenstand.....	5
3 Prüfstelle	5
4 Durchführung der Evaluierung und des Zulassungsverfahrens	6
5 Konformität des TOE zu VS-AP	6
6 Ergebnis des Zulassungsverfahrens.....	6
7 Gültigkeit der Zulassungsaussage.....	6
8 Internationale Zulassungen	7
8.1 NATO	7
9 Veröffentlichung.....	7
10 Hinweise an den Hersteller	7
10.1 Änderungen am IT-Sicherheitsprodukt	7
10.2 Vertrieb.....	8
11 Literaturverzeichnis	9

1 Grundlagen des Zulassungsverfahrens

Die Zulassungsstelle führt das Verfahren nach Maßgabe der folgenden Vorgaben durch:

- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009, Bundesgesetzblatt Teil I Nr. 54, S. 2821
- Allgemeine Verwaltungsvorschrift zum materiellen Geheimsschutz (Verschlusssachenanweisung – VSA) vom 01. April 2023

2 Prüfgegenstand

Gegenstand der Zulassungsaussage ist das IT-Sicherheitsprodukt

L4Re Secure Separation Kernel VS 1.0.0

des Herstellers

**Kernkonzept GmbH
Buchenstraße 16b
01097 Dresden
Deutschland**

3 Prüfstelle

Folgende vom BSI akkreditierte Prüfstelle hat die Prüfung durchgeführt:

**SRC Security Research & Consulting GmbH
CC-Prüfstelle
Graurheindorfer Straße 149a
53117 Bonn
Deutschland**

Dabei wurden wesentliche Beiträge an die folgende Prüfstelle unterbeauftragt:

**atsec information security GmbH
CC-Prüfstelle
Ismaninger Str. 19 / 2. OG
81675 München**

Die folgende Prüfstelle hat die Unterbeauftragung veranlasst:

**SRC Security Research & Consulting GmbH
CC-Prüfstelle
Graurheindorfer Straße 149a
53117 Bonn
Deutschland**

4 Durchführung der Evaluierung und des Zulassungsverfahrens

Die Evaluierung des Evaluierungsgegenstandes im Basisverfahren wurde von der oben angegebenen Prüfstelle durchgeführt. Sie wurde am 15.11.2023 beendet. Die Evaluierung des EU-/NATO-Nachweisberichtes und die Erstellung der Dokumente für die NATO-Zulassung wurde am 28.02.2025 abgeschlossen.

Das Verfahren wurde damit beendet, dass das BSI die Übereinstimmung mit den Richtlinien überprüft und den vorliegenden Report aktualisiert hat.

5 Konformität des TOE zu VS-AP

Das VS-Anforderungsprofil Separation Kernel (SK) zum Schutz von „GEHEIM“ eingestuften Daten (BSI-VS-AP-0015-2019), Version 1.0.1, 02.09.2019 wird in dem Produkt vollständig umgesetzt.

Aus dem Anforderungsprofil werden die Szenarien Eins und Zwei abgedeckt, wenn die in den SecOPs beschriebenen Vorgaben eingehalten werden.

6 Ergebnis des Zulassungsverfahrens

Die initiale nationale Zulassung wurde mit Datum vom 01.01.2024 erteilt.

L4Re Secure Separation Kernel VS 1.0.0 ist hiermit für die Übertragung und Verarbeitung von nationalen Verschlusssachen bis einschließlich zum Geheimhaltungsgrad GEHEIM zugelassen.

7 Gültigkeit der Zulassungsaussage

Dieser Report bezieht sich nur auf die angegebene Version des VS-Produktes.

Die Zulassungsaussage gilt nur

- für die in Annex A (Konstruktionsstände) der SecOPs L4Re Secure Separation Kernel VS 1.0.0 aufgeführten oder referenzierten Konstruktionsstände,
- bei Einhaltung der SecOPs und weiteren Vorgaben zur sicheren Integration von L4Re Secure Separation Kernel VS 1.0.0 in darauf aufbauende Produkte.
Hierzu sind die SecOPs und die Benutzerdokumentation mit jedem ausgelieferten VS-Produkt dem Nutzer zur Verfügung zu stellen und ggf. beim Nutzer in vorhandene Dienstanweisungen zu integrieren. Die Überwachung der wirksamen Umsetzung der Einsatz- und Betriebsbedingungen liegt in der Verantwortung des zuständigen Geheimschutz- bzw. IT-Sicherheitsbeauftragten, des Betreibers und des Anwenders.

Es wird darauf hingewiesen, dass für den sicheren Start des Produktes gemäß [HSecBoot] in der zugelassenen Konfiguration auf kryptographische Mechanismen der Plattformen zurückgegriffen wird, die nicht Quantencomputer-resistent sind.

Hieraus ergibt sich das Risiko, dass ein Angreifer beim Vorhandensein entsprechender Quantencomputer den Sicheren Bootprozess in der aktuellen Version umgeht.

Ansonsten umfasst das Produkt keine weiteren kryptographischen Mechanismen, so dass ein Mitschneiden ausgehenden Netzwerkverkehrs zu einem entfernten Kommunikationspartner und späteres Entschlüsseln („store now – decrypt later“) keine Bedrohung darstellt.

Die Zulassung ist befristet bis zum 31.12.2026.

Die Zulassungsaussage berücksichtigt die technischen Möglichkeiten zum Zeitpunkt der Ausstellung. Angriffe, mit neuen oder weiterentwickelten Methoden, die in Zukunft möglich sind, können im Rahmen dieses Verfahrens nicht berücksichtigt werden. Die Zulassungsaussage ist nur für einen bestimmten Zeitraum gültig, um regelmäßig zu überprüfen, ob das VS-Produkt noch resistent gegen neue Angriffe ist.

8 Internationale Zulassungen

Für dieses IT-Sicherheitsprodukt liegen folgende internationale Zulassungen vor bzw. werden durch das BSI erteilt:

8.1 NATO

Sofern die vorgegebenen Einsatz- und Betriebsbedingungen eingehalten werden, kann L4Re Secure Separation Kernel VS 1.0.0, ohne weitere Einschränkung, in allen Einsatzszenarien für den Schutz von eingestuften Informationen des Geheimhaltungsgrades NATO SECRET verwendet werden.

In allen anderen nationalen Einsatzfällen sind eine Risikobewertung des Einsatzszenarios (Threat und Impact Level nach dem NATO Requirements Model) und die Einhaltung der NATO-Regularien zur Abstrahlsicherheit (d.h. geeignete Hardware, Aufstellungsort und Installation nach SDIP 27, 28 und 29) erforderlich.

Diese ist von der National Communications Security Authority (NCSA) und der zuständigen Security Accreditation Authority (SAA) zu prüfen. Ein Einsatz kann, bei Einhaltung der NATO-Anforderungen und nach positiver Prüfung, durch NCSA und SAA genehmigt werden.

Die Aufgaben einer NCSA werden in Deutschland vom BSI wahrgenommen. Diejenigen einer SAA vom BMI, wobei technische Anfragen, wie z.B. zur Prüfung und Genehmigung einer Risikobewertung, ebenfalls an das BSI zu richten sind.

9 Veröffentlichung

Das IT-Sicherheitsprodukt L4Re Secure Separation Kernel VS 1.0.0 wird in die „Liste der zugelassenen IT-Sicherheitsprodukte und -systeme“ (BSI 7164) aufgenommen; diese kann auf den Webseiten des BSI eingesehen werden.

10 Hinweise an den Hersteller

10.1 Änderungen am IT-Sicherheitsprodukt

Im Falle von Änderungen an der evaluierten Version des IT-Sicherheitsproduktes kann die Gültigkeit auf neue Versionen ausgedehnt werden, sofern für das geänderte IT-Sicherheitsprodukt ein entsprechender Antrag durch die behördlichen Bedarfsträger gestellt wird und die Evaluierung keine sicherheitstechnischen Mängel ergibt.

10.2 Vertrieb

IT-Sicherheitsprodukte und deren Komponenten unterliegen einem eingeschränkten Vertrieb.

Der Export von IT-Sicherheitsprodukten und deren Komponenten unterliegt der deutschen Exportgesetzgebung und bedarf grundsätzlich der Zustimmung der zuständigen Stellen.

11 Literaturverzeichnis

[BSI-Gesetz, 2009]

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009, Bundesgesetzblatt Teil I Nr. 54, S. 2821

[IT-Grundschutz-Kompendium Edition 2020]

Webseite des BSI (inkl. Ergänzungslieferungen),
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

[Verschlusssachenanweisung, 2023]

Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA) vom 01. April 2023

[NATO C-M (2002)49, 2002]

Security within the North Atlantic Treaty Organization vom 26. März 2002



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI

Einsatz- und Betriebsbedingungen

L4Re Secure Separation Kernel VS, Version 1.0.0

BSI-VSA-10624

Stand: 19.03.2025

Geeignet zum Schutz von: GEHEIM

Nationale Version

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: zulassung@bsi.bund.de
Internet: <https://www.bsi.bund.de>
© Bundesamt für Sicherheit in der Informationstechnik 2025

Inhaltsverzeichnis

Inhaltsverzeichnis.....	3
Annexe.....	5
VORWORT	7
1 EINLEITUNG	8
1.1 Inhalt.....	8
1.2 Verwendung.....	8
1.3 Weitergabe	8
1.4 Referenzen	8
1.5 Begriffsbestimmungen	9
1.6 Parteien und Instanzen	11
2 SYSTEMBESCHREIBUNG.....	14
2.1 Einsatzzweck.....	14
2.2 Systemkomponenten und Funktion	15
2.3 Zulassung und zugelassener Konstruktionsstand	15
2.4 Kompatibilität, Interoperabilität, Konformität.....	16
2.5 Betriebsarten.....	16
2.6 Installation, Systemintegration und Konfiguration	16
2.7 Betrieb	16
2.8 Abstrahlsicherheit	17
3 SICHERHEITSMANAGEMENT	18
3.1 Zuständigkeiten für Sicherheits-/Schlüsselmanagement	18
3.2 Beschreibung des Sicherheits-/Schlüsselmanagements	18
3.3 Quantencomputer-Resistenz	18
3.4 Nutzung veralteter Krypto-Algorithmen.....	18
4 VS-EINSTUFUNGEN.....	19
4.1 VS-Behandlungshinweise	19
5 NACHWEISFÜHRUNG UND KONTROLLE.....	20
5.1 Verkauf, Ausleihe und Export	20
5.2 Konformitätserklärung (DoC).....	20
5.3 VS-Nachweisführung und Kontrolle.....	20
6 MATERIELLE SICHERHEIT	21
6.1 Zuständigkeiten.....	21
6.2 Anforderungen an die Materielle Sicherheit.....	21
6.2.1 Allgemein	21
6.2.2 Betriebsbereites Gerät	21
6.2.3 Lagerung und Transport.....	21

6.2.4	Behandlung von Schlüsselmaterial.....	22
6.3	Geräteschutzmechanismen.....	22
6.3.1	Tamper-Schutz	22
6.3.2	Meldung und Maßnahmen	22
6.4	Routinemäßige Vernichtung.....	22
6.4.1	Vernichten/Löschen von Schlüsseln/Zertifikaten.....	22
6.4.2	Produktentsorgung und -vernichtung.....	22
7	PERSONELLE SICHERHEIT	23
7.1	Zuständigkeiten.....	23
7.2	Ermächtigung und Autorisierung.....	23
7.3	Kenntnis nur, wenn nötig (Need-To-Know)	23
8	WARTUNG UND REPARATUR	24
8.1	Zuständigkeiten.....	24
8.2	Vorgaben und Maßnahmen.....	24
9	NOTFALLPROZEDUREN.....	25
10	SICHERHEITSVORFÄLLE.....	26
10.1	Ansprechpartner des Betreibers.....	26
10.2	Meldepflicht und Zuständigkeiten.....	26
10.3	Meldepflichtige Vorfälle	26
10.4	Maßnahmen bei kommunizierten Sicherheitsinformationen	26
10.5	Maßnahmen nach entdeckter Kompromittierung.....	27
11	KONTAKTE.....	28
11.1	Hersteller	28
11.2	BSI Krypto-Support.....	28
11.3	BSI Zulassung	28

Annexe

Annex A – Zulassung und Konstruktionsstand

Annex B – Einstufungsliste

Annex C – Lagerung und Transport - entfällt

Annex D – System Integration und Konfiguration - entfällt

Annex E – Entsorgung und Vernichtung - entfällt

Annex F – Sicherheitsmanagement - entfällt

Annex G – Abstrahlsicherheit - entfällt

Annex I – ETR for Composition (EfC) (VS-NUR FÜR DEN DIENSTGEBRAUCH)

Abbildungsverzeichnis

Abbildung 1: Schematische Darstellung der Architektur von L4Re Secure Separation Kernel VS, Version 1.0.0, der Hardware-Plattform und beispielhafter User-Partitionen.14

Tabellenverzeichnis

Tabelle 1: Referenzen9

Tabelle 2: Begriffsbestimmungen11

Leere Seite

VORWORT

Die vorliegenden Einsatz- und Betriebsbedingungen, international auch als Security Operating Procedures (SecOPs) bezeichnet, für L4Re Secure Separation Kernel VS, Version 1.0.0 werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben und sind integraler Bestandteil der Zulassungsdokumentation von L4Re Secure Separation Kernel VS, Version 1.0.0.

Diese Einsatz- und Betriebsbedingungen ergänzen das Nutzerhandbuch von L4Re Secure Separation Kernel VS, Version 1.0.0 in einigen sicherheitsrelevanten Bereichen und sind gemeinsam mit diesem zu lesen und anzuwenden.

Da es sich bei L4Re Secure Separation Kernel VS, Version 1.0.0 um ein minimales Betriebssystem mit breiten Einsatzmöglichkeiten handelt, wird L4Re Secure Separation Kernel VS, Version 1.0.0 als solches im Allgemeinen nicht direkt von Endnutzern eingesetzt. Vielmehr dient L4Re Secure Separation Kernel VS, Version 1.0.0 als Grundlage für Endprodukte mit hohen Sicherheitsanforderungen. Dementsprechend richten sich diese SecOPs an Endprodukthersteller.

Die Beachtung und Umsetzung dieses Dokumentes ist verbindlich für die Verwendung von L4Re Secure Separation Kernel VS, Version 1.0.0 in einem Endprodukt. Abweichende Regelungen bedürfen der ausdrücklichen schriftlichen Genehmigung durch das BSI.

Dieses Dokument sollte allen Stellen, die IT-Systeme mit L4Re Secure Separation Kernel VS, Version 1.0.0 planen, L4Re Secure Separation Kernel VS, Version 1.0.0 konfigurieren und in ein Endprodukt integrieren, sowie den verantwortlichen IT-Sicherheitsbeauftragten, Geheimschutzbeauftragten und Sicherheitsverantwortlichen zur Verfügung gestellt werden.

Aus Gründen der besseren Lesbarkeit wird für die einzelnen Parteien und Instanzen auf die gleichzeitige Verwendung weiblicher, männlicher oder weiterer Sprachformen verzichtet und das generische Maskulinum verwendet. Sämtliche Personen- bzw. Rollenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Der zu diesem Dokument gehörige Annex I „ETR for Composition (EfC)“ wird aufgrund seiner Einstufung gesondert zur Verfügung gestellt. Er ist beim Hersteller anzufordern.

Falls erforderlich, wird das BSI Ergänzungen zu diesem Dokument herausgeben.

Eventuelle Fragen zu diesem Dokument sind an folgende Adresse zu richten:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
D-53133 Bonn
Germany

E-Mail: zulassung@bsi.bund.de

1 EINLEITUNG

1.1 Inhalt

Das vorliegende Papier beinhaltet die Einsatz- und Betriebsbedingungen für L4Re Secure Separation Kernel VS, Version 1.0.0, international auch als Security Operating Procedures (SecOPs) bezeichnet, für den Schutz von Verschlusssachen (VS) mit dem maximalen Geheimhaltungsgrad GEHEIM.

Das Dokument beschreibt die Mindestanforderungen für die sichere Installation, Integration und Konfiguration sowie für die Kontrolle, den Schutz und den Betrieb von L4Re Secure Separation Kernel VS, Version 1.0.0, zugehörigem Sicherheitsmanagement, Zubehör und produktspezifischer Dokumentation.

1.2 Verwendung

Diese Einsatz- und Betriebsbedingungen gelten für alle Anwendungen, in denen L4Re Secure Separation Kernel VS, Version 1.0.0 zum Schutz von nationaler VS zum Einsatz kommt. Sie sollten allen Personen, die für die Installation und Kontrolle sowie für die Weitergabe, Betrieb und Nutzung von L4Re Secure Separation Kernel VS, Version 1.0.0 verantwortlich sind, zur Verfügung gestellt werden. Dies umfasst ggf. auch weitere unabhängige Stellen, die für die Planung und Inbetriebnahme verantwortlich sind und das Gesamtsystem anschließend an den Betreiber übergeben (Systemintegrator).

1.3 Weitergabe

Im Falle einer Weitergabe von L4Re Secure Separation Kernel VS, Version 1.0.0 an ausländische Nationen oder nicht-deutsche Institutionen gelten besondere Bedingungen, auf die im Weiteren (Kapitel 5) noch eingegangen wird.

1.4 Referenzen

In Abhängigkeit von den Einstufungen der zu schützenden Informationen sind nachfolgend aufgeführte Referenzdokumente zu beachten.

Die nachfolgenden Referenzen beziehen sich im nationalen Kontext grundsätzlich auf die einschlägigen VS-Bestimmungen insbesondere die VSA. Entsprechende Richtlinien der einzelnen Ressorts¹ sind sinngemäß umzusetzen.

Nationale Sicherheitsvorschriften		
	[SÜG]	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz – SÜG)
	[VSA]	Verschlusssachenanweisung - Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz, vom 01.04.2023
	[BSI TL - IT 01]	Technische Leitlinie des BSI „Mitwirkungspflichten in Zulassungsverfahren“, Stand: 10.12.2021

¹ So sind z.B. im Bereich der Bundeswehr insbesondere die dort geltenden Vorschriften (z.B. ZDv A-1130/1, ZDv A-1130/2, ZDv A-1130/3, ZDv A-960/1, ZDv A-962/1) bzw. im Bereich der geheimschutzbetreuten Wirtschaft das Geheimschutzhandbuch (GHB) des BMWi zu beachten.

	[GHB]	Handbuch für den Geheimschutz in der Wirtschaft (GeheimSchutzhandbuch), 2004, Stand: 23.08.2017
TEMPEST/EMSEC		
	<u>EU</u>	
	[IASP 7]	IA Security Policy on TEMPEST (RESTREINT UE/EU RESTRICTED)
	[IASG 7-01]	IA Security Guidelines on Selection and Installation of TEMPEST Equipment (RESTREINT UE/EU RESTRICTED)
	[IASG 7-02]	IA Security Guidelines on TEMPEST Zoning Procedures (RESTREINT UE/EU RESTRICTED)
	[IASG 7-03]	IA Security Guidelines on EU TEMPEST Requirements and Evaluation Procedures (CONFIDENTIEL UE/EU CONFIDENTIAL)
	<u>NATO</u>	
	[AC/322-D(2019)0021]	INFOSEC Technical and Implementation Directive on Emission Security (NATO RESTRICTED)
	[SDIP-27]	NATO TEMPEST Requirements and Evaluation Procedures (NATO CONFIDENTIAL)
	[SDIP-28]	NATO Zoning Procedures (NATO RESTRICTED)
	[SDIP-29]	Selection and Installation of Equipment for the Processing of Classified Information (NATO RESTRICTED)
Sonstige Referenzen		
	<u>Zulassungen/Einsatzurlaubnisse</u>	
	[Zulassung-National]	Nationale Zulassung für den Schutz von GEHEIM: BSI-VSA-10624 vom 19.03.2025 inkl. Anlagen
	<u>Nutzerhandbücher</u>	
	[HConf]	L4Re Configuration Guidance
	[HSecBoot]	L4Re Secure Boot Guidance
	[HProxy]	Development Guidance for a Compartment Communication Proxy based on L4Re

Tabelle 1: Referenzen

1.5 Begriffsbestimmungen

Nachfolgend die Erläuterung einiger Begriffe, die in diesem Dokument benutzt werden:

Allgemeine Begriffe und Abkürzungen	
ATO	Approval To Operate
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAA	Crypto Approval Authority (EU-Begriff; in Deutschland das BSI)
CCI	Controlled Cryptographic Item bzw. Controlled COMSEC Item Die Festlegung für das vorliegende IT-Sicherheitsprodukt L4Re Secure

	Separation Kernel VS, Version 1.0.0 erfolgt in Annex B dieser Dokumentation.
CIS	Communications and Information Systems
COMSEC	Communications Security
DEUmilSAA	Deutsche militärische Security Accreditation Authority Beim ZCSBw angesiedelte Stelle, die für den Bereich der Bundeswehr die Aufgaben einer SAA übernimmt.
EVG	Evaluierungsgegenstand, deutsche Bezeichnung für TOE
IAA	Information Assurance Authority
IT	Informationstechnik
IT-SiBe	IT-Sicherheitsbeauftragter
Kryptomittel	Nationale Kryptomittel im Sinne § 59 [VSA] sind Produkte, Geräte und die dazugehörigen Dokumente sowie zugehörige Schlüsselmittel zur Entschlüsselung, Verschlüsselung und Übertragung von Informationen, die vom Bundesamt für Sicherheit in der Informationstechnik oder für den Geschäftsbereich des Bundesministeriums der Verteidigung vom Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr als solche festgelegt werden. Internationale Kryptomittel werden nach den einschlägigen über- oder zwischenstaatlichen Vorschriften sowie den jeweiligen nationalen Vorschriften anderer Staaten festgelegt. Die Festlegung für das vorliegende IT-Sicherheitsprodukt L4Re Secure Separation Kernel VS, Version 1.0.0 erfolgt in Annex B dieser Dokumentation.
MEP	Manipulationserkennungsplakette (Klebeetikett durch das eine Manipulation am Gerät (Gerätegehäuse) erkennbar gemacht werden kann.)
NCSA	National CIS Security Authority (in Deutschland das BSI)
SAA	Security Accreditation Authority, zu den Aufgaben siehe Kapitel 1.6 „Parteien und Instanzen“
SecOPs	Security Operating Procedures (Einsatz und Betriebsbedingungen)
SLA	Service Level Agreement
SoM	Strength of Mechanism
TA	Tempest Authority
TEMPEST	Bezeichnet sowohl die Nutzung kompromittierender Abstrahlung für Lauschangriffe sowie Maßnahmen zum Schutz gegen kompromittierende Abstrahlung
TOE	Target of Evaluation, englische Bezeichnung für EVG
VS	Verschlusssache(n)
VS-NfD	VS-NUR FÜR DEN DIENSTGEBRAUCH
VS-V	VS-VERTRAULICH
VSA	Verschlusssachenanweisung des Bundes (siehe Referenzen)

ZCSBw	Zentrum für Cyber-Sicherheit der Bundeswehr
Gerätespezifische Begriffe und Abkürzungen	
Endprodukt	Ein auf Basis von L4Re Secure Separation Kernel VS, Version 1.0.0 von einem Endprodukthersteller hergestelltes Produkt.
EPT	Extended Page Tables. Eine Erweiterung von Seitentabellen für effizientere Virtualisierung auf Prozessoren von Intel.
IOMMU	Input-output memory management unit. Speicherverwaltungseinheit zur Unterstützung virtueller Speicheradressen für Geräte mit Hauptspeicherzugriff.
VT-x	Eine Virtualisierungstechnologie auf Prozessoren von Intel.

Tabelle 2: Begriffsbestimmungen

1.6 Parteien und Instanzen

Nachfolgend aufgeführte Parteien und Instanzen² sind mit beschriebenen Aufgaben und Verantwortlichkeiten (Rollen) bei der Umsetzung der Einsatz- und Betriebsbedingungen involviert.

Sofern eine der unten beschriebenen Rollen Aufgaben aus dem Verantwortungsbereich des Geheimschutzbeauftragten übernimmt, legt dieser fest, ob hierfür ein "besonders beauftragter Mitarbeiter" nach § 8 [VSA] zu bestellen ist. Dies kann z.B. die Rolle "Administrator/Systemadministrator" betreffen.

- **Administrator/Systemadministrator** (des Endproduktes)
Die Person(en), die das Endprodukt administrieren. Diese ist (sind) verantwortlich für sichere Einrichtung und Administration des Endproduktes. In der Regel hat der Administrator volle Zugriffsrechte für die Konfiguration und Bedienung des Produktes/Systems.
- **Betreiber** (des Endproduktes)
Die Stelle, die für den Betrieb des IT-Systems verantwortlich ist. Der Betreiber ist u.a. zuständig für
 - o die geschäftlichen und betrieblichen Anforderungen an das IT-System, Vorgaben für dessen Betrieb und Anforderungen bzgl. des Informationsaustausches;
 - o Zuarbeit bei der Erstellung einer Risikobewertung für das IT-System (wenn erforderlich);
 - o die Erstellung eines Planes, um das bei einer Risikobewertung ermittelte Restrisiko zu handhaben;
 - o die Sicherstellung, dass Servicevereinbarungen (SLA) oder ähnliche Mechanismen, die für die Erbringung von IT-Services vereinbart werden, Vorgaben für die Implementierung, den Betrieb, die Überwachung und das Änderungsmanagement von Sicherheitsmaßnahmen enthalten;
 - o die Durchführung der betrieblichen Evaluierung (operational evaluation) des IT-Systems und die Validierung/Autorisierung/Freigabe des IT-Systems für den Betrieb

² Aus Gründen der besseren Lesbarkeit wird für die einzelnen Parteien und Instanzen auf die gleichzeitige Verwendung weiblicher und männlicher Sprachformen verzichtet und das generische Maskulinum verwendet. Sämtliche Personen- bzw. Rollenbezeichnungen gelten gleichermaßen für beide Geschlechter.

nach erfolgter Sicherheitsakkreditierung des IT-Systems durch die SAA (wenn erforderlich);

- o Ermittlungen im Falle eines Sicherheitsvorfalls, Feststellung des Schadens und Berichterstattung (an zuständigen Stellen, sofern eine Sicherheitsakkreditierung vorliegt, insbesondere an die SAA, sowie an den Krypto-Support des BSI),
- o die Verteilung der Einsatz- und Betriebsbedingungen an die Endnutzer.

Im NATO-Kontext wird diese Rolle auch als CIS Operational Authority (CISOA), im EU-Kontext als Information Assurance (IA) Operational Authority bezeichnet.

- **BSI**

Das BSI ist als nationale IT-Sicherheitsbehörde u.a. zuständig für IT-sicherheitstechnische Bewertungen (Evaluierungen) von Sicherheitsprodukten/-systemen und deren Zulassung oder Zertifizierung. Außerdem ist es am Freigabeverfahren nach § 50 [VSA] ggf. zu beteiligen. Das BSI nimmt gegenüber der NATO die Funktion der „German National CIS Security Authority (NCSA)“ wahr. Bei der EU wird diese Funktion auch als „Crypto Approval Authority (CAA) bezeichnet.

- **Geheimschutzbeauftragter**

Nach § 8 [VSA] sorgt der Geheimschutzbeauftragte für die Umsetzung der Verschlusssachanweisung und berät die Dienststellenleitungen in allen Fragen des Geheimschutzes. Geheimschutzbeauftragte haben ein unmittelbares Vortragsrecht bei den Dienststellenleitungen. Geheimschutzbeauftragte sind bei allen geheimenschutzrelevanten Maßnahmen zu beteiligen.

- **Endnutzer (End User; des Endproduktes)**

Die Person(en), die das Endprodukt als Anwender nutzen und bedienen. Diese ist (sind) zuständig für die Umsetzung der in den durch den Endprodukthersteller verfassten Einsatz- und Betriebsbedingungen des Endproduktes aufgestellten Anforderungen an den Endnutzer, um einen ordnungsgemäßen, sicheren Betrieb des Endproduktes zu gewährleisten. In der Regel hat der Endnutzer nur eingeschränkte Berechtigungen zur Bedienung des Endproduktes.

- **Separationskernhersteller**

Der Hersteller Kernkonzept GmbH des VS-IT-Produktes L4Re Secure Separation Kernel VS, Version 1.0.0 wird im Folgenden *Separationskernhersteller* genannt. Er lizenziert und liefert L4Re Secure Separation Kernel VS, Version 1.0.0 und zugehörige Dokumentation an einen Endprodukthersteller. Er selbst stellt keine Endprodukte her. Er unterliegt in Abhängigkeit vom jeweiligen Geheimhaltungsgrad der zu schützenden Informationen bestimmten Vorgaben für die Entwicklung, Produktion, Evaluierung, Zulassung und den Vertrieb seines Produktes. Darüber hinaus ist er zur Einhaltung gesetzlicher Vorgaben für den Export verpflichtet.

- **Endprodukthersteller**

Der Endprodukthersteller stellt auf Basis des L4Re Secure Separation Kernel VS, Version 1.0.0 und unter Beachtung der mitgelieferten Dokumentation ein **Endprodukt** her, welches er dem Betreiber ausliefert. Für das Endprodukt muss er eigene SecOPs bereitstellen, die die hier beschriebenen SecOPs spezialisieren. Er unterliegt in Abhängigkeit vom jeweiligen Geheimhaltungsgrad der zu schützenden Informationen bestimmten Vorgaben für die Entwicklung, Produktion, Evaluierung, Zulassung und den Vertrieb seines Produktes. Darüber hinaus ist er zur Einhaltung gesetzlicher Vorgaben für den Export verpflichtet.

- **IT-Sicherheitsbeauftragter**

IT-Sicherheitsbeauftragte unterstützen und beraten nach § 9 [VSA] die Geheimschutzbeauftragten in allen Fragen des Einsatzes von Informationstechnik zur Handhabung von Verschlusssachen (VS-IT).

- **Kryptoverwalter**

Behörden/Dienststellen, die Kryptomittel im Sinne § 59 Abs. 1 [VSA] handhaben, bestellen

einen Kryptoverwalter gemäß § 61 [VSA], der im Rahmen der VSA für die ordnungsgemäße Verwaltung von Kryptomittel sorgt. Dazu gehören sowohl nachweispflichtige Kryptoprodukte, als auch zugehörige Schlüsselmittel, sofern diese nicht durch ein produktspezifisches, integriertes Schlüsselmanagement selbst erzeugt und verteilt werden.

- **Sicherheitsbevollmächtigter**

Der Sicherheitsbevollmächtigte ist im Bereich der geheimschutzbetreuten Wirtschaft gemäß Kap. 3.1 des [GHB] das zentrale Sicherheitsorgan im Unternehmen. Die Geschäftsleitung überträgt ihm die Zuständigkeit für die Durchführung aller Geheimchutzmaßnahmen und bevollmächtigt ihn entsprechend.

- **Security Accreditation Authority (SAA)**

Das Bundesministerium des Innern und für Heimat (BMI) als Nationale Sicherheitsbehörde für den Geheimchutz ist im Sinne der nationalen Zuständigkeit SAA für IT-Systeme zur Handhabung von Verschlusssachen über- oder zwischenstaatlicher Organisationen. Gemäß § 36 [VSA] müssen IT-Systeme zur Handhabung von Verschlusssachen über- oder zwischenstaatlicher Organisationen (beispielsweise der EU oder der NATO) einem Sicherheitsakkreditierungsverfahren unterzogen werden.

Für den Bereich der Bundeswehr übernimmt die DEUmilSAA diese Aufgaben.

2 SYSTEMBESCHREIBUNG

2.1 Einsatzzweck

L4Re Secure Separation Kernel VS, Version 1.0.0 ist ein nach VS-Anforderungsprofil „Separation Kernel“ (BSI-VS-AP-0015-2019) zugelassenes Softwareprodukt, welches entsprechend zum Schutz als GEHEIM eingestufte Daten geeignet ist. Der zugelassene Einsatz ist auf die im Anforderungsprofil beschriebenen Einsatzszenarien 1 und 2 beschränkt.

Konkret ist L4Re Secure Separation Kernel VS, Version 1.0.0 eine spezielle Konfiguration und Version des quelloffenen L4Re Operating System Frameworks. Dieses basiert auf dem L4Re Microkernel als Betriebssystemkern, welcher ein Mikrokern der dritten Generation mit capability-basiertem Sicherheits-Modell mit obligatorischer Zugriffskontrolle ist. Dies erlaubt die Separierung von Anwendungen in verschiedenen Sicherheitsdomänen, Informationsflusskontrolle und – im Rahmen der Zugriffskontrolle – dynamische Zuweisung von Ressourcen und Kommunikationskanälen. Des Weiteren unterstützt der L4Re Microkernel sowohl statische als auch dynamische Anwendungsszenarien, also Start, Neustart und Beendigung von Anwendungen während der Laufzeit.

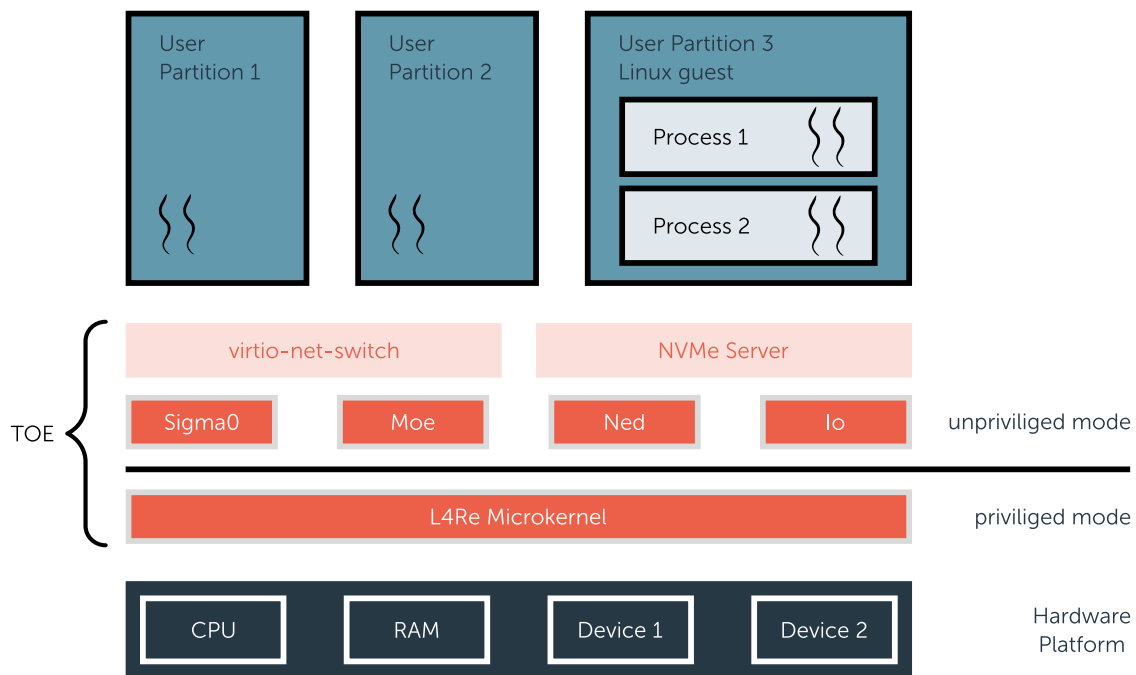


Abbildung 1: Schematische Darstellung der Architektur von L4Re Secure Separation Kernel VS, Version 1.0.0, der Hardware-Plattform und beispielhafter User-Partitionen.

Abbildung 1 stellt die Architektur des Systems schematisch dar. Die Grafik ist an Abbildung 1 im Anforderungsprofil angelehnt. Zwischen der Hardware-Plattform (unten in dunkler Farbe) und den User-Partitionen (oben in hellblau) läuft L4Re Secure Separation Kernel VS, Version 1.0.0 (TOE; target of evaluation; im Anforderungsprofil „trusted code“ genannt). Die in hellem orange dargestellten Komponenten sind optional und können je nach Anwendungsfall genutzt werden. Die Gesamtheit aller dargestellten Komponenten wird in diesem Dokument Endprodukt genannt. Jede in einem Rechteck dargestellte Komponente ist durch die von L4Re Secure Separation Kernel VS, Version 1.0.0 garantierte Adressraumseparierung von anderen Komponenten separiert. Die Prozesse in User-Partition 3 sind aus Sicht von L4Re Secure Separation Kernel VS, Version 1.0.0 nicht voneinander separiert, sie können aber dennoch in unterschiedlichen Adressräumen laufen, wenn das Gast-Betriebssystem dies sicherstellt. Eine detaillierte Beschreibung kann im Security Target gefunden werden.

L4Re Secure Separation Kernel VS, Version 1.0.0 ist als Separationskern konfiguriert, sodass die Sicherheitseigenschaften entsprechend des Security Targets erfüllt werden. L4Re Secure Separation Kernel VS, Version 1.0.0 unterstützt native Anwendungen sowie virtuelle Maschinen (VMs). Die Zugriffsrechte auf alle Ressourcen (also Speicher, Geräte, CPU-Kerne, etc.) werden über Capabilities verwaltet. Anwendungen und VMs können nur auf eine Ressource zugreifen, wenn sie eine Capability mit geeigneten Rechten für diese Ressource besitzen.

Eine Capability ist ein durch L4Re Secure Separation Kernel VS, Version 1.0.0 verwaltetes, unfälschbares Berechtigungstoken. Es beinhaltet eine Referenz auf eine Ressource und Zugriffsrechte. Eine Anwendung kann eine Funktion einer bestimmten Ressource nutzen, indem eine Nachricht via IPC mittels einer Capability, die die Ressource referenziert, gesendet wird. Mittels Capabilities erlaubt L4Re Secure Separation Kernel VS, Version 1.0.0 die wirksame Umsetzung des Prinzips der geringsten Privilegien (POLA; principle of least authority).

Auf Basis der Capability-basierten Zugriffskontrolle erlaubt L4Re Secure Separation Kernel VS, Version 1.0.0 die Kontrolle des Informationsflusses zwischen einzelnen Anwendungen oder Gruppen von Anwendungen, die Compartments genannt werden. Der Begriff Compartment umfasst eine initiale Anwendung zusammen mit allen Anwendungen, welche direkt oder indirekt durch diese initiale Anwendung gestartet werden. Die initialen Anwendungen werden durch die Startkonfiguration von L4Re Secure Separation Kernel VS, Version 1.0.0 bestimmt.

Im Kontext des L4Re Secure Separation Kernel VS, Version 1.0.0 ist eine Anwendung ein Programm, das in ggf. mehreren Threads ausgeführt wird. Alle Threads einer Anwendung haben die gleichen Zugriffsrechte. Anwendungen können mittels eines separaten SDK entwickelt werden, welches nicht Teil des L4Re Secure Separation Kernel VS, Version 1.0.0 ist.

Die Integrität des installierten L4Re Secure Separation Kernel VS, Version 1.0.0 wird durch Secure Boot geschützt. Dies wird für UEFI und Coreboot unterstützt [HSecBoot].

2.2 Systemkomponenten und Funktion

Bei L4Re Secure Separation Kernel VS, Version 1.0.0 handelt es sich um ein reines Softwareprodukt.

In der Regel wird L4Re Secure Separation Kernel VS, Version 1.0.0 vom Separationskernhersteller an den Endprodukthersteller in folgenden Teilen ausgeliefert:

- Zwei Dateiarhive die jeweils das aktuelle L4Re Secure Separation Kernel VS, Version 1.0.0 für x86-Plattformen enthalten; einmal mit VT-x-Unterstützung, einmal ohne.
- Nutzerhandbücher in Dateiform [HConf, HSecBoot, HProxy, diese SecOPs inklusive Annex A und B].

Hinweis:

Der Endprodukthersteller ist verpflichtet, die Vollständigkeit und Integrität der ausgelieferten Dateien unverzüglich, nach Erhalt von L4Re Secure Separation Kernel VS, Version 1.0.0, zu prüfen. Die Dateien sind digital signiert. Den zugehörigen öffentlichen Schlüssel teilt der Separationskernhersteller dem Endprodukthersteller über einen geeigneten separaten Kanal mit.

2.3 Zulassung und zugelassener Konstruktionsstand

Die Art der Zulassung und der aktuell zugelassene Konstruktionsstand von L4Re Secure Separation Kernel VS, Version 1.0.0 sind Annex A zu entnehmen.

Vor einer Installation und Inbetriebnahme muss sichergestellt sein, dass nur der in Annex A benannte, aktuell zugelassene Konstruktionsstand in Verwendung kommt. Dies ist Voraussetzung sowohl für die Freigabe des IT-Systems durch den Betreiber als auch für die Sicherheitsakkreditierung des IT-Systems durch die SAA (falls erforderlich).

2.4 Kompatibilität, Interoperabilität, Konformität

Die Zielplattform von L4Re Secure Separation Kernel VS, Version 1.0.0 ist ein System mit x86_64 Intel CPU mit Broadwell Microarchitektur oder neuer, Unterstützung für VT-x mit EPT und Intel IOMMU [vgl. HConf Abschnitt „Platform requirements“]. Da es sich bei L4Re Secure Separation Kernel VS, Version 1.0.0 um ein Betriebssystem ohne konkret festgelegten Einsatzzweck handelt, sind die Anforderungen bewusst weit gefasst. Für konkrete Anwendungen muss der Endprodukthersteller, ggf. in Abstimmung mit dem Separationskernhersteller, eine Hardwarequalifizierung für die eingesetzte Hardware vornehmen.

2.5 Betriebsarten

L4Re Secure Separation Kernel VS, Version 1.0.0 bietet keine verschiedenen Betriebsarten.

2.6 Installation, Systemintegration und Konfiguration

Die Installation auf konkreter Hardware, die Systemintegration und Konfiguration von L4Re Secure Separation Kernel VS, Version 1.0.0 wird vom Endprodukthersteller vorgenommen. Anforderungen für die Installation und Integration von L4Re Secure Separation Kernel VS, Version 1.0.0 in einem IT-System sowie eine systemspezifische Konfiguration sind im Nutzerhandbuch [HConf, HSecBoot] aufgeführt. Weitere Informationen zu der Integration von L4Re Secure Separation Kernel VS, Version 1.0.0 in andere Produkte sowie Hinweise zur Nachweisführung sind in Annex I enthalten und müssen beachtet werden.

Die Umsetzung dieser Anforderungen ist vom Endprodukthersteller im Rahmen der Installation und Konfiguration sicherzustellen und durch die SAA im Rahmen der Sicherheitsakkreditierung (falls erforderlich) zu prüfen.

Der Endprodukthersteller muss, ggf. in Zusammenarbeit mit Administrator oder Betreiber, ein geeignetes Konzept zum Betrieb und zur Wartung des Endproduktes definieren, welches dessen gesamten Lebenszyklus abdeckt.

2.7 Betrieb

Unter dem „Betrieb“ von L4Re Secure Separation Kernel VS, Version 1.0.0 wird hier die Wartung des Endproduktes durch den Endprodukthersteller verstanden. Anforderungen an den Betrieb des Endproduktes müssen durch den Endprodukthersteller dokumentiert werden.

Der Endprodukthersteller muss mit dem Separationskernhersteller einen Support-Vertrag schließen, um über neue Sicherheitsprobleme und deren Behebungen für L4Re Secure Separation Kernel VS, Version 1.0.0 informiert zu werden. Außerdem muss der Endprodukthersteller geeigneten Kanälen zur Information über Sicherheitsprobleme mit der eingesetzten Hardware verfolgen. Der Endprodukthersteller muss bewerten, inwieweit das Endprodukt von einem Problem betroffen ist, und ggf. entsprechend Konfigurations- oder Softwareaktualisierungen vornehmen und ggf. Betreiber und/oder Administratoren des Endproduktes informieren. Bei schwerwiegenden Sicherheitsproblemen, die nicht unmittelbar behoben werden können, müssen ggf. alle betroffenen Systeme umgehend außer Betrieb genommen werden. [siehe auch HConf Abschnitt „Integrity Check“]

Endet der Support-Vertrag oder der Support für die eingesetzte Version von L4Re Secure Separation Kernel VS, Version 1.0.0, muss der Endprodukthersteller eine Aktualisierung auf eine noch unterstützte Versionen mit entsprechendem Support-Vertrag vornehmen oder alle betroffenen Endprodukte außer Betrieb nehmen.

2.8 Abstrahlsicherheit

L4Re Secure Separation Kernel VS, Version 1.0.0 ist ein reines Software-Produkt. Die Einschätzung zur Abstrahlsicherheit muss vom Endprodukthersteller für das Endprodukt unter Beachtung des Zieleinsatzkontextes vorgenommen werden.

3 SICHERHEITSMANAGEMENT

Nachfolgend werden besondere Anforderungen an das Sicherheitsmanagement bzw. Schlüsselmanagement von L4Re Secure Separation Kernel VS, Version 1.0.0 beschrieben.

3.1 Zuständigkeiten für Sicherheits-/Schlüsselmanagement

Der IT-Sicherheitsbeauftragte, der IT-System-Administrator und, sofern in Annex B Bestandteile des TOE mit dem Warnvermerk CRYPTO oder CCI versehen worden sind, der Kryptoverwalter sind in ihrem Zuständigkeitsbereich verantwortlich für die Umsetzung der Anforderungen.

Sofern eine SAA erforderlich ist, ist die Umsetzung der Vorgaben im Rahmen der Systemakkreditierung von der SAA (falls erforderlich) in geeigneter Weise zu überprüfen.

3.2 Beschreibung des Sicherheits-/Schlüsselmanagements

Das Sicherheitsmanagement für L4Re Secure Separation Kernel VS, Version 1.0.0 ist im Nutzerhandbuch [HSecBoot] beschrieben.

3.3 Quantencomputer-Resistenz

Es wird darauf hingewiesen, dass für den sicheren Start des Produktes gemäß [HSecBoot] in der zugelassenen Konfiguration auf kryptographische Mechanismen der Plattformen zurückgegriffen wird, die **nicht** Quantencomputer-resistent sind.

Hieraus ergibt sich das Risiko, dass ein Angreifer beim Vorhandensein entsprechender Quantencomputer den Sicheren Bootprozess in der aktuellen Version umgeht.

Ansonsten umfasst das Produkt keine weiteren kryptographischen Mechanismen, so dass ein Mitschneiden ausgehenden Netzwerkverkehrs zu einem entfernten Kommunikationspartner und späteres Entschlüsseln („store now – decrypt later“) keine Bedrohung darstellt.

Beim Einsatz muss somit darauf geachtet werden, dass Endprodukte aufbauend auf dem L4Re Secure Separation Kernel VS, Version 1.0.0 für den Sicheren Bootprozess entsprechende QC-resistente Mechanismen bereitstellen, die der L4Re Secure Separation Kernel VS, Version 1.0.0 dann nutzen kann

3.4 Nutzung veralteter Krypto-Algorithmen

Das Produkt L4Re Secure Separation Kernel VS, Version 1.0.0 verwendet selber keine Krypto-Algorithmen und stellt somit ein sogenanntes None-Krypto Produkt dar.

4 VS-EINSTUFUNGEN

4.1 VS-Behandlungshinweise

Die für Kontroll- und Schutzmaßnahmen für L4Re Secure Separation Kernel VS, Version 1.0.0 zugrunde zu legenden VS-Einstufungen sind der als Annex B beigefügten Einstufungsliste zu entnehmen.

5 NACHWEISFÜHRUNG UND KONTROLLE

5.1 Verkauf, Ausleihe und Export

L4Re Secure Separation Kernel VS, Version 1.0.0 unterliegt einem eingeschränkten Vertrieb durch den Separationskernhersteller. Der Export bzw. die Verbringung³ aus Deutschland unterliegt evtl. der deutschen Exportgesetzgebung. Zur Klärung ist das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) zu kontaktieren.

Der Export bzw. die Verbringung von L4Re Secure Separation Kernel VS, Version 1.0.0 aus einem anderen Land unterliegt evtl. der jeweiligen Exportkontrollgesetzgebung. Der Export ist somit mit der zuständigen Behörde/Institution zu klären. Bei der Rückkehr von Dienstreisen ist zu beachten, dass diese Gesetzgebung u.U. zu einem Verstoß gegen diese SecOPs führen kann, der zu verhindern ist; eine Abstimmung mit dem eigenen Geheimschutzbeauftragten ist somit erforderlich.

Für eine Ausleihe durch Separationskernhersteller oder Endnutzer gelten die gleichen Vorgaben.

5.2 Konformitätserklärung (DoC)

In L4Re Secure Separation Kernel VS, Version 1.0.0 werden keine kryptographischen Mechanismen implementiert, sondern lediglich Typ B-Algorithmen der entsprechenden Plattformen für den Sicheren Start verwendet. Die Unterzeichnung einer Konformitätserklärung ist daher nicht erforderlich.

5.3 VS-Nachweisführung und Kontrolle

Eine VS-Nachweisführung wird für L4Re Secure Separation Kernel VS, Version 1.0.0 nicht gefordert.

³ Dies schließt Dienstreisen außerhalb Deutschlands ein.

6 MATERIELLE SICHERHEIT

6.1 Zuständigkeiten

Dieses Kapitel beschreibt sicherheitsrelevante Aspekte hinsichtlich des Einsatzes von L4Re Secure Separation Kernel VS, Version 1.0.0. Die strikte Einhaltung der nachfolgend aufgeführten Anweisungen ist erforderlich, um dauerhaft die Sicherheit der mit L4Re Secure Separation Kernel VS, Version 1.0.0 zu schützenden eingestuft Informationen zu gewährleisten. Für die Umsetzung und Einhaltung dieser Vorgaben sind der Geheimschutzbeauftragte, der IT-Sicherheitsbeauftragte und, sofern in Annex B Bestandteile des TOE mit dem Warnvermerk CRYPTO oder CCI versehen worden sind, der Kryptoverwalter verantwortlich.

Sofern eine SAA erforderlich ist, ist die Umsetzung der Vorgaben im Rahmen der Systemakkreditierung von der SAA in geeigneter Weise zu überprüfen.

6.2 Anforderungen an die Materielle Sicherheit

Die für den jeweiligen Betreiber und Endnutzer geltenden Geheimschutzbestimmungen zur materiellen Sicherheit sind zu beachten.

Darüber hinaus gelten nachstehende Sicherheitsvorgaben.

6.2.1 Allgemein

Für L4Re Secure Separation Kernel VS, Version 1.0.0 sind Sicherheitsvorkehrungen in Übereinstimmung mit der Einstufungsliste in Annex B zu treffen:

- Vor der Installation ist die Integrität vom L4Re Secure Separation Kernel VS, Version 1.0.0 zu prüfen [entsprechend HConf Abschnitt „Integrity Check“]. Es ist sicherzustellen, dass die aktuellste Version vorliegt.
- Nach der Installation ist die Integrität des installierten L4Re Secure Separation Kernel VS, Version 1.0.0 mittels Secure Boot zu schützen [entsprechend HSecBoot].
- Jede vermutete Manipulation des zugelassenen Produktes ist unverzüglich dem zuständigen Geheimschutzbeauftragten oder IT-Sicherheitsbeauftragten zu melden (siehe Kapitel 10 „SICHERHEITSVORFÄLLE“).
- Notwendige Sicherheitsvorkehrungen für das Endprodukt müssen durch den Endprodukthersteller dokumentiert werden.

6.2.2 Betriebsbereites Gerät

Die in Annex B aufgeführten VS-Einstufungen und Behandlungshinweise sind zu beachten.

Im Betrieb entspricht die VS-Einstufung von L4Re Secure Separation Kernel VS der Einstufung des verwendeten Schlüsselmaterials, bzw. der höchsten Einstufung der zu schützenden Informationen. Zu schützende Informationen und Schlüsselmaterial hängen von der durch den Endprodukthersteller vorgenommenen Konfiguration und dem Einsatzkontext des Endproduktes ab.

6.2.3 Lagerung und Transport

Die Auslieferung vom Separationskernhersteller zum Endprodukthersteller geschieht in Form signierter Datei-Archive. Die Integrität der erhaltenen Archive muss vom Endprodukthersteller durch

Prüfung der Signatur sichergestellt werden. Die Korrektheit des öffentlichen Signaturschlüssels muss über einen geeigneten Kanal verifiziert werden.

Nachfolgende Transporte oder Lagerungen liegen in der Verantwortung des Endproduktherstellers, des Administrators bzw. des Betreibers. Sich aus der Dokumentation [HConf, HSecBoot] ergebende Einschränkungen müssen beachtet werden. Der Endprodukthersteller stellt ggf. zusätzliche Anforderungen.

6.2.4 Behandlung von Schlüsselmaterial

Der Endprodukthersteller und, sofern in Annex B Bestandteile des TOE mit dem Warnvermerk CRYPTO oder CCI versehen worden sind, der Kryptoverwalter sind für eine sichere Handhabung des Schlüsselmaterials verantwortlich.

Vorgaben aus der Dokumentation [HSecBoot] sind einzuhalten.

6.3 Geräteschutzmechanismen

6.3.1 Tamper-Schutz

Der Einsatz von L4Re Secure Separation Kernel VS, Version 1.0.0 sieht die Nutzung von Secure Boot vor [siehe HSecBoot]. Damit wird beim Booten des Systems die Integrität des TOE geprüft, bevor es gestartet wird. Schlägt die Integritätsprüfung fehl, wird der Boot-Vorgang abgebrochen. Eine automatische Löschung ist durch L4Re Secure Separation Kernel VS, Version 1.0.0 nicht vorgesehen.

Ein aktiver Tamper-Schutz ist ggf. Teil eines Endproduktes. Die notwendigen Maßnahmen im Falle des Auslösens des Tamper-Schutzes werden entsprechend vom Endprodukthersteller festgelegt. Zu beachten sind auch die Hinweise in Kapitel 10.

6.3.2 Meldung und Maßnahmen

Anforderung für das Melden eines Sicherheitsvorfalls oder vermuteten Sicherheitsvorfalls und zu ergreifende Maßnahmen sind in Kapitel 10 aufgeführt.

6.4 Routinemäßige Vernichtung

6.4.1 Vernichten/Löschen von Schlüsseln/Zertifikaten

Im Rahmen der Installation von L4Re Secure Separation Kernel VS, Version 1.0.0 kommt Schlüsselmaterial für Secure Boot zum Einsatz [siehe HSecBoot]. Die Definition eines geeigneten Umgangs mit dem (privaten) Schlüsselmaterial obliegt dem Endprodukthersteller. Selbiges gilt für Schlüsselmaterial, das ggf. für den Betrieb des Endproduktes notwendig ist. L4Re Secure Separation Kernel VS, Version 1.0.0 bietet keine vorgefertigte Funktionalität zur Vernichtung oder Löschung von Schlüsselmaterial.

6.4.2 Produktentsorgung und -vernichtung

Bzgl. der Entsorgung und Vernichtung von L4Re Secure Separation Kernel VS, Version 1.0.0 bestehen keine besonderen Anforderungen. Jedoch kann der Endprodukthersteller Anforderungen für das Endprodukt stellen.

7 PERSONELLE SICHERHEIT

Zusätzlich zu den Maßnahmen und Kriterien, die in den Referenzen [SÜG] und [VSA] beschrieben sind, gelten die nachfolgend aufgeführten Sicherheitsanforderungen.

L4Re Secure Separation Kernel VS, Version 1.0.0, wie es vom Separationskernhersteller geliefert wird, beinhaltet keine eingestuft Informationen. Die hier beschriebenen Bestimmungen sind entsprechend allgemein gehalten und deren Anwendbarkeit hängt vom konkreten Einsatzzweck von L4Re Secure Separation Kernel VS, Version 1.0.0 ab.

7.1 Zuständigkeiten

Die aufgeführten Maßnahmen bzgl. der personellen Sicherheit und Autorisierung des Personals sind vom Geheimschutzbeauftragten, Sicherheitsbevollmächtigten und dem IT-Sicherheitsbeauftragten zu beachten und umzusetzen.

7.2 Ermächtigung und Autorisierung

Zugang zu Verschlusssachen (VS), die im Sinne von § 4 Abs. 1, 2 [SÜG] mit dem Geheimhaltungsgrad VS-VERTRAULICH oder höher eingestuft sind, darf nur Personen gewährt werden, die zuvor nach dem SÜG und den allgemeinen Verwaltungsvorschriften zur Durchführung von Sicherheitsüberprüfungen überprüft und zum Zugang ermächtigt wurden.

VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH dürfen nur den Personen zugänglich gemacht werden, die auf Grund ihrer Aufgabenerfüllung von ihr Kenntnis haben müssen. Bevor eine Person Zugang zu Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH erhält, ist sie auf Anlage V zur Verschlusssachenanweisung [VSA] zu verpflichten. Dabei ist ihr gegen Empfangsbestätigung ein Exemplar der Anlage V zugänglich zu machen.

7.3 Kenntnis nur, wenn nötig (Need-To-Know)

Der Zugang zu einem auf L4Re Secure Separation Kernel VS, Version 1.0.0 basierenden Endprodukt oder zu Teilen dessen ist in Abhängigkeit der damit verarbeiteten oder gespeicherten Informationen ggf. gemäß dem Prinzip „Kenntnis nur, wenn nötig (Need-To-Know)“ zu begrenzen. Ggf. fallen darunter dann auch die für das Endprodukt angepassten oder erstellten Konfigurationsdateien für L4Re Secure Separation Kernel VS, Version 1.0.0. Die Sicherheitseigenschaften von L4Re Secure Separation Kernel VS, Version 1.0.0 gelten bei korrekter Konfiguration dennoch unabhängig von der Kenntnis der Konfiguration.

8 WARTUNG UND REPARATUR

8.1 Zuständigkeiten

Folgende Vorgaben sind bei Wartung und Reparatur von L4Re Secure Separation Kernel VS, Version 1.0.0 zu beachten. In der Regel sind der Betreiber (ggf. unterstützt durch den Geheimschutzbeauftragten, den IT-Sicherheitsbeauftragte, den Systemadministrator und, sofern in Annex B Bestandteile des TOE mit dem Warnvermerk CRYPTO oder CCI versehen worden sind, den Kryptoverwalter) sowie der Endprodukthersteller für die Einhaltung der Maßnahmen in ihrem jeweiligen Zuständigkeitsbereich verantwortlich.

8.2 Vorgaben und Maßnahmen

Folgende Vorgaben für Wartung und Reparatur von L4Re Secure Separation Kernel VS, Version 1.0.0 sind zu beachten:

- Bei Wartungs-/Instandsetzungsarbeiten ist entsprechend vertrauenswürdigen Personal einzusetzen. Für weitere Details siehe Kap 7.2
- Bei Rekonfiguration oder Upgrades ist – wie schon bei der Erstinstallation – die mitgelieferte Dokumentation zu beachten [HConf, HSecBoot].
- Für das Endprodukt können sich weitere Vorgaben ergeben, die vom Endprodukthersteller dokumentiert werden müssen.

9 NOTFALLPROZEDUREN

Für den Schutz nationaler VS sind für L4Re Secure Separation Kernel VS, Version 1.0.0 keine speziellen Notfallprozeduren vorgesehen. Ggf. sind für das Endprodukt Notfallprozeduren notwendig, die vom Endprodukthersteller dokumentiert werden müssen.

10 SICHERHEITSVORFÄLLE

10.1 Ansprechpartner des Betreibers

Der Endprodukthersteller ist verpflichtet, dem Separationskernhersteller einen Ansprechpartner für Sicherheitsthemen z.B. den Geheimschutz- oder IT-Sicherheitsbeauftragten inkl. Kontaktdaten zu benennen und diese Informationen auf dem aktuellen Stand zu halten. Der Separationskernhersteller wird diesen Ansprechpartner nur für Informationen zu Sicherheitsvorfällen, erforderlichen Sicherheitsmaßnahmen, sicherheitsrelevanten Produktupdates sowie Aktualisierungen dieser Zulassung kontaktieren.

10.2 Meldepflicht und Zuständigkeiten

Für die Untersuchung und den Bericht meldepflichtiger Sicherheitsvorfälle (siehe Abschnitt 10.3) ist der Endprodukthersteller ggf. in Abstimmung mit dem Betreiber des Endproduktes (unterstützt durch den Geheimschutzbeauftragten und den IT-Sicherheitsbeauftragten) zuständig. Sofern für das System eine Sicherheitsakkreditierung vorliegt, ist die SAA zu informieren.

Die in der Referenz [BSI TL - IT 01] aufgeführten Mitwirkungspflichten von Separationskern- und Endprodukthersteller als Hersteller sowie Betreiber und Endnutzer als Bedarfsträger im Sinne der Technischen Leitlinie bei der Behandlung von Sicherheitsvorfällen (Incidents) sind zu beachten.

10.3 Meldepflichtige Vorfälle

Der Endprodukthersteller muss jegliches unerwartete Verhalten, von dem er nicht sicher ausschließen kann, dass es ein sicherheitsrelevanter Fehler von L4Re Secure Separation Kernel VS, Version 1.0.0 ist, unverzüglich an den Separationskernhersteller melden (siehe Abschnitt 11.1).

Eine Meldung muss die Versionsnummer von L4Re Secure Separation Kernel VS, Version 1.0.0, das beobachtete Verhalten und das erwartete Verhalten beinhalten.

10.4 Maßnahmen bei kommunizierten Sicherheitsinformationen

Der Separationskernhersteller analysiert, ob ein ihm gemeldeter Vorfall tatsächlich auf L4Re Secure Separation Kernel VS, Version 1.0.0 zurückzuführen ist, d.h., ob eine Verletzung der im Security Target beschriebenen Eigenschaften (insbesondere Separierungseigenschaften) für den Vorfall verantwortlich ist.

Bei entdeckten Schwachstellen von L4Re Secure Separation Kernel VS, Version 1.0.0 oder entdeckten Sicherheitsproblemen in seiner Einsatzumgebung informiert der Separationskernhersteller insbesondere das BSI. Außerdem kommunizieren das BSI oder der Separationskernhersteller nach Absprache mit dem BSI Informationen, i.d.R. verbunden mit umzusetzenden Maßnahmen (bspw. unverzügliche Update-Pflicht, Änderung in der Konfiguration des Produkts, Änderung der Einsatz- und Betriebsbedingungen, etc.).

Diese Informationen und Handlungsanweisungen werden durch den Separationskernhersteller an den in 10.1 genannten Ansprechpartner des Endproduktherstellers gesendet.

Diesen Anweisungen ist verpflichtend Folge zu leisten.

10.5 Maßnahmen nach entdeckter Kompromittierung

Die Maßnahmen nach entdeckter Kompromittierung müssen durch den Endprodukthersteller entsprechend des Einsatzzweckes und der Einsatzumgebung des Endproduktes festgelegt werden.

11 KONTAKTE

11.1 Hersteller

Hendrik Tews (Projektverantwortlicher)
Adam Lackorzynski (CTO)
Michael Hohmuth (CEO)

Kernkonzept GmbH
Buchenstraße 16b
01097 Dresden

E-Mail-Adresse für verantwortungsvolle Meldung von Sicherheitsproblemen:
security@kernkonzept.com. Für verschlüsselte Nachrichten ist unter
<https://www.kernkonzept.com/de/kontakt/> ein PGP-Schlüssel mit dem Fingerprint C4DC 2909 A22E
D080 C012 5373 4055 CBA2 A4FD 855B verlinkt.

11.2 BSI Krypto-Support

Bei entdeckter oder vermuteter Manipulation nennen Sie bitte nur die Gerätebezeichnung und Ihre Kontaktinformation.

Weitere Informationen müssen vertraulich ausgetauscht werden.

Bundesamt für Sicherheit in der Informationstechnik
Krypto-Support
Postfach 20 03 63
53133 Bonn

E-Mail: krypto-support@bsi.bund.de

11.3 BSI Zulassung

Bei Fragen zum Verfahren verweisen wir auf unsere FAQ-Übersicht im Internet unter
<https://www.bsi.bund.de/Zulassung>

Sollten darüber hinaus noch Fragen offen sein, so können Sie sich – sofern es sich um nicht sensible Inhalte handelt – per E-Mail an folgende Adresse wenden:

E-Mail: zulassung@bsi.bund.de

ANNEX A

Zulassung und Konstruktionsstand

L4Re Secure Separation Kernel VS, Version 1.0.0

Zulassungs-ID BSI-VSA-10624

1 Zulassung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für L4Re Secure Separation Kernel VS, Version 1.0.0 mit der Zulassungs-ID BSI-VSA-10624 mit Datum 01.01.2024 eine Zulassung für den Schutz von Informationen ausgestellt, die national als GEHEIM eingestuft sind.

Die in den Einsatz- und Betriebsbedingungen getroffenen Regelungen sind einzuhalten.

Nachfolgend ist der aktuell zugelassene Konstruktionsstand von L4Re Secure Separation Kernel VS, Version 1.0.0 aufgeführt. Der Konstruktionsstand wird für jede zugelassene Produktversion festgehalten und ist integraler Bestandteil der Zulassungsdokumentation.

2 Überprüfung des Konstruktionsstandes

Der Hersteller ist für die Auslieferung von L4Re Secure Separation Kernel VS, Version 1.0.0 mit dem korrekten, zugelassenen Konstruktionsstand und der korrekten Version verantwortlich. Vor einer Installation und Inbetriebnahme ist vom Betreiber des IT-Systems und der SAA (falls vorhanden), ggf. unterstützt durch den IT-Sicherheitsbeauftragten zu prüfen, ob das zu installierende Produkt zugelassen ist und der Konstruktionsstand des ausgelieferten Produktes mit dem nachfolgend aufgeführten, zugelassenen Konstruktionsstand übereinstimmt. Vor der ersten Nutzung ist der Betrieb des Produktes durch den jeweiligen Dienststellenleiter für den Einsatz für den entsprechenden nationalen Geheimhaltungsgrad freizugeben.

3 Abweichungen vom Konstruktionsstand

Werden Abweichungen zwischen dem hier aufgeführten und dem ausgelieferten Konstruktionsstand festgestellt, sind die in Kapitel 11 des Hauptteils dieses Dokumentes aufgeführten Kontakte zu konsultieren, um eine Klärung herbeizuführen.

4 Konstruktionsstand

Nachfolgend ist der aktuell zugelassene Konstruktionsstand von L4Re Secure Separation Kernel VS, Version 1.0.0 aufgeführt. Der Konstruktionsstand wird für jede zugelassene Produktversion festgehalten und ist integraler Bestandteil der Zulassungsdokumentation.

L4Re Secure Separation Kernel VS, Version 1.0.0 liegt in Version 1.0.0 vor. Die Zielplattform ist ein System mit x86_64 Intel CPU mit Broadwell Microarchitektur oder neuer, Unterstützung für VT-x mit EPT und Intel IOMMU. Das Produkt umfasst folgende Bestandteile:

- Datei-Archiv, das die Software in einer Version mit VT-x-Unterstützung enthält. SHA-256:
911f7183493c4f7a89e7444457d6262b60310192d1d099447690e228766ec1f1
- Datei-Archiv, das die Software in einer Version ohne VT-x-Unterstützung enthält. SHA-256:
2963496c19fa7737c464f241e5746d972c4e6cadf3832e0e55cb010ca52d086e
- Nutzerhandbücher:
 - PDF-Datei mit Development Guidance for a Compartment Communication Proxy based on L4Re. Stand 2023-09-05. SHA-256:
474d953f9c04924c14973dca519fbf688561c3cbf76ce89c29ab29fe5e004798
 - PDF-Datei mit L4Re Configuration Guidance. Stand 2023-10-11. SHA-256:
cd786e0ab8b53b2d09a495fa87e33292794e7d6ee86decc886694d5a8ef5e0d9
 - PDF-Datei mit L4Re Secure Boot Guidance. Stand 2023-09-05. SHA-256:
2f5cb6a90c6bb42b76692dbb49ab7a7501981cc2b6f3cc71f74326ef20846864

Des Weiteren ist folgende Dokumentation für L4Re Secure Separation Kernel VS, Version 1.0.0 separat erhältlich:

- Datei-Archiv mit L4Re Interface and Usage Documentation. SHA-256:
d52ea7aff50f9070c4c5296733977cfb3ab65d9db256654e96003df5b4537003

ANNEX B

Einstufungsliste

L4Re Secure Separation Kernel VS, Version 1.0.0

Zulassungs-ID BSI-VSA-10624

		Geheimhaltungsgrad ^{a b}				OFFEN ^a	Bemerk.
		STRENG GEHEIM	GEHEIM	VS- Vertr.	VS-NfD		
1	L4Re Secure Separation Kernel VS, Version 1.0.0 SW-Installationsmedium					X	1)
2	Private Schlüssel für Secure-Boot-Setup					X	2) 4)
3	L4Re Secure Separation Kernel VS, Version 1.0.0, installiert, betriebsbereit					X	
4	L4Re Secure Separation Kernel VS, Version 1.0.0, ausgeschalteter Zustand					X	3) 4)

Allgemeine Bemerkung:

L4Re Secure Separation Kernel VS, Version 1.0.0 selbst erfordert keinerlei Einstufungen, jedoch kann der Endprodukthersteller für ein auf L4Re Secure Separation Kernel VS, Version 1.0.0 basierendes Endprodukt Einstufungen fordern.

- 1) Das Installationsmedium ist nicht eingestuft, jedoch bezüglich seiner Integrität zu schützen.
- 2) Grundsätzlich sind die Schlüssel nicht eingestuft, doch jederzeit gegen unbefugten Zugriff zu schützen. Werden im Betrieb eingestufte Informationen verarbeitet, kann dies auch eine Einstufung der Schlüssel erforderlich machen.
- 3) Eine VS-Nachweisführung wird für L4Re Secure Separation Kernel VS, Version 1.0.0 nicht gefordert.

-
- a Nationale Kryptomittel im Sinne § 59 Abs. 1 VSA sind Produkte, Geräte und die dazugehörigen Dokumente sowie zugehörige Schlüsselmittel zur Entschlüsselung, Verschlüsselung und Übertragung von Informationen, die vom BSI als solche festgelegt werden. Kryptomittel sind gem. Abschnitt IX, VSA insbesondere mittels Kryptoverwalter zu handhaben. Kryptomittel verfügen gem. § 59 Abs. 2 VSA bei vorliegender Einstufung über den Warnvermerk „CRYPTO“ bzw. „KRYPTO“ oder bei nicht vorliegender Einstufung den Warnvermerk „CCI“. EU-Vorschriften hierzu sind im IASG2-03 Annex B, respektive für die NATO im SDIP-293-1 Kap. 6 aufgeführt.
VS-IT-Produkte, die keine Kryptomittel im Sinne von § 59 Abs. 1 VSA sind, werden in der obigen Tabelle dagegen lediglich mit „X“ markiert.
- b Bei der Verwendung des Produktes zum Schutz von NATO / EU-Verschlusssachen gelten korrespondierende internationale Geheimhaltungsgrade und Markierungen.

- 4) L4Re Secure Separation Kernel VS, Version 1.0.0 und private Schlüssel sind separat zu lagern und zu transportieren.

Abkürzungen Einstufungen/Kennzeichnungen:

VS-NfD (VS-NUR FÜR DEN DIENSTGEBRAUCH)

VS-Vertr. (VS-VERTRAULICH)

ANNEX I

ETR for Composition (EfC)

L4Re Secure Separation Kernel VS, Version 1.0.0

Zulassungs-ID BSI-VSA-10624

1 Beschreibung

Im Annex I werden Hinweise zur Nutzung des Produktes gegeben, die bei der Einbindung in andere Produkte und deren Evaluierung zu beachten sind. Dieses Dokument richtet sich an Hersteller von Produkten, die L4Re Secure Separation Kernel VS, Version 1.0.0 in ihre eigenen Produkte integrieren und auf den geprüften Sicherheitsmechanismen aufbauen wollen sowie an Evaluatoren, die mit der Bewertung von informationssichernden Systemen auf Basis des L4Re Secure Separation Kernel VS, Version 1.0.0 beauftragt sind.

Der Annex I ist eingestuft und daher diesem Dokument nicht angehängt. Dieses Dokument ist entsprechend ein Platzhalter.

Der Hersteller muss den Annex I jedem Bedarfsträger ohne Aufforderung zur Verfügung stellen, damit die Kunden über die Restrisiken informiert sind. Sollte der Annex R nicht vorliegen, kann dieser beim Hersteller angefordert werden