Informations
Technik
Zentrum Bund

LISSA

LISSA

Lieferkette **I**TZBund für **S**ichere **S**oftw**A**re

Beitrag zum eGovernment
Wettbewerb 2026

Motivation

Cloud, KI, Cyber-Sicherheit und digitale Souveränität führen zu großen Veränderungen in der Entwicklung und dem Betrieb von Fachverfahren für die Verwaltung.

Softwarelieferketten rücken dabei immer stärker in den Fokus – zum einen, um Souveränität über den Entwicklungsprozess zu behalten, zum anderen nehmen „Supply Chain Angriffe“ exponentiell zu.

Vor diesen Herausforderungen steht nicht nur das ITZBund, das mehr als 1.400 Fachverfahren für die Bundesverwaltung betreibt, sondern die gesamte Verfahrensentwicklung in der öffentlichen Verwaltung.

Das ITZBund entwickelt mit LISSA, der „Lieferkette ITZBund für Sichere Software“, ein Standardprodukt zum Aufbau von automatisierten und sicheren Softwarelieferketten für die Bundesverwaltung.

LISSA im Kontext

Standardisierter und automatisierter Lieferweg für Individualentwicklung von Fachverfahren

LISSA prüft auf:

- Schwachstellen
- Schadcode
- Softwarequalität
- Compliance-Richtlinien

Warum LISSA?

Sicherheit

LISSA stoppt viren- oder schwachstellenbehaftete Software bereits bei der Einlieferung, bevor sie abgesicherte Betriebszonen erreicht. Durch wiederholte Sicherheitsprüfungen wird das Zero-Trust-Prinzip umgesetzt, da keiner Quelle blind vertraut wird.

01

Souveränität & Standardisierung

Die Software wird in geschützten ITZBund-Umgebungen gebaut, für volle Kontrolle und Transparenz. Die Nutzung von LISSA verpflichet die Softwareentwicklung auf Einhaltung von Sicherheits- und Qualitätsstandards und gewährleist eine kontinuierliche Überprüfung.

02

Effizienz

LISSA beschleunigt die Softwareentwicklung durch Automatisierung und unterstützt die Entwicklungsteams mit direktem Feedback und Security Reports. Ein Dashboard bietet eine Übersicht über verfahrensspezifische Quality Gates.

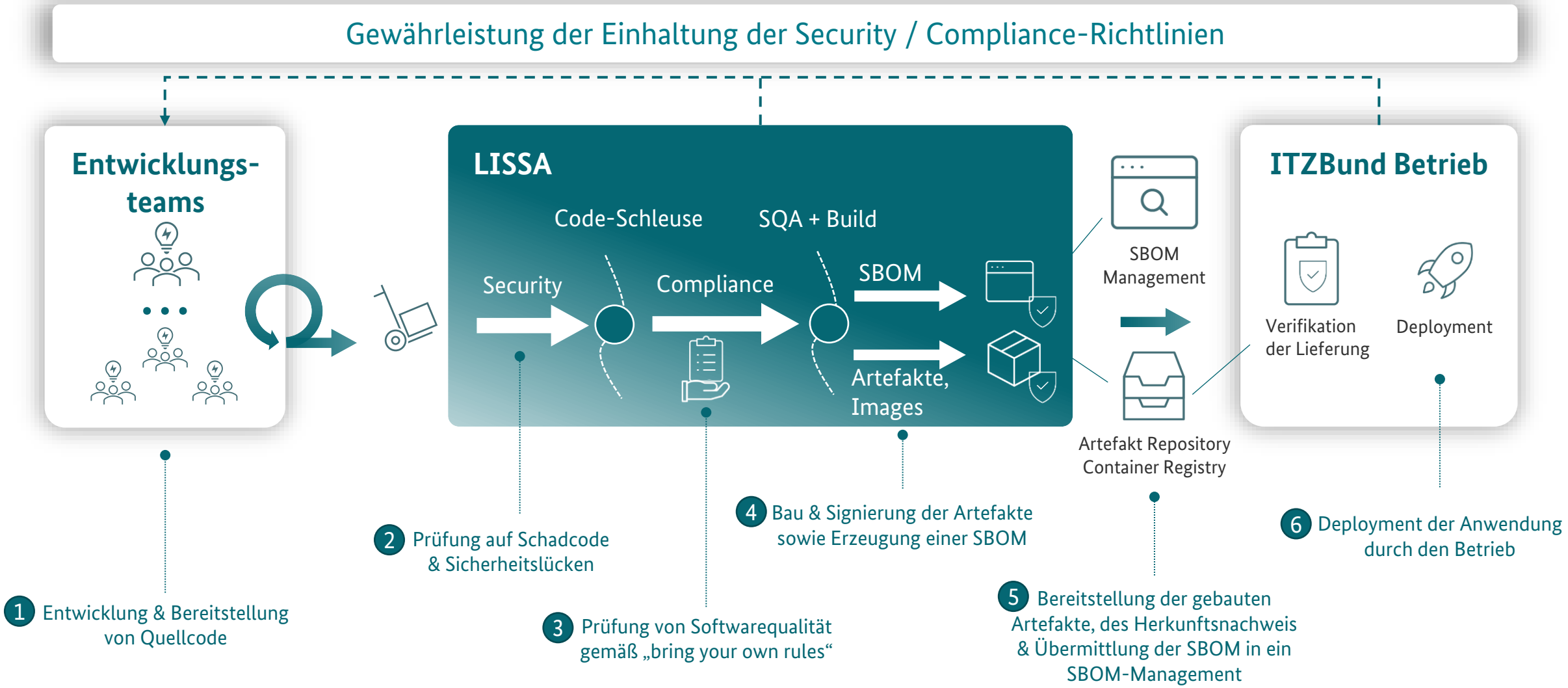
03

Stabilität

Signierte Artefakte und SBOMs ermöglichen eine lückenlose Nachvollziehbarkeit. Von Sicherheitslücken betroffene Anwendungen können schnell identifiziert und gepatcht werden. Das erhöht die Qualität, die IT-Sicherheit und die Betriebsstabilität.

04

Wie funktioniert LISSA?



Wie funktioniert LISSA?

1

Entwicklungsteams entwickeln in ihrem Zyklus und ihren Umgebungen Software für Fachverfahren gemäß vorgegebener Compliance-Richtlinien. Zum Lieferzeitpunkt stellen Sie den Quellcode sowie die Build-Vorschriften zur Einlieferung bereit.

2

Die Codeschleuse, verortet in einer DMZ, holt den Quellcode bei Änderungen automatisiert ab und prüft ihn auf Schadcode und Sicherheitslücken. Kritische Befunde führen zum sofortigen Abbruch der Lieferkette

3

Die SQA-Build-Komponente zieht den geprüften Quellcode von der Code-Schleuse in die geschützte Betriebs-umgebung. Sie führt Sicherheitsprüfungen erneut durch, sowie eine automatisierte Softwarequalitätsanalyse (SQA). Die SQA-Prüfregeln können durch die Behörde selbst festgelegt werden.

4

Aus dem Quellcode werden gemäß der mitgelieferten Build-Vorschriften Softwareartefakte (Compilate) und Container-Images erzeugt. Zusätzlich wird eine Software Bill of Material (SBOM) generiert und der Lieferprozess protokolliert.

5

Die gebauten Artefakte werden signiert und in einem geschützten Repository, bzw. einer geschützten Registry dem Betrieb zur Verfügung gestellt. Dem Betrieb wird ein Herkunftsnachweis des gebauten Artefakt zur Verfügung gestellt. Die SBOM wird in eine SBOM-Verwaltung abgelegt.

6

Die gebauten Artefakte können über automatisierte Deployment-Prozesse automatisiert aus den geschützten Repositories/Registries abgeholt und nach weiteren betrieblichen Sicherheitsprüfungen auf die gewünschten Zielumgebungen ausgerollt werden.

LISSA unterstützt regulatorische Vorgaben!

SBOM – Transparenz über Softwarebestandteile

- Maschinenlesbare Stückliste der in einer Software enthaltenen Komponenten
- unterstützt die schnelle Identifikation von Schwachstellen und betroffene Produkte
- wird durch den Cyber Resilience Act gefordert; das BSI konkretisiert die Anforderungen über die Technische Richtlinie TR-03183-2

Provenance – Nachweis der Softwareherkunft

- Dokumentiert, woher ein Software-Artefakt stammt und wie es erstellt wurde
- Macht den Lieferprozess für Audits und Prüfungen nachvollziehbar

LISSA stellt beides automatisiert bereit!

LISSA sichert ab!

Zero Trust

durch Security-Prüfungen in beiden Komponenten & damit beiden Schutzzonen

Transparenz über Sicherheitslücken

zur Steigerung der Reaktionsfähigkeit

Quarantäneprozess

bei Fund von Schadcode oder Sicherheitslücken und Stopp der Einlieferung

Protokollierung sicherheitsrelevanter Ereignisse

zur zentralen Analyse durch ein Security Operations Center (SOC)

Sicherstellung der Integrität & Herkunft

um die Software auf dem Lieferweg vor Kompromittierung zu schützen

LISSA skaliert! LISSA ist erweiterbar!

Moderne Cloud-Infrastrukturen

Der Aufbau von LISSA mit Containern & Kubernetes ermöglicht eine automatische Skalierung und Aktualisierung der Softwarelieferkette.

Modularer Aufbau

LISSA prüft automatisiert verbindliche Sicherheits- und Qualitätsvorgaben bei jeder Lieferung. Behörden können dabei flexibel ihre eigenen Prüfkriterien integrieren.

Die Lieferkette ist modular - zusätzliche Prüfschritte können einfach in LISSA aufgenommen werden.

Mehrwert von LISSA

- Schutz vor Supply Chain Angriffen
- Security by Design
- Standardisierung und Digitale Souveränität
- Effizienz durch Automatisierung
- Steigerung der Produktivität

LISSA wird genutzt!

Pilotierung seit 6 Monaten mit verschiedenen Fachverfahren

hohe Nachfrage bei Fachverfahren

Produktaufbau läuft

Interesse bei Kundenbehörden wie BVA, BMF und BSI

Informations
Technik
Zentrum Bund

LISSA

Vielen Dank

Wir freuen uns auf Ihre Stimme!

Beitrag zum eGovernment
Wettbewerb 2026

Disclaimer

Die Rechte dieser Präsentation liegen beim ITZBund. Eine Nutzung dieser Präsentation ist nur für den Kreis der Teilnehmerinnen und Teilnehmer bestimmt.

Eine Veröffentlichung oder eine sonstige Verwertungshandlung im Sinne des §15 UrhG darf nicht erfolgen. Darüber hinausgehende Nutzungen bzw. Weiterverwendungen der Präsentation bedürfen der schriftlichen Genehmigung des ITZBund.

Jegliche Form der Nutzung, Vervielfältigung, Modifizierung, Speicherung, Veröffentlichung und Darstellung des dargestellten Bild- und Iconmaterials außerhalb dieser Präsentation ist nicht gestattet. Der überwiegende Teil des zur Verfügung gestellten Bildmaterials stammt aus Rahmenvereinbarung mit Getty Images Deutschland GmbH und 123RF Limited. Für die Bereitstellung von Bild- und Iconmaterial steht Ihnen das Team der Presse- und Öffentlichkeitsarbeit im ITZBund zur Verfügung (pressestelle@itzbund.de).