

Konsultationsverfahren Deutschland-Stack – Einreichung Forum Sovereign Cloud Stack-Standards der Open Source Business Alliance e.V.

Im Leitbild des Deutschland-Stacks wird Souveränität, Interoperabilität und europäische Anschlussfähigkeit adressiert. Passend dazu wurde von der EU Kommission gerade das [EU Cloud Sovereignty Framework¹](#) veröffentlicht.

Daher ist es im Sinne des Deutschland-Stacks naheliegend, auf interoperable Komponenten und Schnittstellen zu setzen, deren Interoperabilität durch Standards und deren Konformitätstests sichergestellt und verifiziert wird. Das ursprünglich vom Bundesministerium für Wirtschaft und Klimaschutz geförderte Projekt *Sovereign Cloud Stack (SCS)* hat *zertifizierbare*, und dementsprechend *verifizierbare*, Standards für interoperable Cloud-Infrastrukturen entwickelt. Die kontinuierliche Weiterentwicklung und Steuerung dieser Standardisierung ist, im Nachgang zum Förderprojekt, durch das im neutralen Rahmen der OSBA e.V. im Zusammenspiel mit der [SCS-Community](#) sichergestellt. Im Rahmen des Förderprojektes wurde auch eine modulare, Open Source Referenzimplementierung entwickelt². Neben dieser schlüsselfertigen Lösung ist in den letzten Jahren ein Ökosystem an Software Lösungen, die die SCS-Standards implementieren, entstanden.³

Der Deutschland-Stack sollte auf vom Bund finanzierte, bereits etablierte Standards zurückgreifen. Die SCS-Standards bieten genau das für souveräne Cloud-Infrastrukturen, weshalb wir in dieser Einreichung eine Positionierung des SCS im Kontext der Kriterien des Deutschland-Stack vornehmen. Diese Einreichung versteht sich auch im Kontext der [Stellungnahme der Open Source Business Alliance](#), daher werden Punkte die dort aufgegriffen werden, hier nicht wiederholt.

In der Betrachtung der Schichten des Tech-Stacks zählt SCS auf die Schichten [Plattform](#) > Integration und [Strategie, Architektur und Governance](#) ein.

Digitale Souveränität

Der SCS setzt digitale Souveränität in die Praxis um, indem er offene Standards, Open-Source-Implementierungen und transparente Betriebspraktiken kombiniert. Er vereinfacht die Bereitstellung sicherer und qualitativ hochwertiger Cloud-Dienste, reduziert Abhängigkeiten und fördert die Zusammenarbeit. SCS gewährleistet die Einhaltung europäischer Datenschutzstandards wie der DSGVO.

SCS definiert 4 Stufen der Digitalen Souveränität⁴, welche mit den SCS-Zertifizierungsleveln einher gehen:

Stufe der digitalen Souveränität	SCS Konformität
1: Einhaltung von Rechtsvorschriften (DSGVO)	1: ENISA/Gaia-X Kennzeichnungen & rechtliche Regelungen (nicht SCS-spezifisch)
2: Wahlmöglichkeit zwischen vielen Anbietern, In-Sourcing-Option (On-Premise)	2: "SCS-compatible" – technische Kompatibilität (Konformitätstests bestanden: CNCF, OIF, SCS)

1 Vgl. Kommentierung des EU Souveränitäts Framework durch SCS: <https://sovereigncloudstack.org/de/announcements/euSovCloud/>

2 <https://github.com/sovereignCloudStack/>

3 Vgl. z.b. YAOOK als gutes Beispiel: <https://alasca.cloud/projects/yaook/>

4 Erschienen u.a. in „Datenschutz und Datensicherheit“ - [Link](#)

3: Technologische Transparenz und Fähigkeit zur Mitwirkung und Gestaltung	3: "SCS-open" – SBOM für funktionalen Stack verfügbar und vollständig OSS (4 Opens)
4: Operative Transparenz und verfügbares Wissen (Kompetenzaufbau)	4: "SCS-sovereign" – Ops/IAM stacks sind OSS sowie transparent bei Monitoring und Incidents, Mitwirkung an OpenOperations (5 Opens)

Diese differenzierte Betrachtung ermöglicht den Einsatz einer breiten technologischen Basis, wobei hier deutlich zu sagen ist, dass Open Source Software die Grundlage für digitale Souveränität ist, denn sie stellt sicher, dass die Systeme, die im Rahmen des Deutschland-Stack verwendet werden, überprüfbar, gestaltbar und ersetzbar sind.

Interoperabilität

Interoperabilität in Cloud-Infrastrukturen ist bereits gewährleistet, wenn diese die SCS-compatible-Standards⁵ erfüllen. Durch den Einsatz von offenen, standardisierten Schnittstellen wird eine technische Kompatibilität geschaffen, die notwendige Basis für eine Wahlfreiheit zwischen verschiedenen Anbietern, die auch die Möglichkeit des In-Sourcings (On-Premise-Betriebs) sichergestellt. Die SCS-Standards erstrecken sich von der Infrastructure-as-a-Service⁶ (IaaS) Schicht, über Kubernetes-as-a-Service⁷ (KaaS), zu *Identity and Access Management (IAM/IDAM)* sowie den operationalen Teil. Hierbei werden bestehende Standards und in der Industrie anerkannte Best-Practices aufgegriffen. Kubernetes selbst bswp. ist schon ein umfangreicher Industrie-Standard. Durch die SCS Standards auf der KaaS Ebene, werden Aspekte abgedeckt, die Kubernetes von Haus aus nicht abdeckt (beispielsweise die Node Distribution und Verfügbarkeit⁸). Die Praxisnähe der Standards wird durch die erprobten Implementierungen, die durch die Unternehmen in der SCS Community entwickelt werden, gestützt (vgl. auch Abschnitt: Marktreife). Für Greenfield-Szenarien wie auch als einzelne Bausteine bietet sich Software aus dem SCS Ökosystem an. Der Stack soll die Vernetzung und den Datenaustausch auf einer gemeinsamen digitalen Infrastruktur zwischen Stakeholdern auf verschiedenen Ebenen ermöglichen. Das SCS Projekt hat sich nicht nur Infrastructure-as-a-Service (IaaS) und Kubernetes-as-a-Service (KaaS) angeschaut, sondern das in einem Gesamtkontext im Verbund mit *Identity and Access Management (IAM/IDAM)* betrachtet. Hierbei ist ein Architektur Blueprint⁹ entstanden, der auch in [GovStack](#) übernommen wurde. Dieses Zusammenspiel von Standard-Komponenten kann in eine Referenzarchitektur einfließen, die im Rahmen des Deutschland-Stack als Beispielumsetzung an die Hand gegeben werden kann

Zukunftsfähigkeit

[Sovereign Cloud Stack](#) (SCS) war ein Projekt der [Open Source Business Alliance e.V.](#) (OSBA), welches von 2021 bis 2024 durch das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) mit ursprünglich 14,9 Mio. EUR gefördert wurde. Die Weiterführung nach dem Förderzeitraum, mittels der Finanzierung von Unternehmen aus dem entstandenen Ökosystem, unterstreicht die Traktion und Relevanz der entstandenen Standards und Implementierungen. Die Weiterführung durch Unternehmen aus dem im Projekt entstandenen Ökosystem nach Ende der Förderung zeigt den Stellenwert und Nachhaltigkeit der SCS-Standards und deren Implementierungen. Die Weiterentwicklung der [SCS-Standards](#) wird durch das [Forum SCS-Standards](#) im neutralen Rahmen der OSBA gesteuert und von Unternehmen innerhalb der [SCS-Community](#) fortgeführt.

Die Standardisierung im Rahmen von SCS ist ein offener Prozess zu dem nicht nur Stakeholder eingeladen sind – vielmehr wird im Rahmen dieses Prozesses aktiv auf relevante Akteure zugegangen um deren Bedürfnisse zu

⁵ Einstiegsseite in die SCS Standardisierung: <https://docs.scs.community/standards>

⁶ Infrastructure-as-a-Service Standards: <https://docs.scs.community/standards/iaas/>

⁷ Kubernetes-as-a-Service Standards: <https://docs.scs.community/standards/kaas/>

⁸ Vgl. <https://docs.scs.community/standards/scs-0214-v2-k8s-node-distribution/>

⁹ <https://cloud.govstack.global>

erfahren und deren Sichtweisen zu berücksichtigen. Unterstrichen wird dies durch die starke Kooperation mit z.B. [ALASCA e.V.](#) und der Einladung in die IG BvC („Interessengemeinschaft Betrieb von Containern“).

Die Adaption der SCS-Standards in mehreren Implementierungen am Markt unterstreicht, dass diese nicht auf eine konkrete Implementierung zugeschnitten sind. Neben der im Förderprojekt entstandenen Referenzimplementierung¹⁰ sind auf der Infrastrukturebene beispielsweise YAOOK¹¹ oder auch OpenStack vanilla Clouds voll standardisiert im Einsatz.

Marktrelevanz

Bereits während des Projektes an sich hat am Markt eine Akzeptanz der SCS-Standards stattgefunden und es wurden sowohl von privatwirtschaftlichen Akteuren wie auch der öffentlichen Hand Angebote auf Basis dieser Standards und mit Software aus dem SCS Ökosystem aufgebaut. Beispiele für die Adaption sind:

- [Thüringer Verwaltungscloud des Thüringer Landesrechenzentrums](#)
- [BayernCloud Schule \(BayCS\)](#) – BayCS läuft auf bei Plusserver auf der „pluscloud open“, eines der ersten kommerziellen SCS Angebote am Markt.
- [Regionales Rechenzentrum Erlangen \(RRZE\) der FAU Erlangen-Nürnberg](#)
- [SCS Rechenzentrum für das 5G Campusnetzprojekt Hochschule Osnabrück¹³](#)

In weiteren Fällen wurden die SCS-Standards von existierenden Angeboten am Markt umgesetzt oder zusätzlich implementiert.¹⁴

Im Kontext des Deutschland-Stack relevanter ist jedoch die Einbettung der SCS-Standards in Referenzarchitekturen wie bspw. die „Building Block Specification for Cloud Infrastructure“ von GovStack.

Es bestehen bereits umfassende Trainings- und Schulungsangebote zum Sovereign Cloud Stack – von grundlegenden Einführungen in SCS und die zugehörigen Standards bis hin zu Schulungen zum Aufbau individueller Cloud-Infrastrukturen auf Basis der modularen Referenzimplementierung. Diese richten sich insbesondere an Cloud-Betreiber und Integratoren. Darüber hinaus ist vorgesehen, künftig auch die Anbieter dieser Schulungen im Rahmen eines eigenen Zertifizierungsverfahrens zu akkreditieren.

Vertrauenswürdigkeit

Konsequenterweise setzt Vertrauenswürdigkeit voraus, dass die eingesetzten technologischen Komponenten quelloffen sind und Transparenz über eine Software Bill of Material (SBOM) hergestellt wird. Im Zusammenspiel mit offenen Standards und offenen Schnittstellen wird so eine größtmögliche Auditierbarkeit und Nachvollziehbarkeit hergestellt. Im Rahmen des SCS Förderprojektes wurde auch im Bereich Supply Chain Security gearbeitet. Für viele der Softwarekomponenten aus dem SCS Ökosystem werden SBOMs bereitgestellt und die Entwicklungsprozesse durch Best-Practices abgesichert.

Nachhaltigkeit

Die Nachhaltigkeit des Sovereign Cloud Stack und dessen Standards zeigt sich in der erfolgreichen Fortführung über die Förderphase hinaus und im Aufbau eines stetig wachsenden, offen zugänglichen Ökosystems mit

¹⁰ Vgl. auch die Einreichung von OSISM: <https://gitlab.opencode.de/dstack/d-stack-home/-/issues/257>

¹¹ Vgl. Einreichung von Dr. Daniel Gerber: <https://gitlab.opencode.de/dstack/d-stack-home/-/issues/229>

¹² Vgl. Einreichung von Cloud&Heat: <https://gitlab.opencode.de/dstack/d-stack-home/-/issues/300>

¹³ Vgl. Projektseite vom 5G Campusnetzprojekt: <https://hs-osnabrueck.de/i40>

¹⁴ <https://scs.community/2024/05/13/cost-of-making-an-openstack-cluster-scs-compliant/>

neutraler Governance-Struktur. Damit ist der langfristige Betrieb unabhängig von einzelnen Anbietern oder Projekten gesichert.

Zertifizierbare Standards gewährleisten eine kontinuierliche Qualitätssicherung und fördern die langfristige Interoperabilität zwischen unterschiedlichen Cloud-Infrastrukturen.

Ein zentraler Bestandteil der SCS-DNA ist der konsequente Einsatz von Open Source. Sämtliche Standards, Prozesse, Software-Komponenten sowie Trainings- und Schulungsmaterialien¹⁵ sind unter von der OSI anerkannten Open-Source-Lizenzen frei verfügbar. Diese Offenheit ermöglicht Nachvollziehbarkeit, Wiederverwendung und gemeinschaftliche Weiterentwicklung – zentrale Prinzipien nachhaltiger digitaler Infrastruktur.

Conclusio

Die SCS-Standards und seine implementierten Komponenten bieten eine erprobte, offene und zertifizierbare Grundlage für den Aufbau souveräner und interoperabler Cloud-Infrastrukturen. Sie schaffen damit die technische und organisatorische Basis, um die Ziele des Deutschland-Stacks – Souveränität, Interoperabilität und europäische Anschlussfähigkeit – wirksam umzusetzen.

Zur Vertiefung des Themas wird ein Workshop zum Schwerpunkt Interoperabilität mit zertifizierbaren Standards empfohlen, in dem der praktische Einsatz der SCS-Standards im Deutschland-Stack näher beleuchtet werden kann.

¹⁵ <https://sovereigncloudstack.org/de/announcements/scs-training-material/>