KERNKONZEPT

SCHNELLER SICHER ZULASSEN MIT DEM KOMPOSITIONSANSATZ

Dr. Michael Vogel | Dr. Michael Hohmuth | Katrin Kahle | Matthias Lange

Motivation

- Erfordernis mehr und schneller zu zulassen
- Steigende Komplexität der IT-Systeme
- Effiziente Nutzung begrenzter Ressourcen

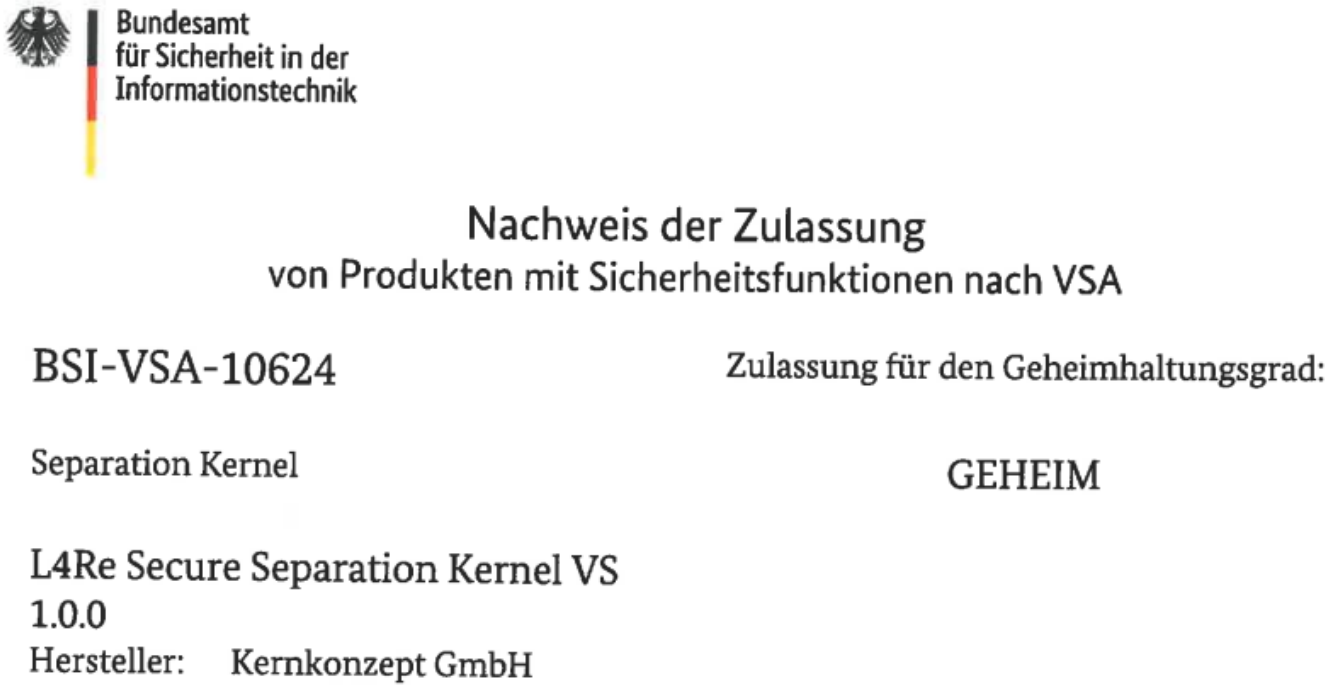
KOOPERATION GEWINNT

DIVIDE & CONQUER

L4RE SECURE SEPARATION KERNEL

01

Zulassung des L4Re SSK VS



Bundesamt
für Sicherheit in der
Informationstechnik

Nachweis der Zulassung
von Produkten mit Sicherheitsfunktionen nach VSA

BSI-VSA-10624

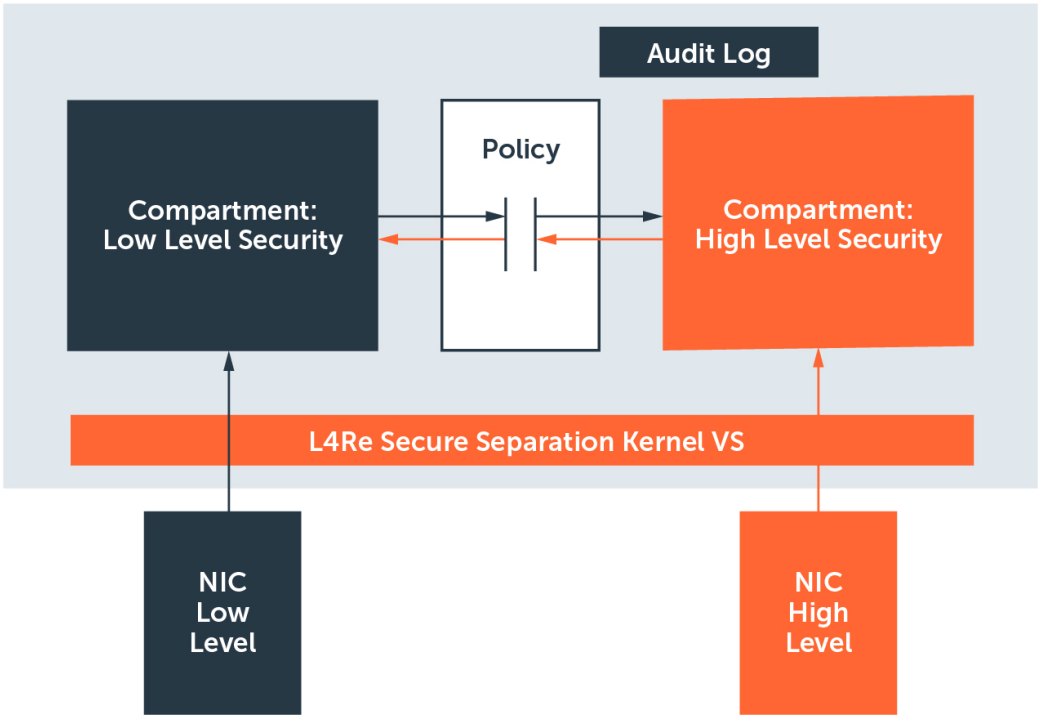
Zulassung für den Geheimhaltungsgrad:

Separation Kernel

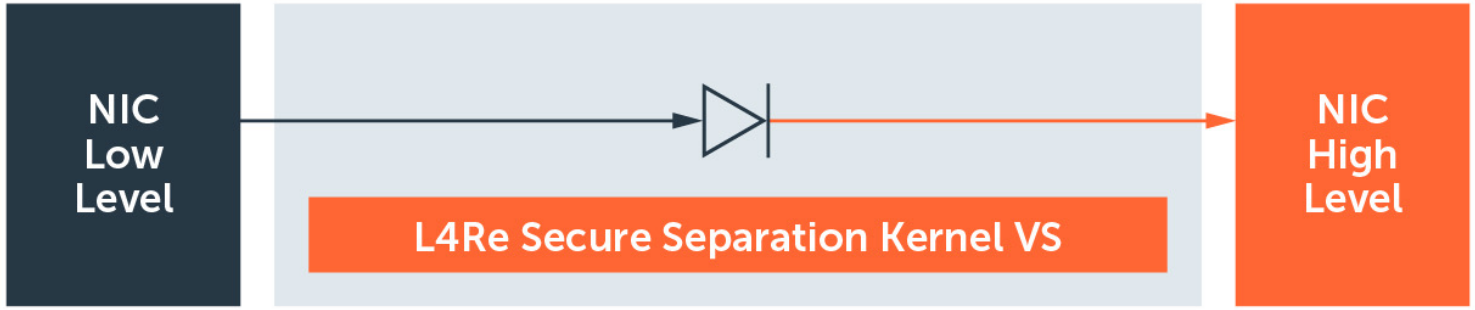
GEHEIM

L4Re Secure Separation Kernel VS
1.0.0
Hersteller: Kernkonzept GmbH

Beispiel: Information Exchange Gateway



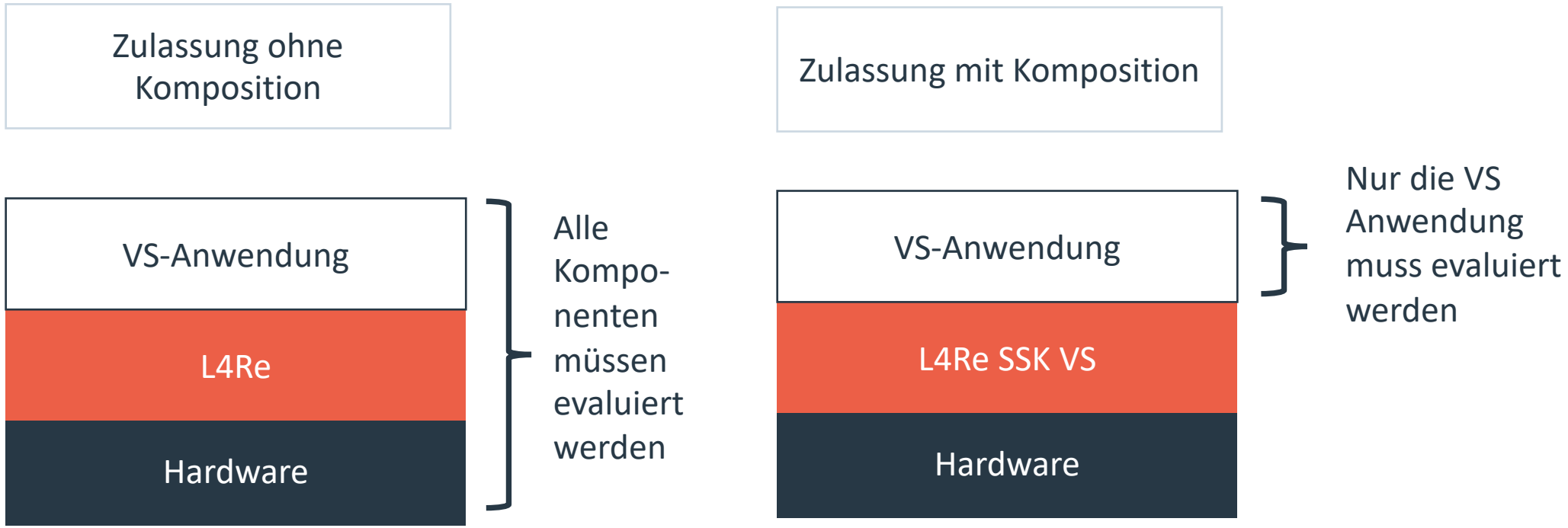
Beispiel: Datendiode



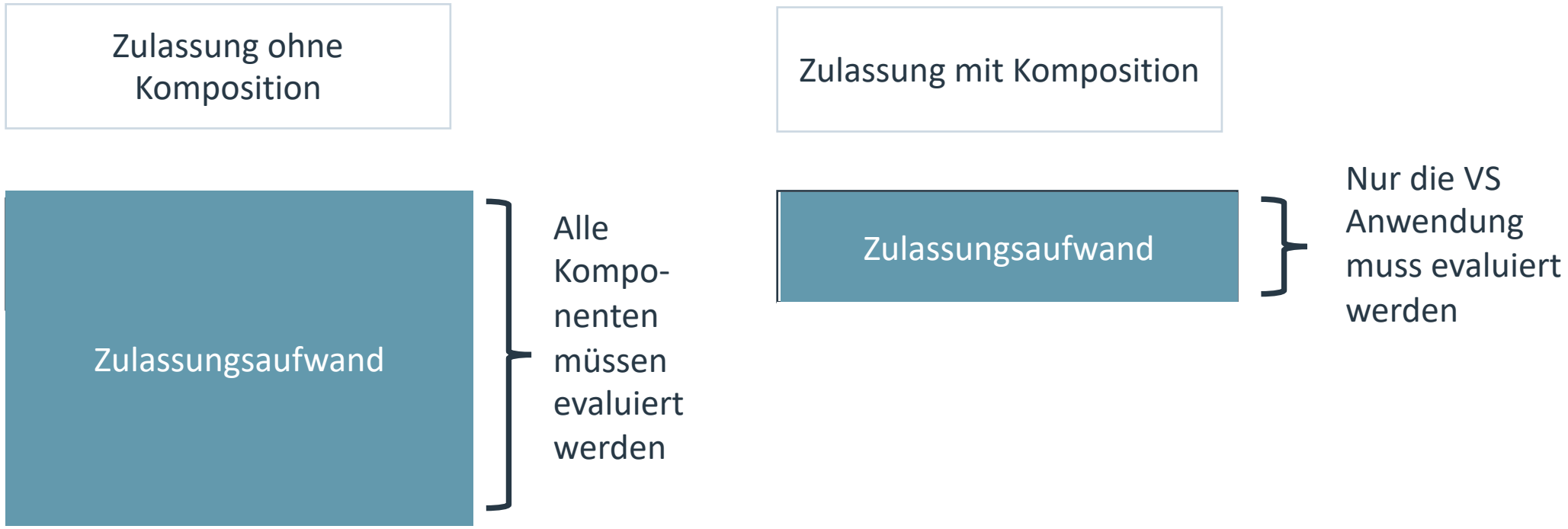
L4Re SSK

+ Technologie
+ Dokumente
  - ST, Guidance, SecOps
+ Support
+ Wiederverwendung ohne neue Evaluation

Zulassungsaufwand und Komposition



Zulassungsaufwand und Komposition



KOMPOSITIONSANSATZ

02

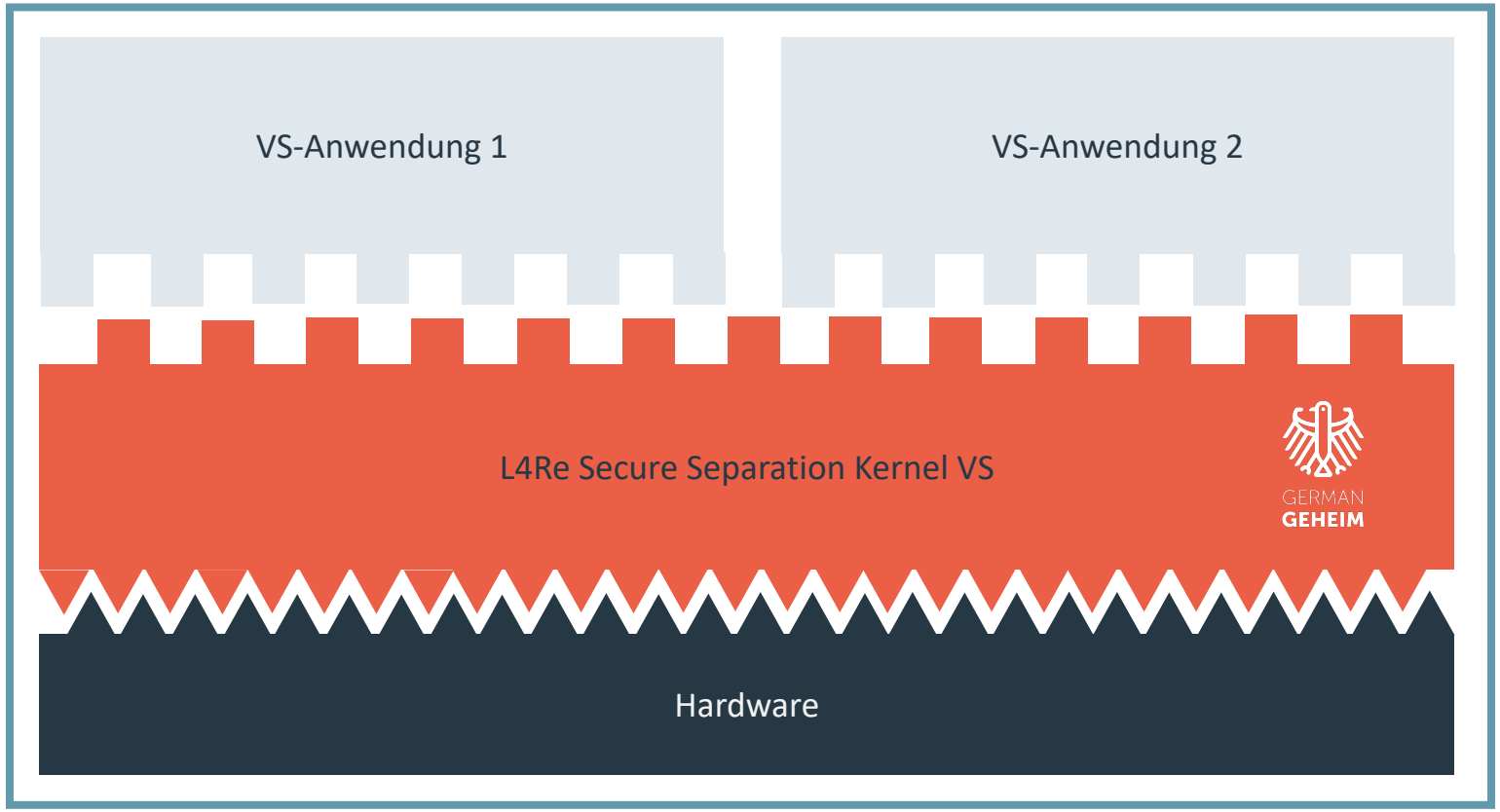
Kompositionsansatz

- Typischerweise ist die Plattform die Hardware
  - Inkl. der notwendigen Softwareanteile (z.B. Firmware)
- Evaluierte Sicherheitsfunktionen der Plattform müssen bei der Evaluierung des Kompositionsprodukts nicht erneut betrachtet werden
- Anleitung zur Komposition
  - ETR for Composition

Kompositionsprodukt

Applikation

Plattform



Anleitung zur Komposition

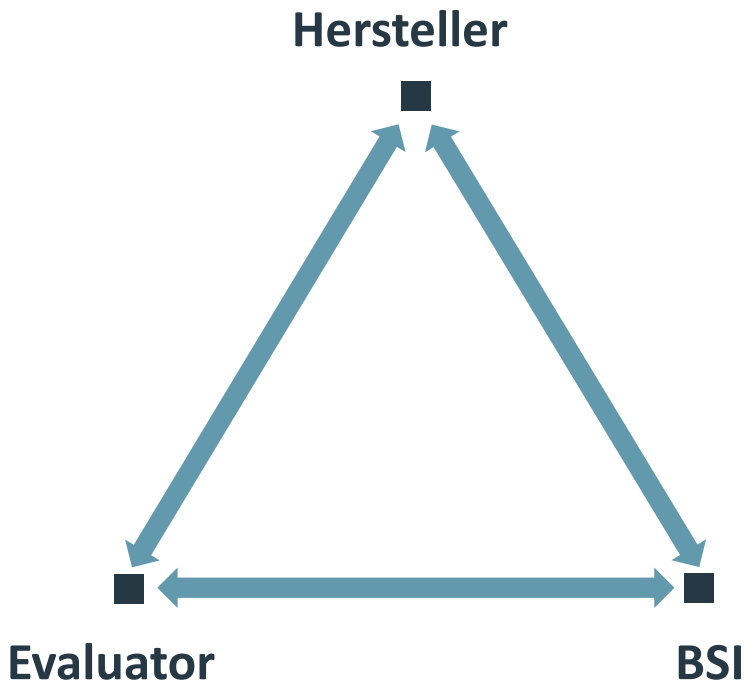
- ETR for Composition
  - Erstellung aufwändig
- Anleitung für den Evaluator
  - Keine über den EfC hinausgehenden Prüfungen notwendig

Alternativen

- ✚ Sicherheitsfunktionen der Plattform jedes mal erneut evaluieren
  - Hersteller muss Informationen bereitstellen auf die er u.U. keinen Zugriff hat
- ✚ Hersteller hat u.U. keine Informationen über die sichere Integration der Plattform
  - Wie soll der Evaluator prüfen?

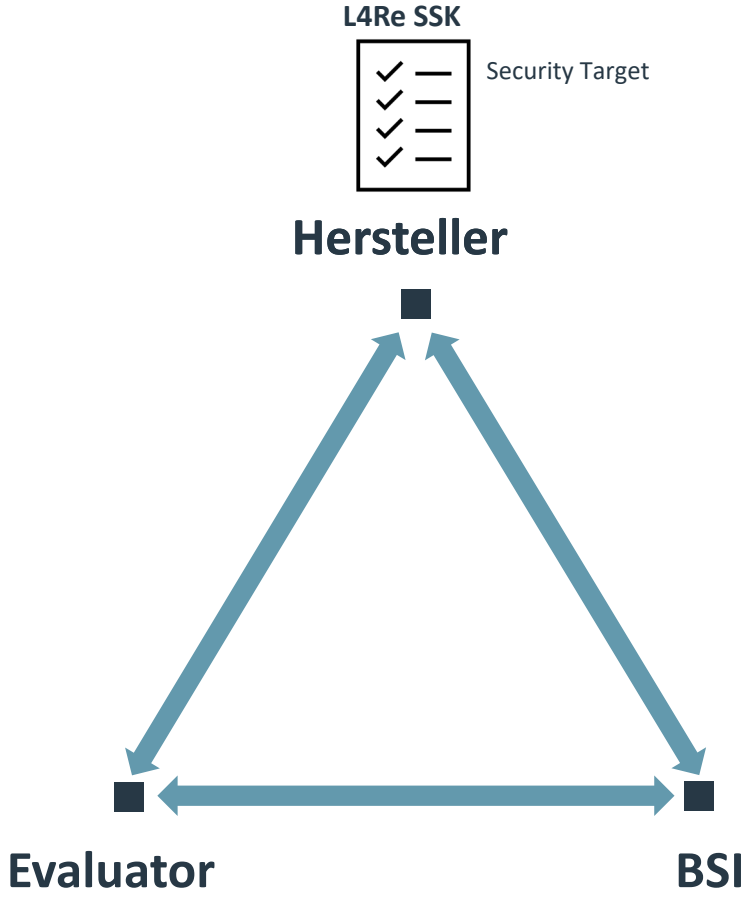
KOMPOSITION MIT L4RE SSK

03



Security Target

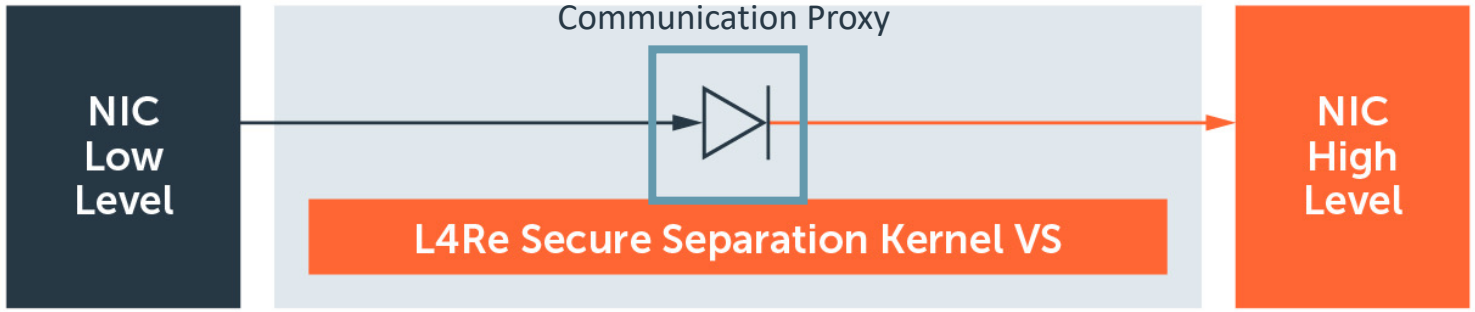
- Übersicht TOE
- Input für eigenes ST
  - Nutzung der Sicherheitsfunktionen

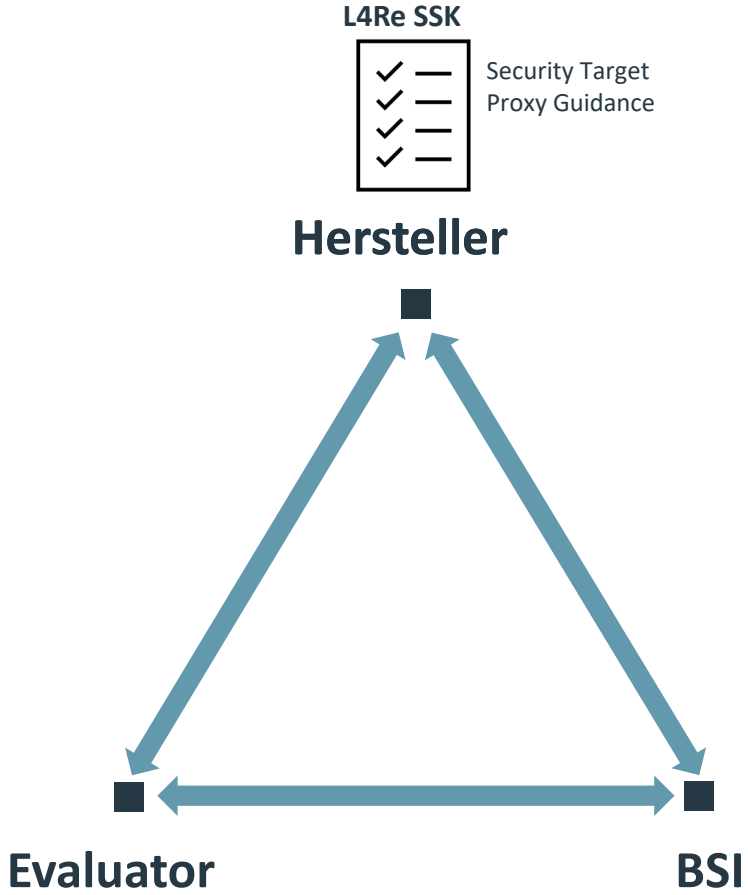


Proxy Guidance

- Flexible Erweiterung des L4Re SSK
- Anleitung
- Komponenten werden vom Evaluator dagegen geprüft

Beispiel: Datendiode





Configuration Guidance

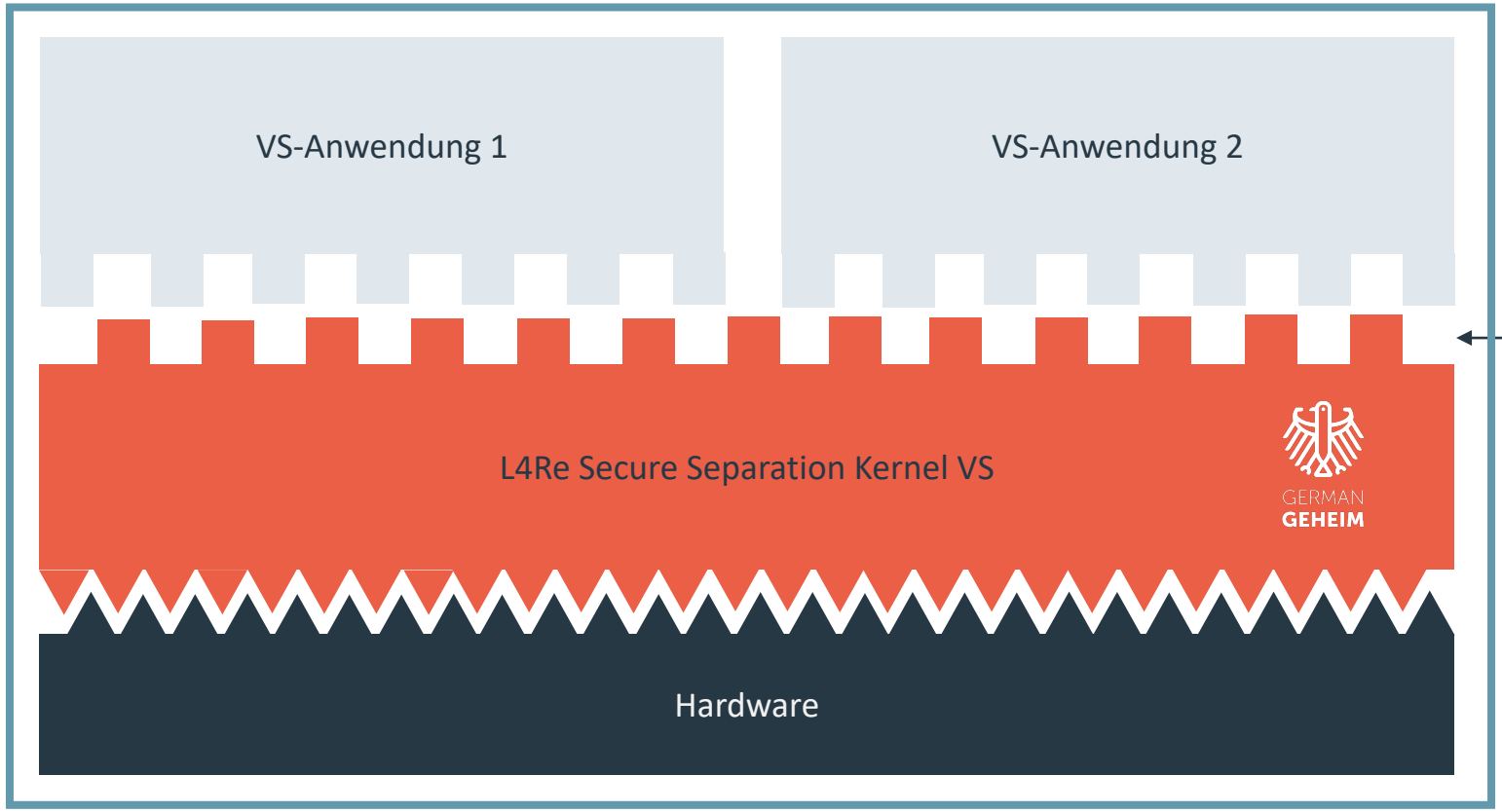
+ Konfiguration

+ Sichere Verwendung

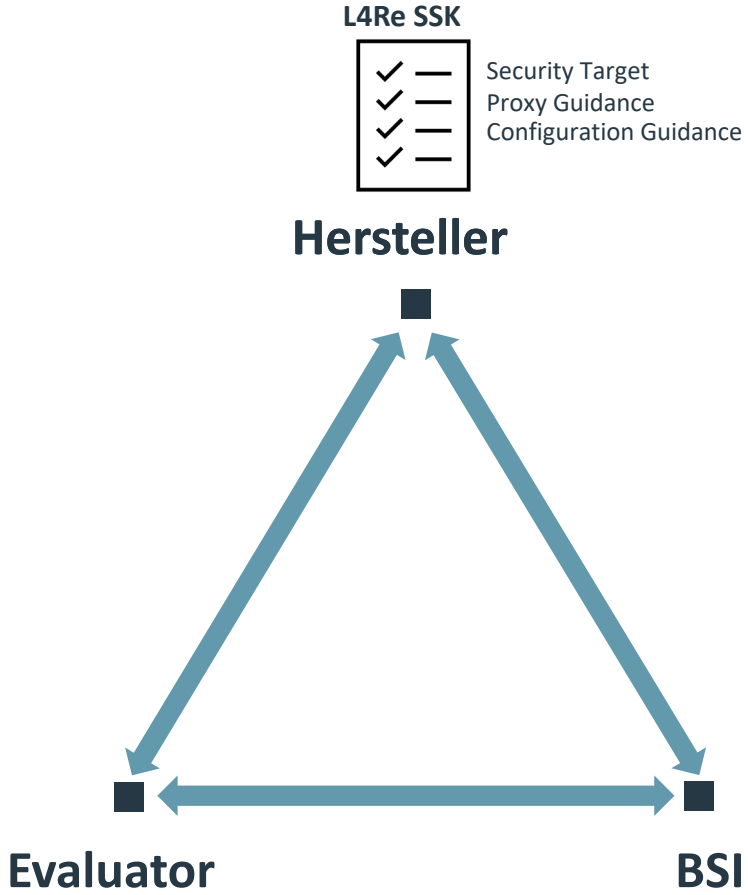
Kompositionsprodukt

Applikation

Plattform

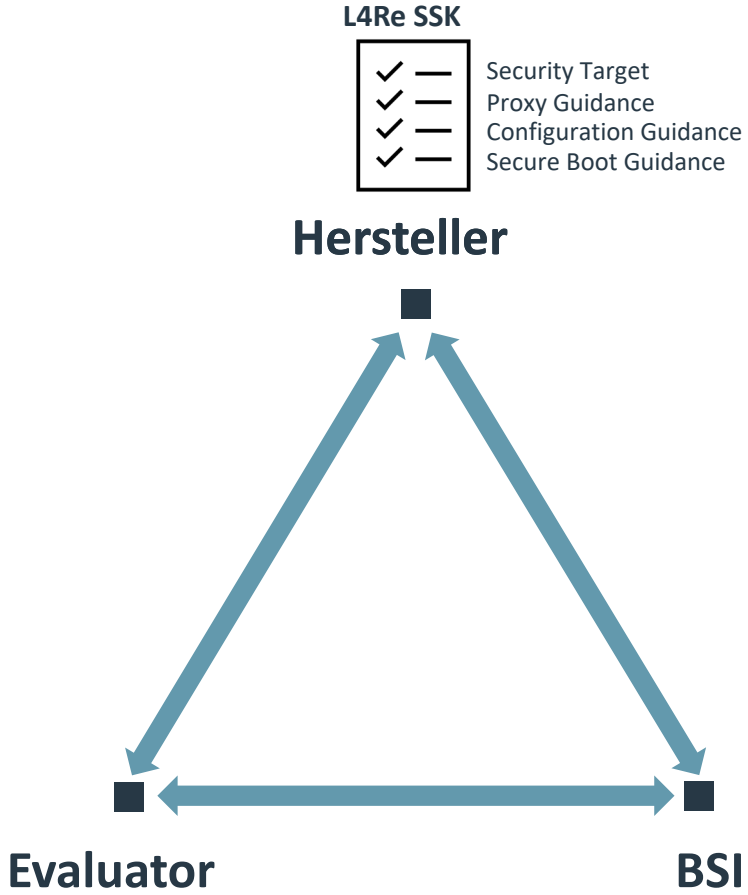


Anwendung der Configuration und Proxy Guidance



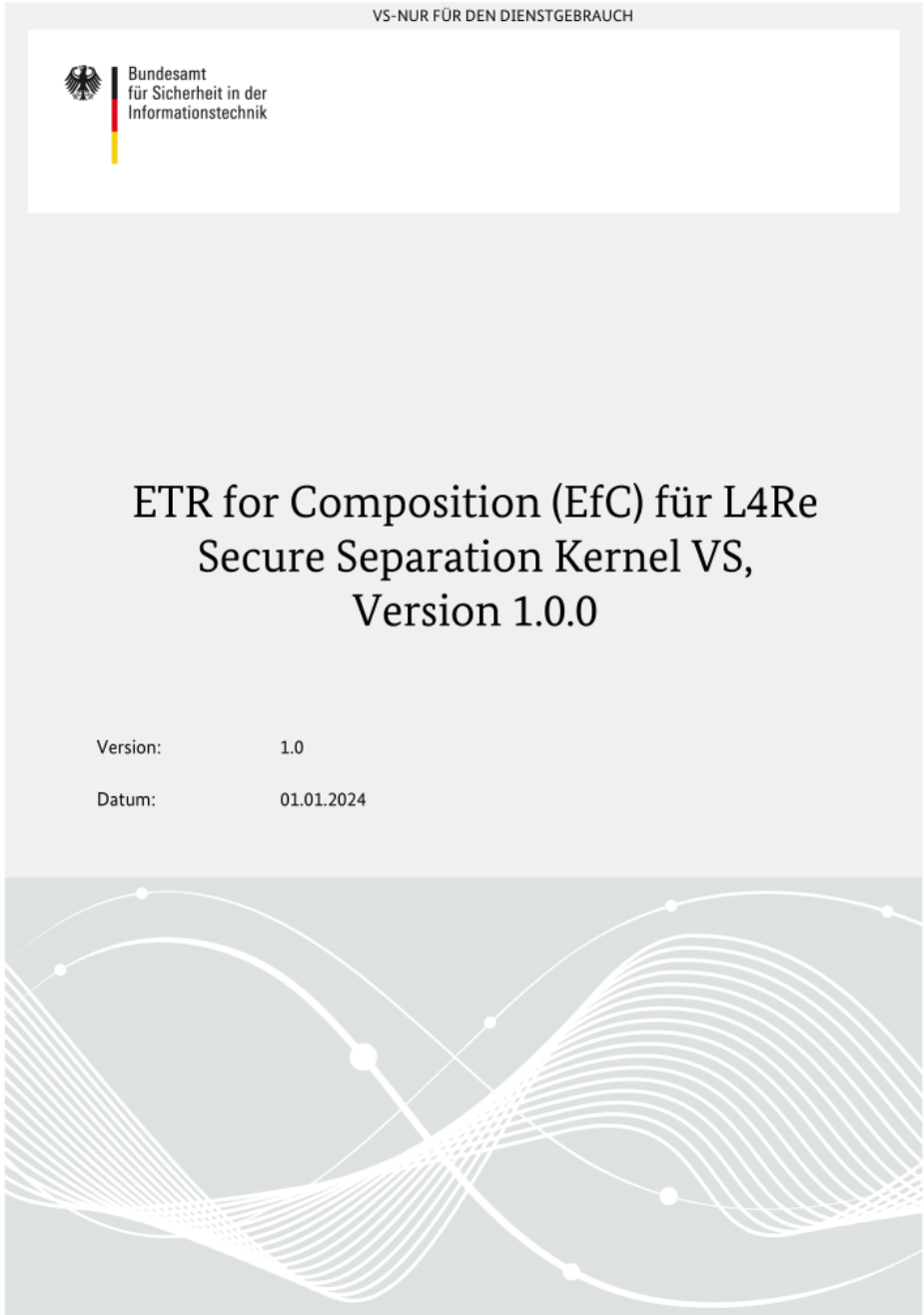
Secure Boot Guidance

- Integrität und Authentizität des Produkts
- Teil der Sicherheitsfunktion der Plattform



SecOps

- Anforderungen an die Umgebungs- und Einsatzbedingungen
- ETR for Composition


VS-NUR FÜR DEN DIENSTGEBRAUCH
Bundesamt
für Sicherheit in der
Informationstechnik
ETR for Composition (EfC) für L4Re
Secure Separation Kernel VS,
Version 1.0.0
Version: 1.0
Datum: 01.01.2024

VORTEILE FÜR HERSTELLER

04

Vorteile für Hersteller

- Freie Wahl der Prüfstelle für ihre Anwendung
- Senkung des Zulassungsrisikos
- Zeit- und Kostenersparnis
- Effizientere Ressourcennutzung

KOOPERATION GEWINNT

VIELEN DANK!

www.kernkonzept.com
matthias.lange@kernkonzept.com

www.atsec.com
mvogel@atsec.com