Sovereign Cloud Stack

Sovereign Cloud Stack

Zertifizierbare Standards für digital souveränes Cloud-Computing

Felix Kronlage-Dammers – fkr@osb-alliance.com

OSBA

sovereigncloudstack.org

Sovereign Cloud Stack

OpenBSD

freifunk.net

Open Source for fun and (non-)profit.

gridscale

Sea-Watch.org

ECO DIGIT

bytemine

guug
German Unix User Group

OSBA

Felix Kronlage-Dammers
fkr@osb-alliance.com

Open Source Business Alliance

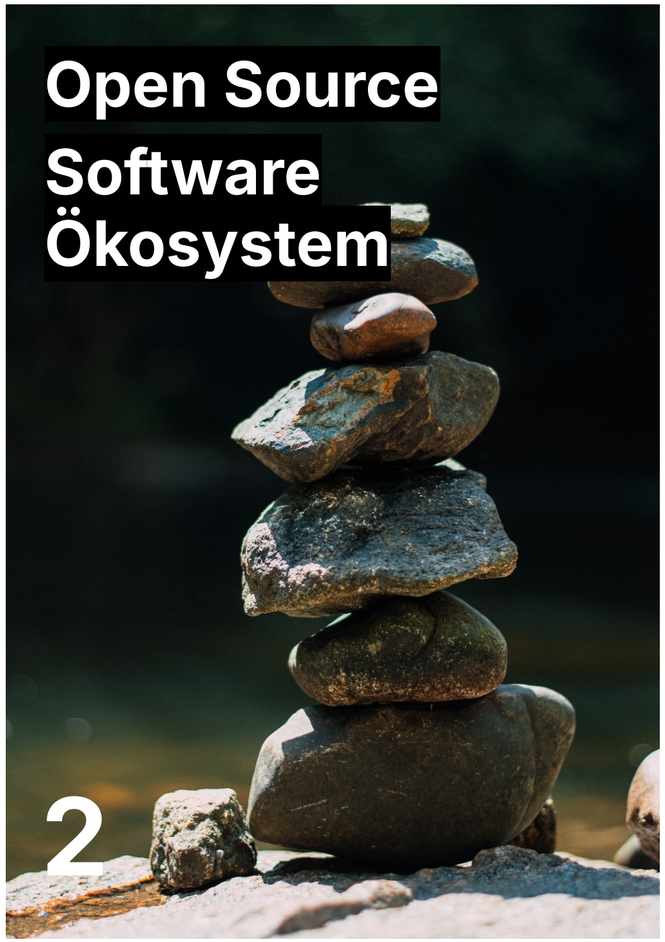

Sovereign
Cloud Stack

Sovereign Cloud Stack

Sovereign Cloud Stack (SCS) ist eine europäische Initiative, die ein offenes, transparentes und anbieterneutrales Cloud-Ökosystem schafft, das Souveränität und Interoperabilität gewährleistet.

OSBA

Sovereign Cloud Stack – Erzeugnisse



Sovereign Cloud Stack

„Digitale Souveränität ist Handlungsfähigkeit“

„Unser Staat ist in hohem Maße abhängig von wenigen großen Techkonzernen, ein ernstzunehmender Kontrollverlust über die staatliche IT ist die Folge.“

(ZenDiS)

OSBA

https://www.zendis.de

Sovereign Cloud Stack

„Digitale Souveränität“ beschreibt „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“.

(IT-Planungsrat)

OSBA

https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf

Datensouveränität != Digitale Souveränität

SAP und Arvato versprechen "souveräne" Microsoft-Cloud für Behörden

Die beiden deutschen Konzerne wollen Clouddienste von Microsoft für den öffentlichen Sektor bereitstellen. So sollen Behörden die Dienste sicher nutzen können.

Lesezeit: **3 Min.** In Pocket speichern 85

(Bild: Gorodenkoff / shutterstock.com)

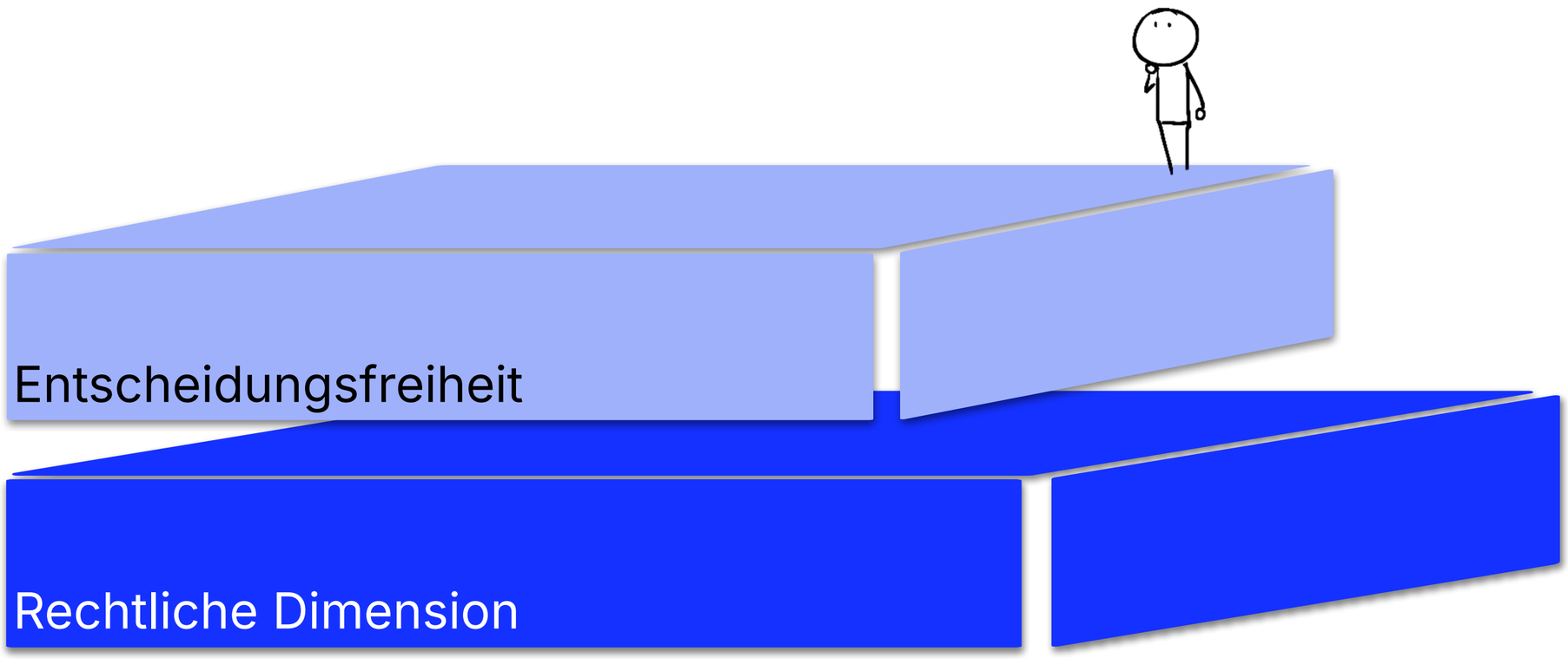
https://www.heise.de/news/SAP-und-Arvato-versprechen-souveraene-Microsoft-Cloud-fuer-Behoerden-6346760.html

Sovereign Cloud Stack

Rechtliche Dimension

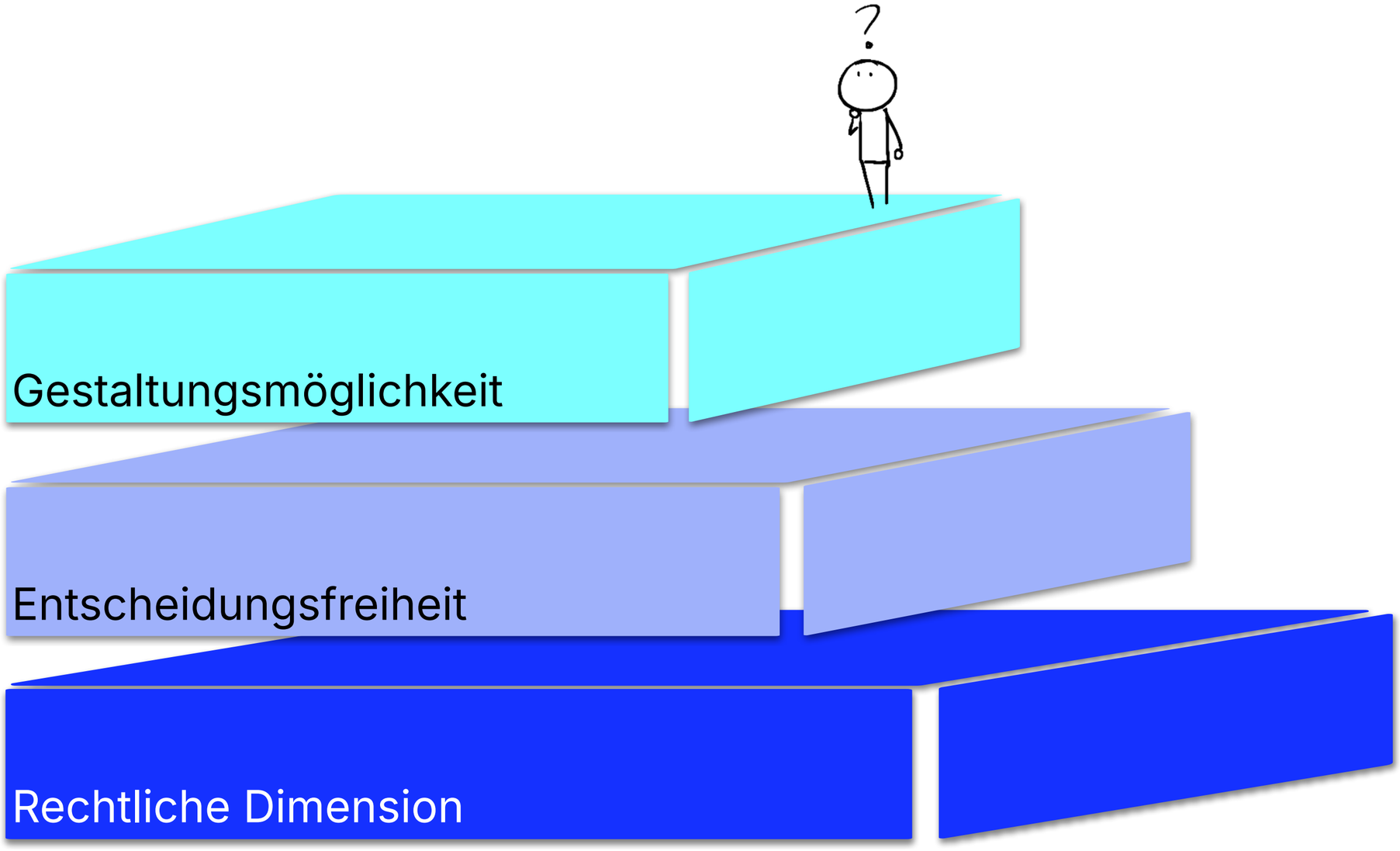
Sovereign Cloud Stack

?



OSBA

Sovereign Cloud Stack



OSBA

Sovereign Cloud Stack

Kompetenz

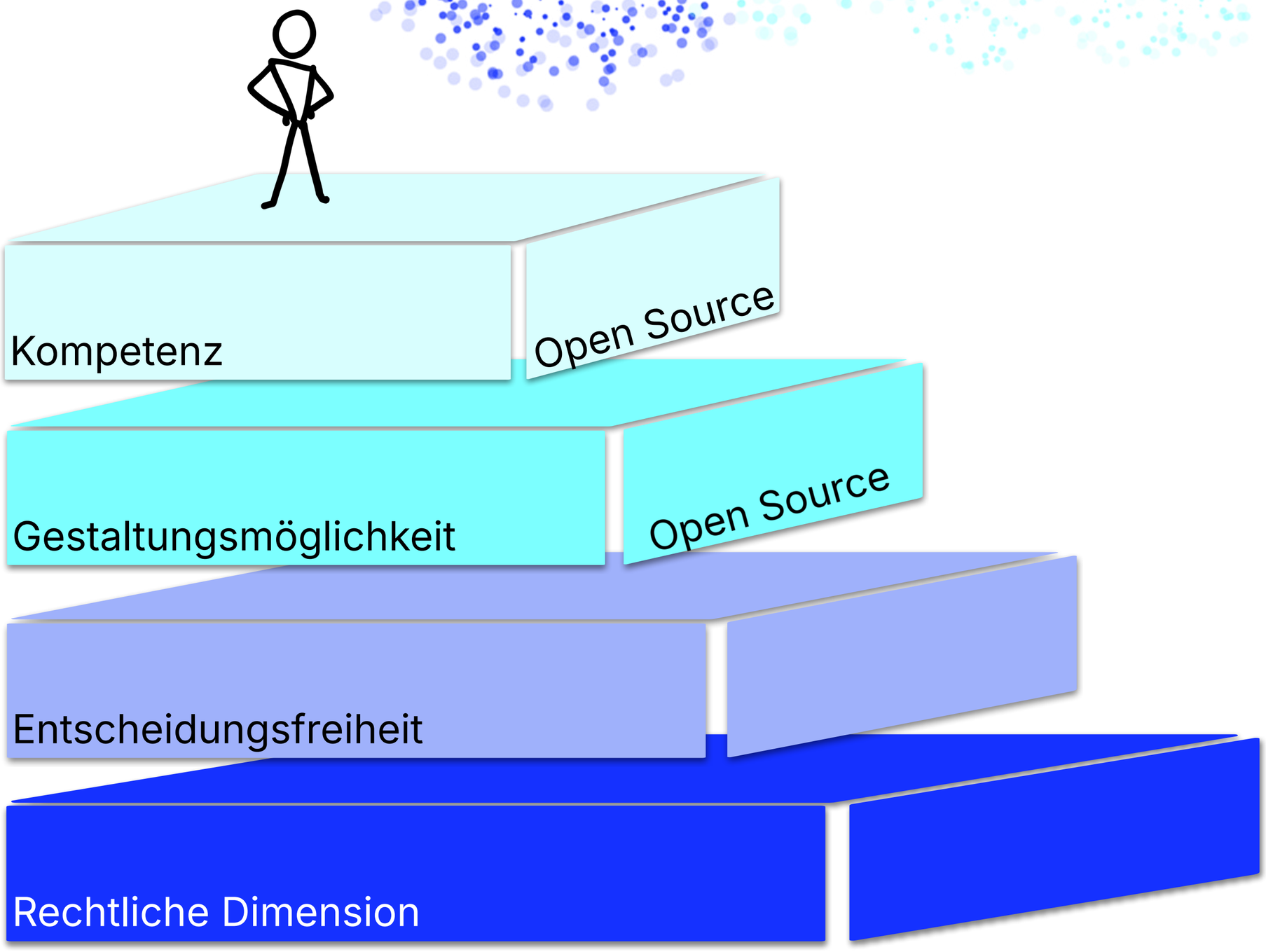
Gestaltungsmöglichkeit

Entscheidungsfreiheit

Rechtliche Dimension

OSBA

Sovereign Cloud Stack



OSBA

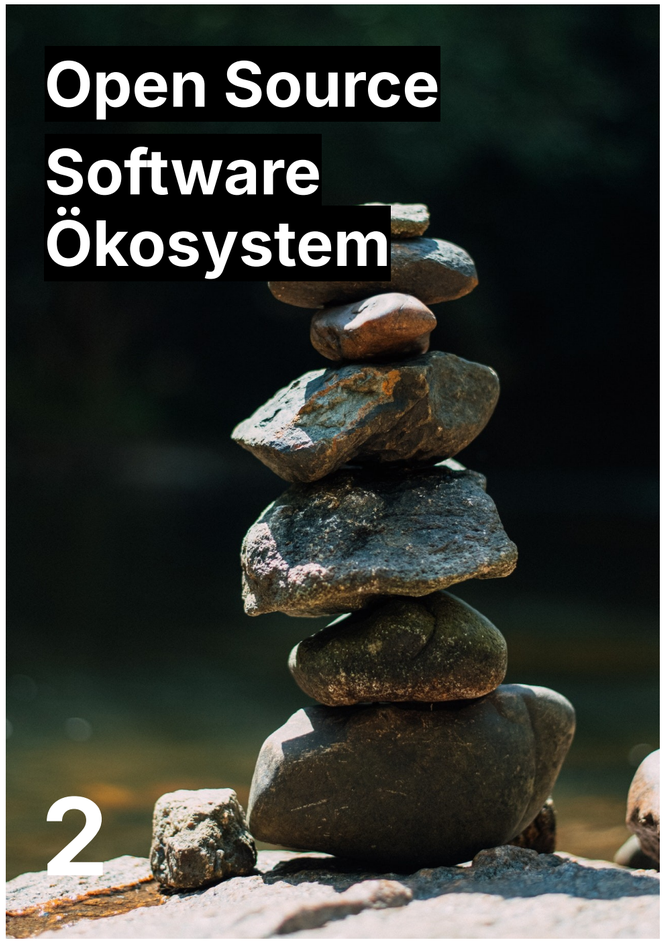
Sovereign Cloud Stack

Open Source Software ist die Grundlage für digitale Souveränität, denn sie stellt sicher, dass die Systeme, die in Verwaltung, Wirtschaft und Zivilgesellschaft verwendet werden, überprüfbar, gestaltbar und ersetzbar sind.

(Open Source Business Alliance)

OSBA

Sovereign Cloud Stack – Erzeugnisse



Digitale Souveränität & SCS Zertifizierung

Stufe der digitalen Souveränität

4: Operative Transparenz und verfügbares Wissen (Kompetenzaufbau)

3: Technologische Transparenz und Fähigkeit zur Mitwirkung und Gestaltung

2: Wahlmöglichkeit zwischen vielen Anbietern, In-Sourcing-Option (On-Premise)

1: Einhaltung von Rechtsvorschriften (DSGVO)

SCS Zertifizierungslevel

4: “**SCS-sovereign**” – Ops/IAM stacks sind OSS sowie transparent bei Monitoring und Incidents, Mitwirkung an OpenOperations (5 Opens)

3: “**SCS-open**” – SBOM für Funktionalen Stack verfügbar und vollständig OSS (4 Opens)

2: “**SCS-compatible**” – technische Kompatibilität (Konformitätstests bestanden: CNCF, OIF, SCS)

1: ENISA/Gaia-X Kennzeichnungen & rechtliche Regelungen (nicht SCS-spezifisch)

Sovereign Cloud Stack

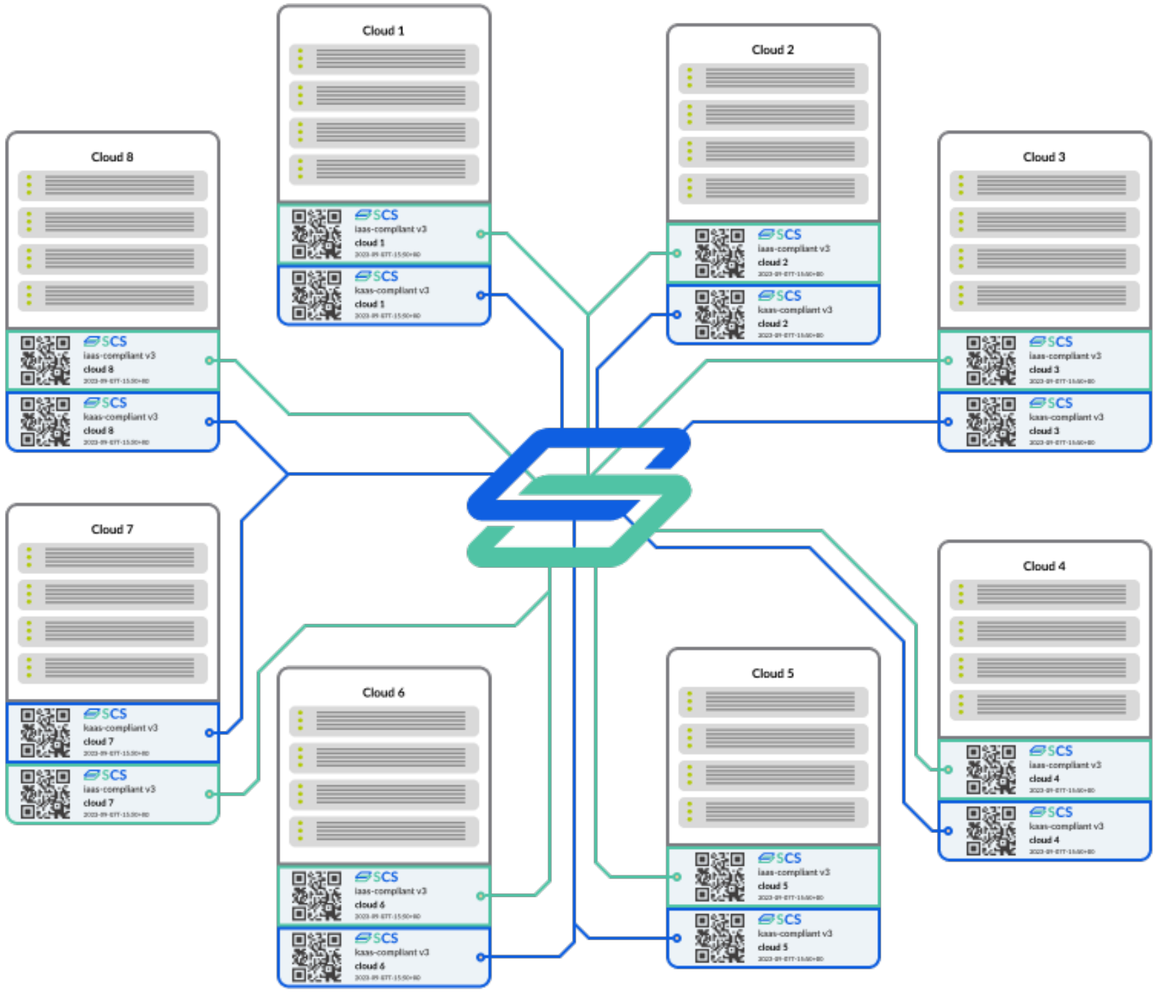
SCS Standards

OSBA

sovereigncloudstack.org

Sovereign Cloud Stack

Wozu Interoperabilität?




Allied Telesis
CentreCOM™ MX10
IEEE 802.3 MICROTRANSCEIVER
10 BASE 2
(MAU)
MULTIVISION
Adapter
Tiornega
Q MOUSE
D9 FF


FOR EXPORT ONLY
TRAVEL ADAPTOR

```
157  def get_server_external_ipv4(cloud, server):
158      """Find an externally routable IP for the server.
159
160      There are 5 different scenarios we have to account for:
161
162      * Cloud has externally routable IP from neutron but neutron APIs don't
163        work (only info available is in nova server record) (rackspace)
164      * Cloud has externally routable IP from neutron (runabove, ovh)
165      * Cloud has externally routable IP from neutron AND supports optional
166        private tenant networks (vexxhost, unitedstack)
167      * Cloud only has private tenant network provided by neutron and requires
168        floating-ip for external routing (dreamhost, hp)
169      * Cloud only has private tenant network provided by nova-network and
170        requires floating-ip for external routing (auro)
171
172      :param cloud: the cloud we're working with
173      :param server: the server dict from which we want to get an IPv4 address
174      :return: a string containing the IPv4 address or None
175      """
```

Digitale Souveränität & SCS Zertifizierung

Stufe der digitalen Souveränität

4: Operative Transparenz und verfügbares Wissen (Kompetenzaufbau)

3: Technologische Transparenz und Fähigkeit zur Mitwirkung und Gestaltung

2: Wahlmöglichkeit zwischen vielen Anbietern, In-Sourcing-Option (On-Premise)

1: Einhaltung von Rechtsvorschriften (DSGVO)

SCS Zertifizierungslevel

4: “**SCS-sovereign**” – Ops/IAM stacks sind OSS sowie transparent bei Monitoring und Incidents, Mitwirkung an OpenOperations (5 Opens)

3: “**SCS-open**” – SBOM für Funktionalen Stack verfügbar und vollständig OSS (4 Opens)

2: “**SCS-compatible**” – technische Kompatibilität (Konformitätstests bestanden: CNCF, OIF, SCS)

1: ENISA/Gaia-X Kennzeichnungen & rechtliche Regelungen (nicht SCS-spezifisch)

Architectural Layers

Ops Layer

Tooling and infrastructure design for easy, efficient and transparent ways to operate an SCS Cloud.

Learn More

Container Layer

SCS offers a robust solution for managing container workloads on a Kubernetes infrastructure.

Learn More

IaaS Layer

SCS offers OpenStack infrastructure solutions based on KVM virtualization to deploy VM workloads and enabling the container layer optionally.

Learn More

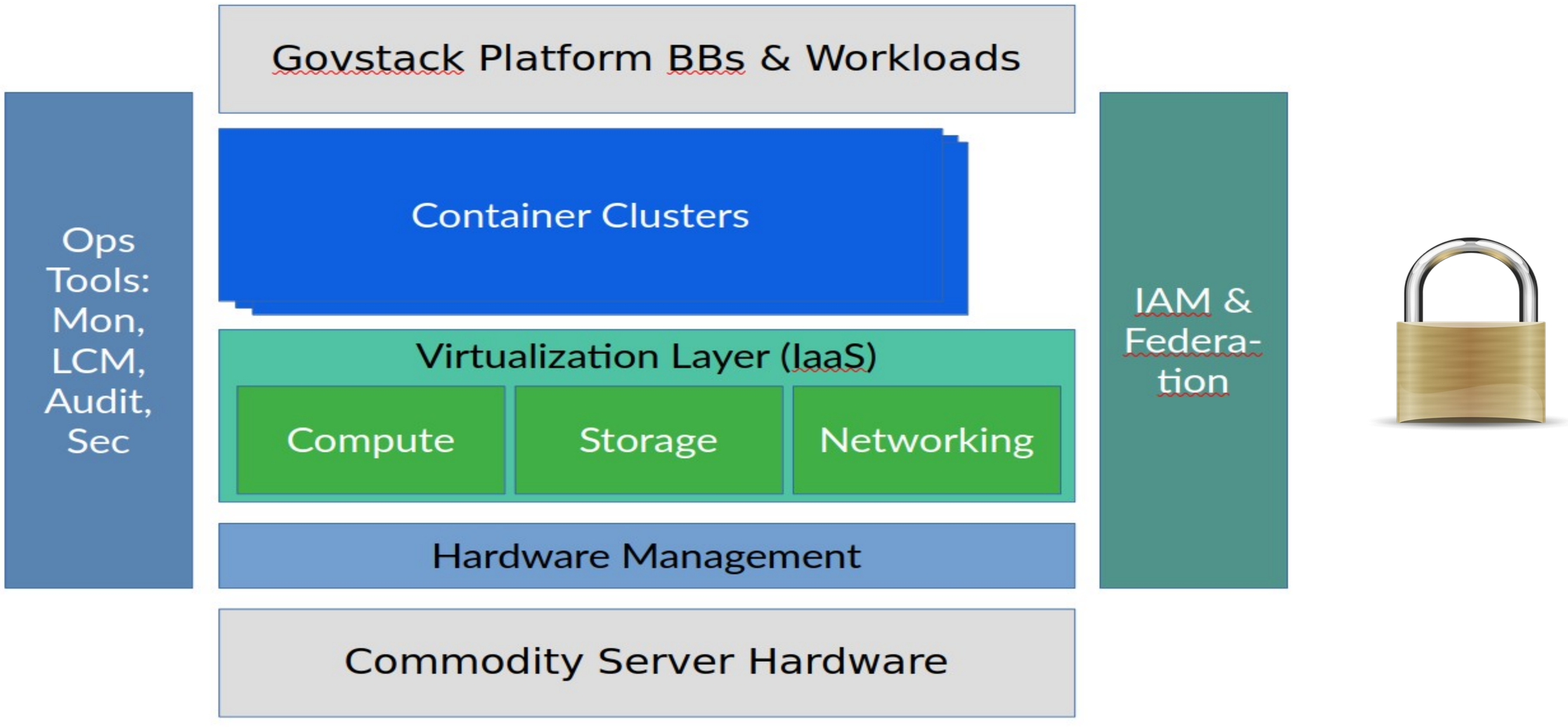
IAM Layer

Working on Keycloak federated identity provider within our Team IAM.

Learn More

Sovereign Cloud Stack

SCS Architektur (Referenzarchitektur)
Von Grund aufgebaut



OSBA

Sovereign Cloud Stack

Overview

Standards are the core deliverable of SCS. By standardizing the open source software components of a cloud computing stack, their versions, how they are to be configured, deployed and utilized, SCS guarantees the reproducibility of a certain behavior of this technology.

SCS standards are discussed, developed and maintained in the community by the corresponding teams (see Track in the table below), which naturally include existing users of SCS.

*Legend to the column headings and entries:

- Document states: Draft, Effective, Deprecated (and no longer effective)
- Entries in the effective column marked with an * are stable right now but turn to effective documents in the near future
- Entries in the effective column marked with a † will turn deprecated in the near future

Standard	Track	Description	Draft	Effective	Deprecated*
scs-0001	Global	Sovereign Cloud Standards	-	v1	-
scs-0002	Global	Standards, Docs and Organisation	v2	v1	-
scs-0003	Global	Sovereign Cloud Standards YAML	v1	-	-
scs-0004	Global	Regulations for achieving SCS-compatible certification	-	v1	-
		Supplement: Implementation hints for achieving SCS-compatible certification	w1	-	-
scs-0005	Global	Governance of the SCS community	v2	v1	-
scs-0006	Global	SCS GitHub Organization - Management of Inactive Users and Repositories	v1	-	-
scs-0007	Global	Certification of integrators	-	v1	-
		Supplement: Implementation hints for achieving Certified SCS Integrator	w1	-	-
scs-0100	IaaS	SCS Flavor Naming Standard	-	v3	v1, v2
		Supplement: Implementation and Testing Notes	w1	-	-
scs-0101	IaaS	SCS Entropy	-	v1	-
		Supplement: Implementation and Testing Notes	w1	-	-
scs-0102	IaaS	SCS Image Metadata	-	v1	-
		Supplement: Implementation and Testing Notes	w1	-	-
scs-0103	IaaS	SCS Standard Flavors and Properties	-	v1	-

https://docs.scs.community/standards/

OSBA

Global Standards

This track encompasses the foundational standards that guide the overall structure, documentation, and general topics related to the Sovereign Cloud Stack. It serves as the core framework, ensuring consistency, clarity, and comprehensibility across all aspects of the cloud stack, fostering an environment where information is easily accessible and understood.

*Legend to the column headings and entries:

- Document states: Draft, Effective, Deprecated (and no longer effective)
- Entries in the effective column marked with an * are stable right now but turn to effective documents in the near future
- Entries in the effective column marked with a † will turn deprecated in the near future

Standard	Description	Draft	Effective	Deprecated*
scs-0001	Sovereign Cloud Standards	-	v1	-
scs-0002	Standards, Docs and Organisation	v2	v1	-
scs-0003	Sovereign Cloud Standards YAML	v1	-	-
scs-0004	Regulations for achieving SCS-compatible certification	-	v1	-
	Supplement: Implementation hints for achieving SCS-compatible certification	w1	-	-
scs-0005	Governance of the SCS community	-	v1	-
scs-0006	SCS GitHub Organization - Management of Inactive Users and Repositories	v1	-	-
scs-0007	Certification of integrators	v1	-	-
	Supplement: Implementation hints for achieving Certified SCS Integrator	w1	-	-

IaaS Standards

The IaaS Layer Standards track focuses on the protocols, guidelines, and specifications that govern the infrastructure as a service layer. This encompasses standards for virtual machines, storage, networking, and other foundational resources, ensuring seamless, efficient, and secure operation, interoperability, and management of the underlying cloud infrastructure.

*Legend to the column headings and entries:

- Document states: Draft, Effective, Deprecated (and no longer effective)
- Entries in the effective column marked with an * are stable right now but turn to effective documents in the near future
- Entries in the effective column marked with a † will turn deprecated in the near future

Standard	Description	Draft	Effective	Deprecated*
scs-0100	SCS Flavor Naming Standard	-	v3	v1, v2
	Supplement: Implementation and Testing Notes	w1	-	-
scs-0101	SCS Entropy	-	v1	-
	Supplement: Implementation and Testing Notes	w1	-	-
scs-0102	SCS Image Metadata	-	v1	-
	Supplement: Implementation and Testing Notes	w1	-	-
scs-0103	SCS Standard Flavors and Properties	-	v1	-
scs-0104	SCS Standard Images	-	v1	-
	Supplement: Implementation Notes	w1	-	-
scs-0110	SSD Flavors	-	v1	-
scs-0111	Decisions for the Volume Type Standard	v1	-	-
scs-0112	SONiC Support in SCS	v1	-	-
scs-0113	Security Groups Decision Record	v1	-	-
scs-0114	SCS Volume Types	-	v1	-
scs-0115	Default Rules for Security Groups	-	v1	-
scs-0116	SCS Key Manager Standard	-	v1	-
	Supplement: Implementation and Testing Notes	w1	-	-
scs-0117	Volume Backup Functionality	-	v1	-
scs-0118	SCS Taxonomy of Failsafe Levels	v1	-	-
	Supplement: Examples of Failure Cases and their impact on IaaS and KaaS resources	w1	-	-

KaaS Standards

Standards in this track are concerned with Kubernetes as a Service layer, outlining norms and best practices for deploying, managing, and operating Kubernetes clusters. These standards aim to ensure that the orchestration of containers is streamlined, secure, and compatible across various cloud environments and platforms.

*Legend to the column headings and entries:

- Document states: Draft, Effective, Deprecated (and no longer effective)
- Entries in the effective column marked with an * are stable right now but turn to effective documents in the near future
- Entries in the effective column marked with a † will turn deprecated in the near future

Standard	Description	Draft	Effective	Deprecated*
scs-0200	Using Sonobuoy for KaaS conformance tests	v1	-	-
scs-0210	SCS K8S Version Policy	-	v2	v1
	Supplement: Implementation and Testing Notes	w1	-	-
scs-0211	SCS KaaS default storage class	v2	v1	-
	Supplement: Implementation and Testing Notes	w1	-	-
scs-0212	Requirements for container registries	v1	-	-
scs-0213	Kubernetes Nodes Anti Affinity	v1	-	-
scs-0214	Kubernetes Node Distribution and Availability	-	v2	v1
	Supplement: Implementation and Testing Notes	w1	-	-
scs-0215	Robustness features for Kubernetes clusters	v1	-	-
scs-0216	Requirements for testing cluster-stacks	v1	-	-
scs-0217	Kubernetes cluster hardening	v1	-	-
scs-0218	Container registry for SCS standard implementation	v1	-	-
scs-0219	KaaS Networking Standard	-	v1	-
	Supplement: Implementation Notes	w1	-	-

Requirements

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

In addition, "FORBIDDEN" is to be interpreted equivalent to "MUST NOT".

scs-0100: SCS Flavor Naming Standard

The SCS Flavor Naming Standard provides a systematic approach for naming instance flavors in OpenStack environments, ensuring backward compatibility and clarity on key features like the number of vCPUs, RAM, and Root Disk, as well as extra features like GPU support and CPU generation. The standard aims for usability and portability across all SCS flavors.

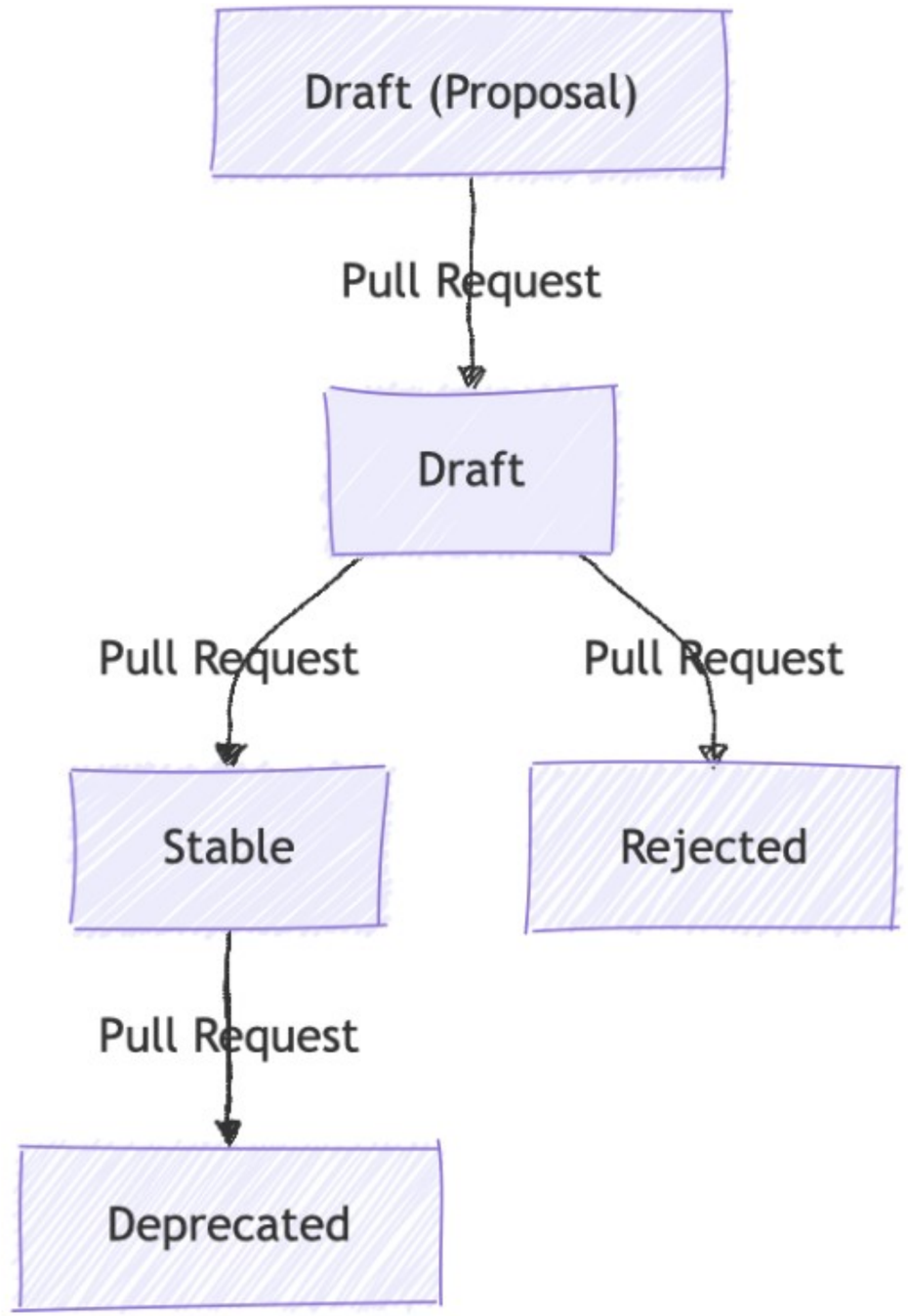
Version	Type	State	stabilized	deprecated
scs-0100-v1	Standard	Deprecated	2022-09-08	2023-10-31
scs-0100-v2	Standard	Deprecated	2023-02-21	2023-11-30
scs-0100-v3	Standard	Stable	2023-06-14	-

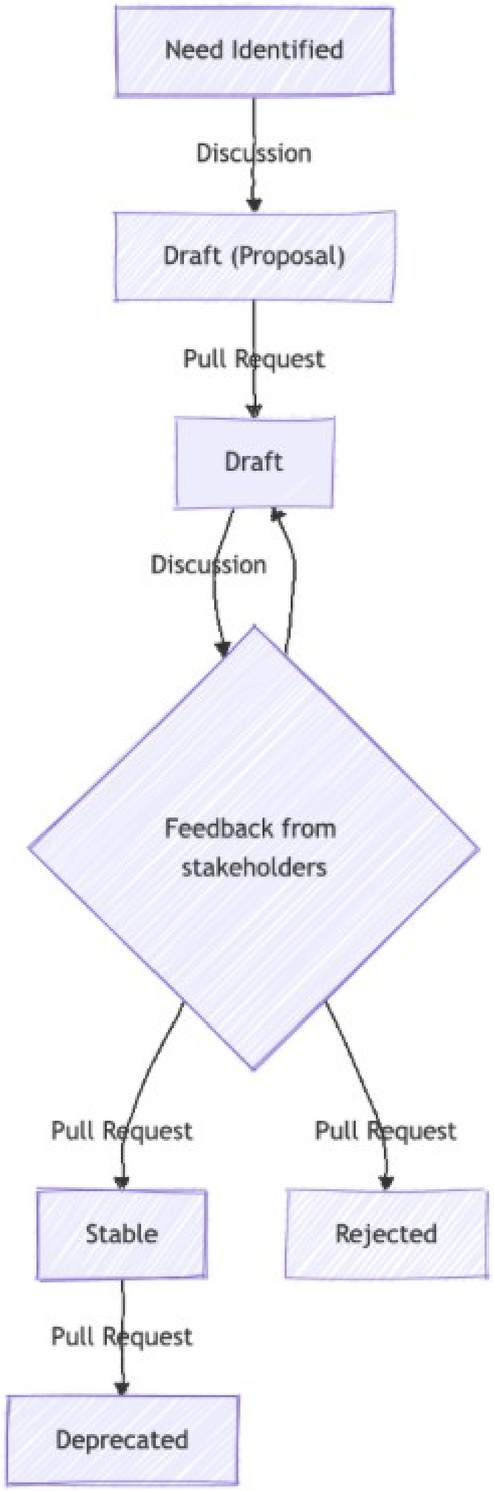
Supplement: Implementation and Testing Notes

Version	State	stabilized	deprecated
w1	Draft	-	-

Previous
« IaaS Standards

Next
V1 »


Draft (Proposal)
Pull Request
Draft
Pull Request
Pull Request
Stable
Rejected
Pull Request
Deprecated


Need Identified
Discussion
Draft (Proposal)
Pull Request
Draft
Discussion
Feedback from stakeholders
Pull Request
Pull Request
Stable
Rejected
Pull Request
Deprecated


SITUATION:
THERE ARE
14 COMPETING
STANDARDS.
14?! RIDICULOUS!
WE NEED TO DEVELOP
ONE UNIVERSAL STANDARD
THAT COVERS EVERYONE'S
USE CASES.
YEAH!
SOON:
SITUATION:
THERE ARE
15 COMPETING
STANDARDS.

Collaboration on Cloud Standards

Kurt Garloff, Marius Feldmann

November 27, 2023

Collaboration on Cloud Standards

Sovereign Cloud Stack and ALASCA e.V.: joining forces for good standards

IG BvC

Die IG BvC stellt sich vor ...

IG BvC (Interessengemeinschaft Betrieb von Containern)

Die IG Betrieb von Containern (IG BvC) ist ein Zusammenschluss von Datenzentralen, Softwarelieferanten und Organisationen der Öffentlichen Verwaltung.

PublicCloudSIG

Status: Active

Chairs:

```
* Tobias Rydberg <tobias.rydberg@cleura.com>
* Felix Kronlage-Dammers <fkr@osb-alliance.com>
```

The aim of this group is to represent the interests of the OpenStack public cloud provider community, and to further adoption of OpenStack public cloud usage.

Sovereign Cloud Stack

SCS Zertifizierung

OSBA

Digitale Souveränität & SCS Zertifizierung

Stufe der digitalen Souveränität

4: Operative Transparenz und verfügbares Wissen (Kompetenzaufbau)

3: Technologische Transparenz und Fähigkeit zur Mitwirkung und Gestaltung

2: Wahlmöglichkeit zwischen vielen Anbietern, In-Sourcing-Option (On-Premise)

1: Einhaltung von Rechtsvorschriften (DSGVO)

SCS Zertifizierungslevel

4: “**SCS-sovereign**” – Ops/IAM stacks sind OSS sowie transparent bei Monitoring und Incidents, Mitwirkung an OpenOperations (5 Opens)

3: “**SCS-open**” – SBOM für Funktionalen Stack verfügbar und vollständig OSS (4 Opens)

2: “**SCS-compatible**” – technische Kompatibilität (Konformitätstests bestanden: CNCF, OIF, SCS)

1: ENISA/Gaia-X Kennzeichnungen & rechtliche Regelungen (nicht SCS-spezifisch)

Regulations for achieving SCS-compatible certification

Introduction

The Sovereign Cloud Stack (SCS) issues certificates with various scopes, among them *SCS-compatible IaaS* (infrastructure as a service) and *SCS-compatible KaaS* (Kubernetes as a service).

This document details how a cloud service provider (henceforth also called operator) can attain such a certificate for one of their clouds.

Motivation

As operator, I want to obtain a certificate with the scope SCS-compatible IaaS or SCS-compatible KaaS.

Regulations

Certification of integrators

Introduction

The purpose of this document is to describe a concept for how implementation partners can obtain certification as SCS integrators. In essence, this certificate is intended to express that an organization has sufficient technical knowledge and experience to provide technical support to companies using SCS. For this purpose, two essential criteria are defined that must be fulfilled. In addition, there are a few other criteria that can be taken into account in favor of certification.

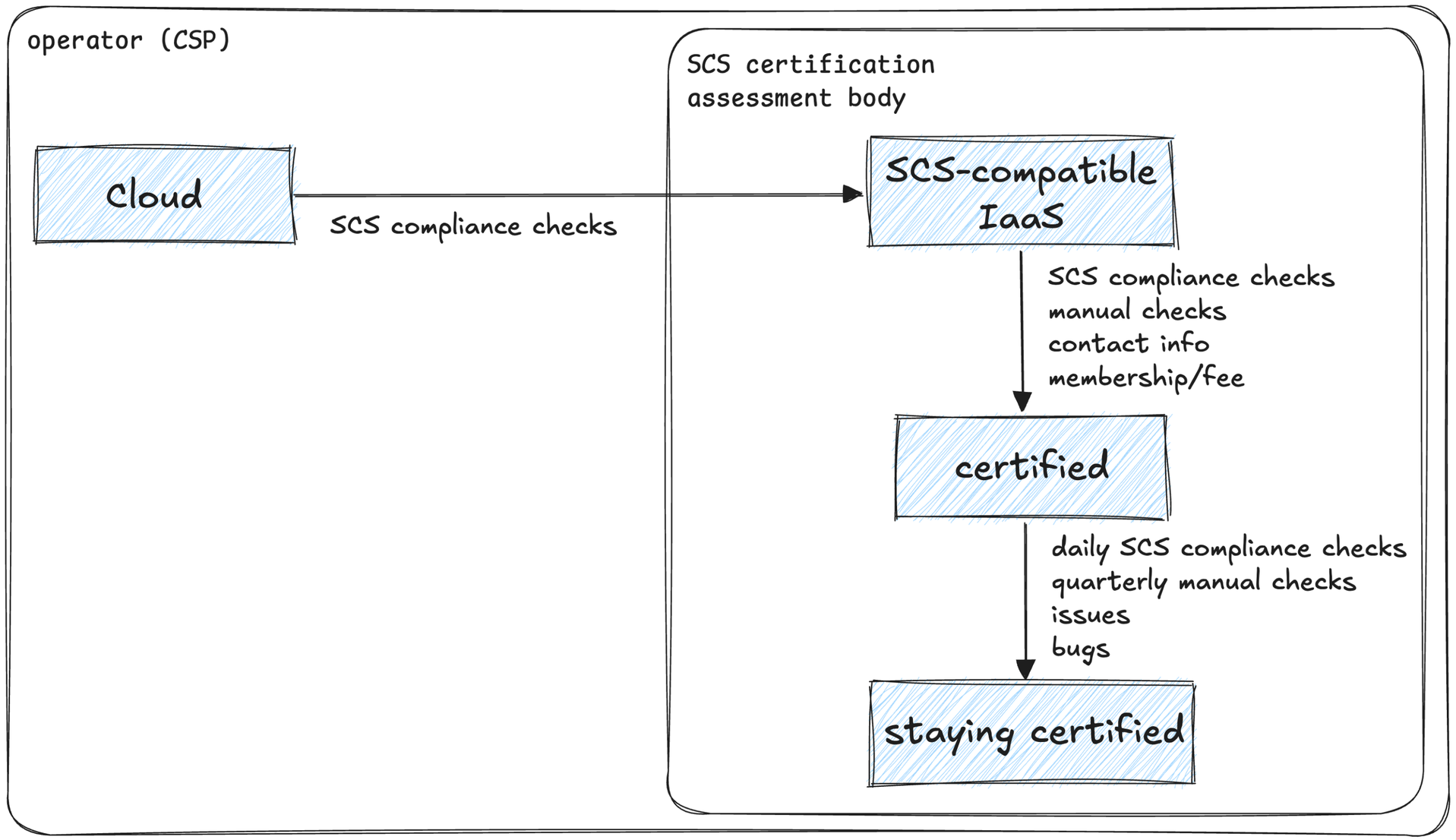
Motivation

As an integrator, I want to obtain a certificate with the scope of *Certified SCS IaaS Integrator* or *Certified of SCS KaaS Integrator*.

Regulations

Sovereign Cloud Stack

Certified SCS-compatible IaaS



OSBA

SCS-compatible IaaS

Scope versions ->	v3	v4	v5.1
State	Deprecated	Deprecated	Effective
Stabilized at	2024-02-28	2024-02-28	2024-12-19
Modules			
OpenStack Powered Compute v2022.11	X	X	X
scs-0100-v3.1: Flavor naming v3.1	X	X	X
scs-0101-v1: Entropy v1		X	X
scs-0102-v1: Image metadata v1	X	X	X
scs-0103-v1: Standard flavors		X	X
scs-0104-v1: Standard images		X (image_spec)	X (image_spec)
scs-0114-v1: Volume Types			X
scs-0115-v1: Default rules for security groups			X
scs-0116-v1: Key manager			X
scs-0117-v1: Volume backup			X
scs-0121-v1: Availability Zones			X
scs-0123-v1: Mandatory and Supported IaaS Services			X
scs-0302-v1: Domain Manager Role			X

SCS Compliance Check Pipeline Manual

The SCS compliance check suite runs automated tests, generates a signed report for the run, and feeds it to the compliance monitor. Roughly speaking, this process has to be performed daily, for instance, using a continuous-integration "pipeline".

Providers of public clouds do not need to use their own pipelines; those clouds can be tested via the official SCS compliance check pipeline.

Alternatively, if using this pipeline is not feasible (for instance, for private clouds) or not desired, cloud-service providers can run the tests and feed the compliance monitor themselves.

The next subsection shows common requirements for each of these two cases. The two subsections after that are each dedicated to the specific cases.

Common requirements for the compliance checks

for SCS-compatible IaaS

Self-testing and technical adjustments

In order for a cloud service offering to obtain a certificate, it has to conform to all mandatory requirements of all standards of the respective scope, which will be tested at regular intervals, and the results of these tests will be made available publicly.

The best approach to get your cloud into compliance is by installing the test suite locally. Have a look at the blog article.

A description of how *SCS-compatible IaaS* compliance can be achieved on OpenStack environments that do not use the SCS reference implementation is written up in the blog article Cost of making an OpenStack Cluster SCS compliant.

Kurt Garloff
October 14, 2024

SCS-compatible IaaS: Example test and adjust

Run the tests

Get the test suite by cloning the SCS standards repo. In order to run the tests, you need to have normal customer (tenant) access to the cloud or container infrastructure that you want to test. (This is by design; we explicitly do not require nor recommend admin level access for normal compliance testing.)

Costs of making an OpenStack cluster SCS-compliant

Hannes Baum, Martin Morgenstern
May 13, 2024

Have you ever wondered how much effort it would take to adopt SCS standards in your OpenStack cloud? We wanted to know this too, and as part of our work in the SCS standards team, we evaluated the process of making a vanilla OpenStack cluster SCS-compliant. In this blog post, we want to share the results of our findings and the process we went through. Rest assured – it is actually quite easy to adopt SCS standards!

Where we started from

Our focus in this evaluation was on OpenStack clusters and therefore the IaaS standards, because for the IaaS layer we already had a reference *SCS Compatible IaaS* scope at the time we started (in the future, a similar evaluation and blog post for the KaaS layer is planned).

Details for subject scaleup-occ2

scaleup-occ2: SCS-compatible IaaS

- spec overview

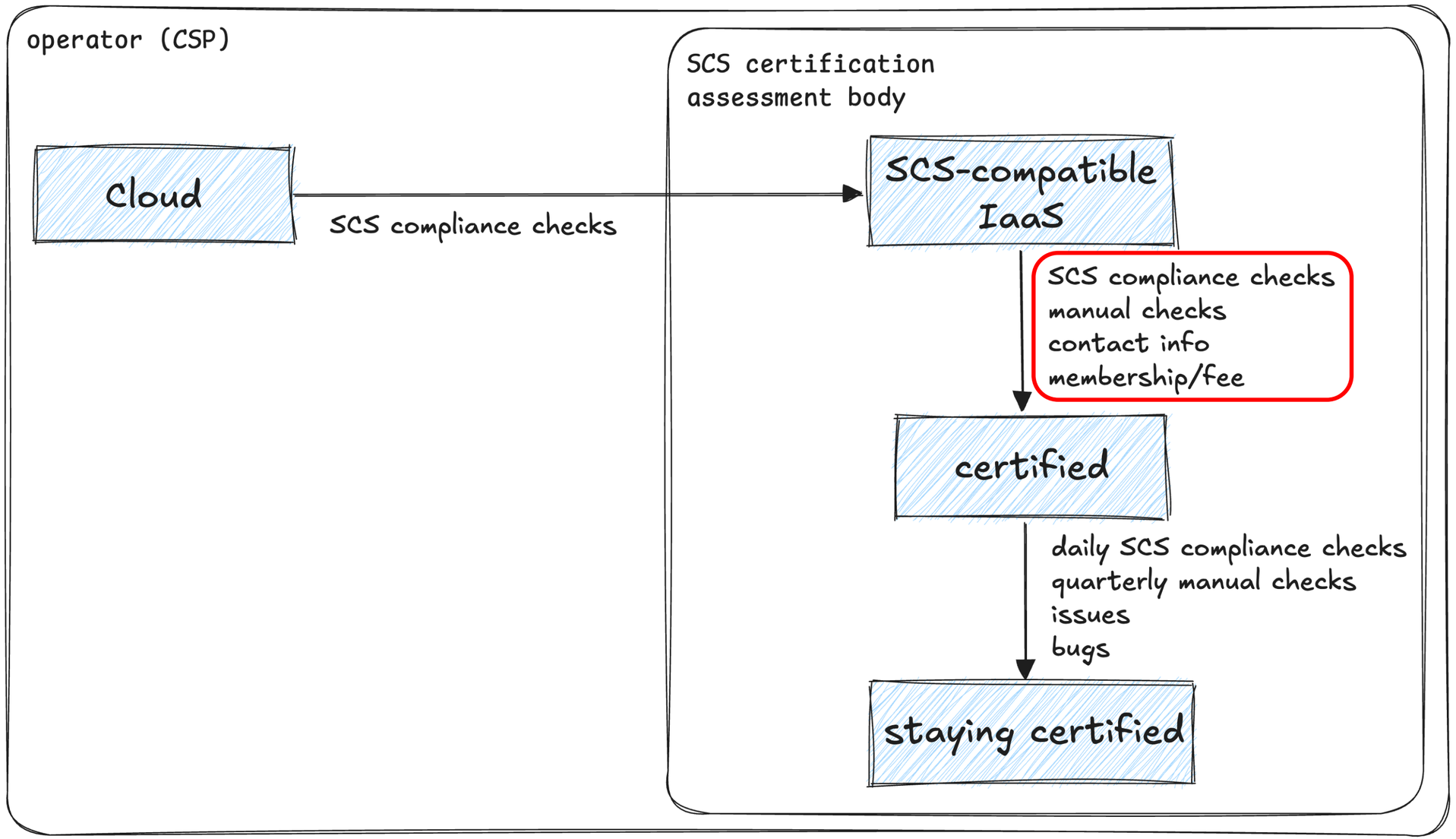
v5.1 (effective): PASS

Target main: PASS

testcase id	result	description
flavor-name-check	✔	Must fulfill all requirements of https://docs.scs.community/standards/scs-0100-v3-flavor-naming
entropy-check	✔	Must fulfill all requirements of https://docs.scs.community/standards/scs-0101-v1-entropy
image-metadata-check	✔	Must fulfill all requirements of https://docs.scs.community/standards/scs-0102-v1-image-metadata
standard-flavors-check	✔	Must fulfill all requirements of https://docs.scs.community/standards/scs-0103-v1-standard-flavors
standard-images-check	✔	Must fulfill all requirements of https://docs.scs.community/standards/scs-0104-v1-standard-images
volume-types-check	✔	Must fulfill all requirements of https://docs.scs.community/standards/scs-0114-v1-volume-type-standard
security-groups-default-rules-check	✔	Must fulfill all requirements of https://docs.scs.community/standards/scs-0115-v1-default-rules-for-security-groups
key-manager-check	✔	Must fulfill all requirements of https://docs.scs.community/standards/scs-0116-v1-key-manager-standard
volume-backup-check	✔	Must fulfill all requirements of https://docs.scs.community/standards/scs-0117-v1-volume-backup-service
service-apis-check	✔	Must fulfill all requirements of https://docs.scs.community/standards/scs-0123-v1-mandatory-and-supported-IaaS-services (except for documentation requirements, which are tested manually with service-apis-docs-check).

Target preview: MISS

testcase id	result	description
⚠️ availability-zones-check	⚠	Note: manual check! Must fulfill all requirements of https://docs.scs.community/standards/scs-0121-v1-Availability-Zones-Standard
⚠️ service-apis-docs-check	⚠	Note: manual check! Must fulfill documentation requirements of https://docs.scs.community/standards/scs-0123-v1-mandatory-and-supported-IaaS-services.
⚠️ domain-manager-check	⚠	Note: manual check! Must fulfill all requirements of https://docs.scs.community/standards/scs-0302-v1-domain-manager-role


operator (CSP)
Cloud
SCS compliance checks
SCS certification assessment body
SCS-compatible IaaS
SCS compliance checks
manual checks
contact info
membership/fee
certified
daily SCS compliance checks
quarterly manual checks
issues
bugs
staying certified

Sovereign Cloud Stack

Sovereign Cloud Stack

Urkunde

Das Forum SCS-Standards der Open Source Business Alliance e.V. bescheinigt dem Unternehmen das

Produktname Cloud

den Anforderungen der Spezifikationen

Name des Zertifikatsscopes

entspricht. Das Unternehmen FOOBAR darf sich hiermit als

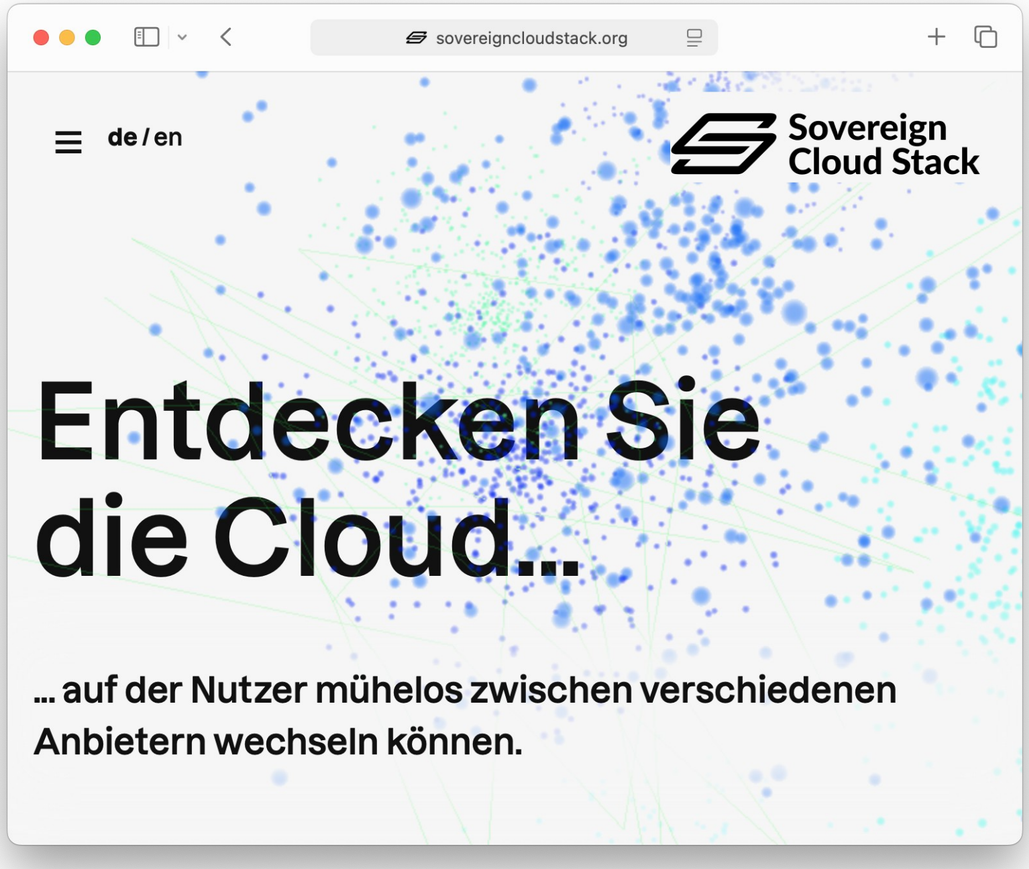
Name des Zertifikats

bezeichnen.

Berlin, den 05. Juni 2025

Attestiert von:

Gültig bis Dezember 2027



OSBA

Compliant cloud environments

This is a list of clouds that we test on a nightly basis against the certificate scope *SCS-compatible IaaS*.

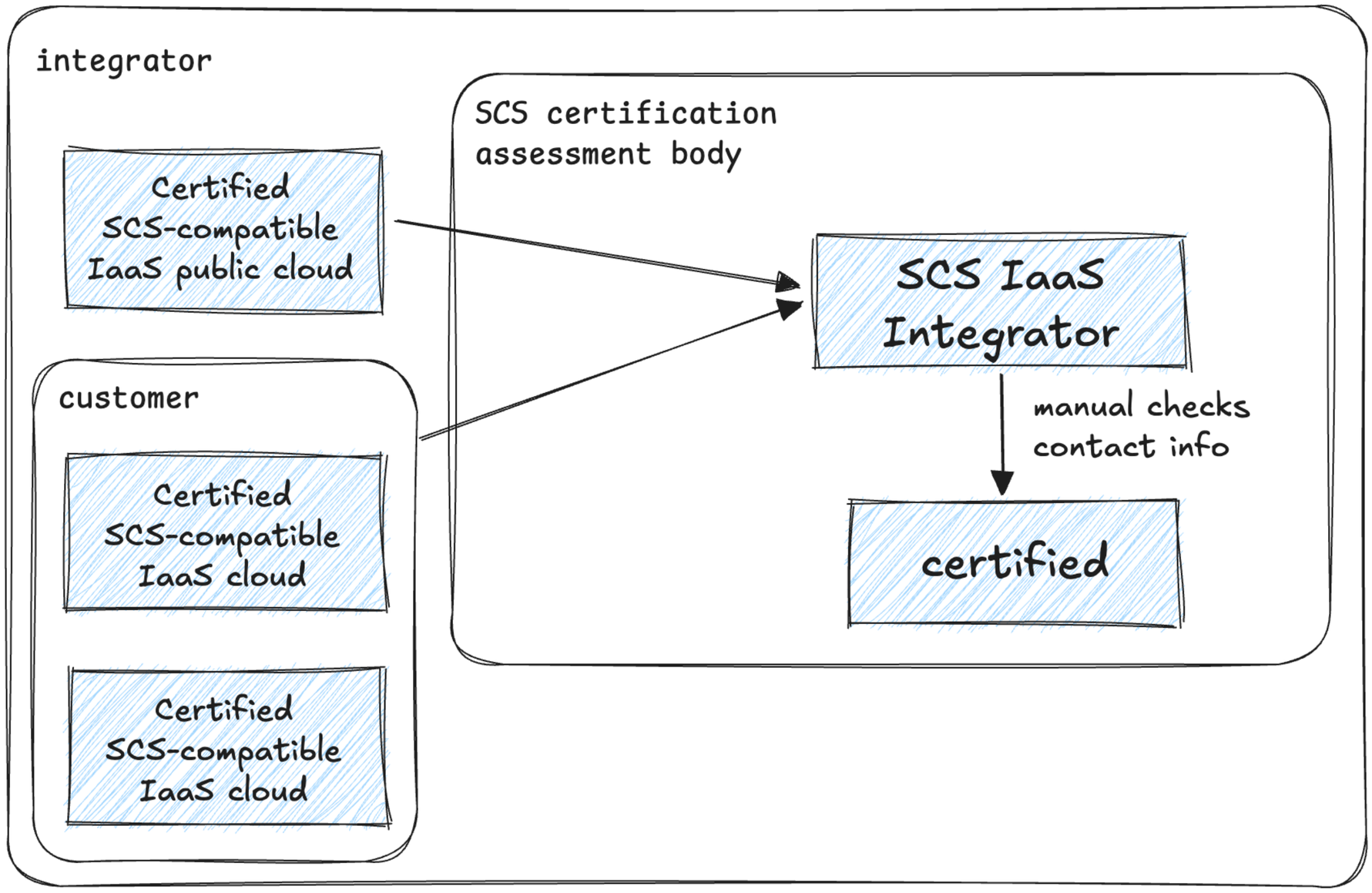
This table shows the most recent **verified** results.

Version numbers are suffixed by a symbol depending on state: * for *draft*, † for *warn* (soon to be deprecated), and †† for *deprecated*.

Name	Description	Operator	SCS-compatible IaaS	HealthMon
scs2	Dev/Test/Demo environment (2nd gen) provided for SCS & GAIA-X context	plusserver GmbH	✅ v5.1	HM
aov.cloud	Community cloud for customers	aov IT.Services GmbH	✅ v5.1	HM
CC@RRZE	Private Compute Cloud (CC) for FAU	Regionales Rechenzentrum Erlangen	✅ v5.1	(soon)
CNDS	Public cloud for customers	artcodix GmbH	✅ v5.1	HM
pluscloud open	Public cloud for customers (4 regions)	plusserver GmbH	✅ v5.1	HM1 HM2 HM3 HM4
PoC WG-Cloud OSBA	Cloud PoC for FITKO	Cloud&Heat Technologies GmbH	✅ v4†	HM
REGIO.cloud	Public cloud for customers	OSISM GmbH	✅ v5.1	HM
ScaleUp Open Cloud	Public cloud for customers	ScaleUp Technologies GmbH & Co. KG	✅ v5.1	HM
syseleven	Public OpenStack Cloud (2 SCS regions)	SysEleven GmbH	🟧 v3††	(soon)
Wavestack	Public cloud for customers	noris network AG/Wavecon GmbH	✅ v5.1	HM

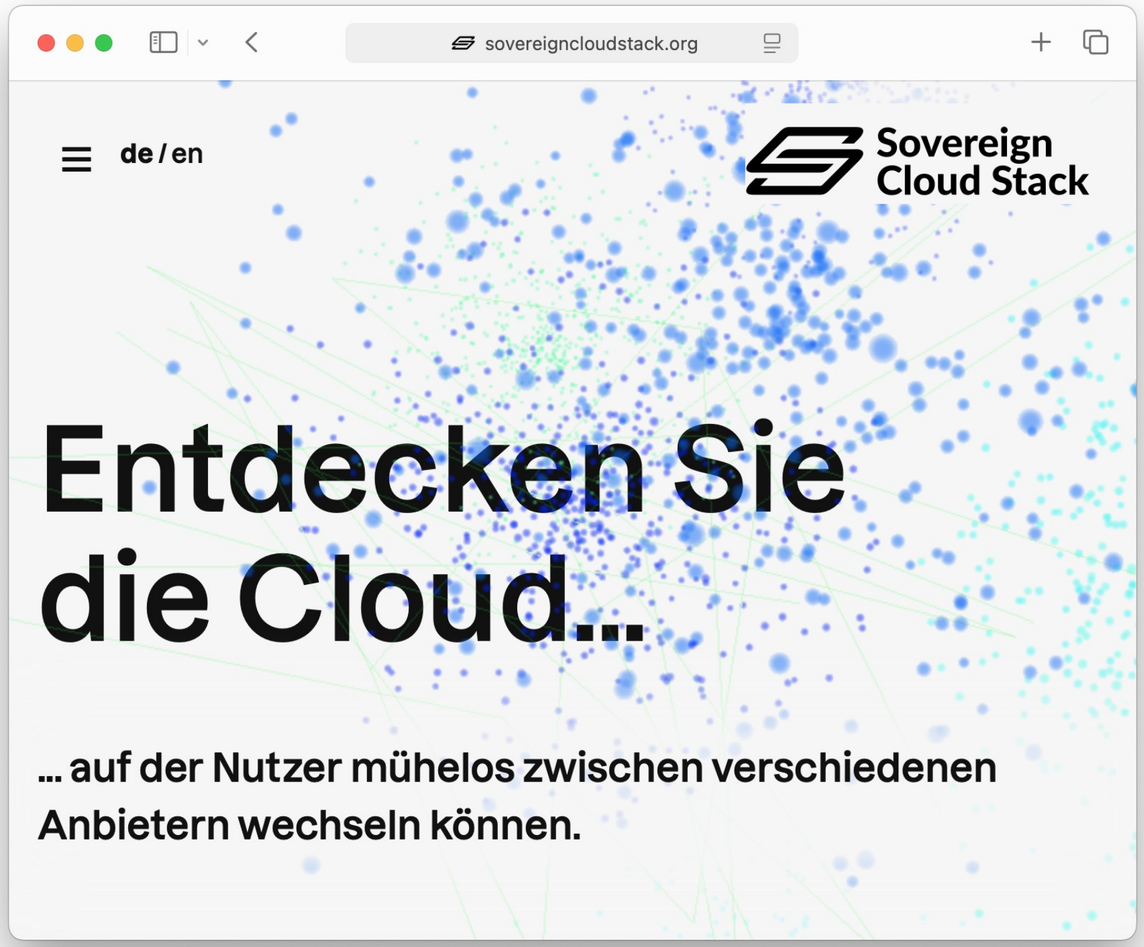
Sovereign Cloud Stack

Certified SCS IaaS Integrator



OSBA

Sovereign Cloud Stack



OSBA

Sovereign Cloud Stack

SCS-compatible KaaS

Scope versions ->	v1
State	Effective
Stabilized at	2024-11-25
Modules	
CNCF Kubernetes conformance	X
scs-0210-v2: Kubernetes version policy	X
scs-0214-v2: Kubernetes node distribution and availability	X
scs-0219-v1: KaaS networking	X

WIP

Work in Progress

OSBA

sovereigncloudstack.org

Sovereign Cloud Stack (SCS) wird nachhaltig abgesichert

FEATURED | PRESSEMITTEILUNGEN | VERBANDS-NEWS | 23. OKTOBER 2024

OSBA und Mitgliedsunternehmen gründen das Forum SCS-Standards

Berlin, 23.10.2024: Der Sovereign Cloud Stack (SCS) stellt alle Cloud-technologischen Grundlagen zur Verwirklichung digitaler Souveränität und zur Umsetzung von Open-Source-Strategien bereit und gibt Nutzerinnen und Nutzern die Kontrolle über ihre Daten. Das vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) finanzierte und von der Open Source Business Alliance (OSBA) durchgeführte Forschungsprojekt endet wie geplant am 31.12.2024. Für die nachhaltige Absicherung der zentralen Ergebnisse und die Weiterentwicklung der Standards haben die OSBA und bisher 14 ihrer Mitgliedsunternehmen bereits gesorgt.

Der Sovereign Cloud Stack wird auch nach der Projektphase, die das Bundesministerium für Wirtschaft und Klimaschutz mit rund 13,2 Millionen Euro finanziert hat, professionell weiterentwickelt und dem Cloud-Markt zur Verfügung stehen. Die OSBA und bisher 14 Mitgliedsunternehmen des Verbands gründen zum 01.01.2025 das Forum SCS-Standards. Dieser Zusammenschluss innerhalb der OSBA wird die Standards und Zertifizierungen sowie deren jeweilige Weiterentwicklungen zukünftig verantworten. Damit wird auch in Zukunft die Qualitätssicherung nachhaltig abgesichert. So können alle Nutzer des Sovereign Cloud Stack einschließlich des gesamten Ökosystems um SCS herum sicher sein, eine zukunftsfähige Cloudtechnologie zu verwenden.

Sovereign Cloud Stack

secunet

UhuruTec

S7n Cloud Services GmbH

ScaleUp Technologies

Syself

B1 SYSTEMS

dataport

noris network

stackXperts

artcodix

SysEleven

plusserver

ITDZ IT FÜR BERLIN

dataR Next-Gen Colocation

OSISM

dNation MAKING CLOUD EASY

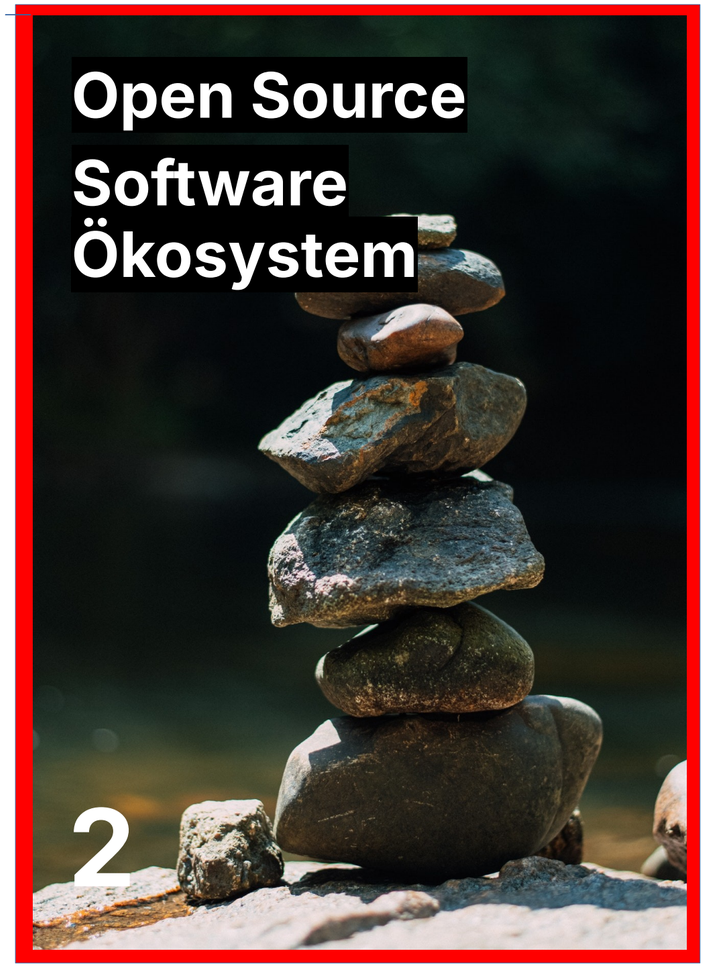
Yorizon

CLOUD & HEAT

OSBA

Sovereign Cloud Stack

Sovereign Cloud Stack – Erzeugnisse

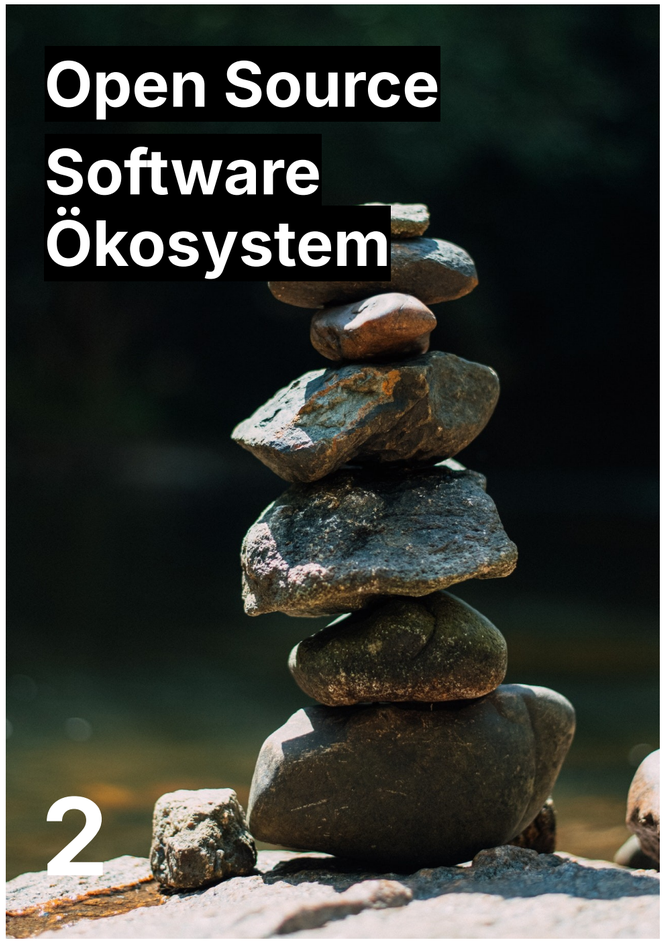


Progress on the SCS reference implementation

Kurt Garloff & Christian Berendt (SCS Project Board)

Aufzeichnung auf YouTube ansehen

Sovereign Cloud Stack – Erzeugnisse



Lean SCS Operator Coffee

Felix Kronlage-Dammers

July 05, 2022

Last week we've had the second edition of the "Lean SCS Operator Coffee". This format was sparked by the R2 retro we had a while ago. From the community of the SCS Operators came the request to have a format where the operators are able to interact and share their experiences in operating SCS environments.

Lean Coffee?

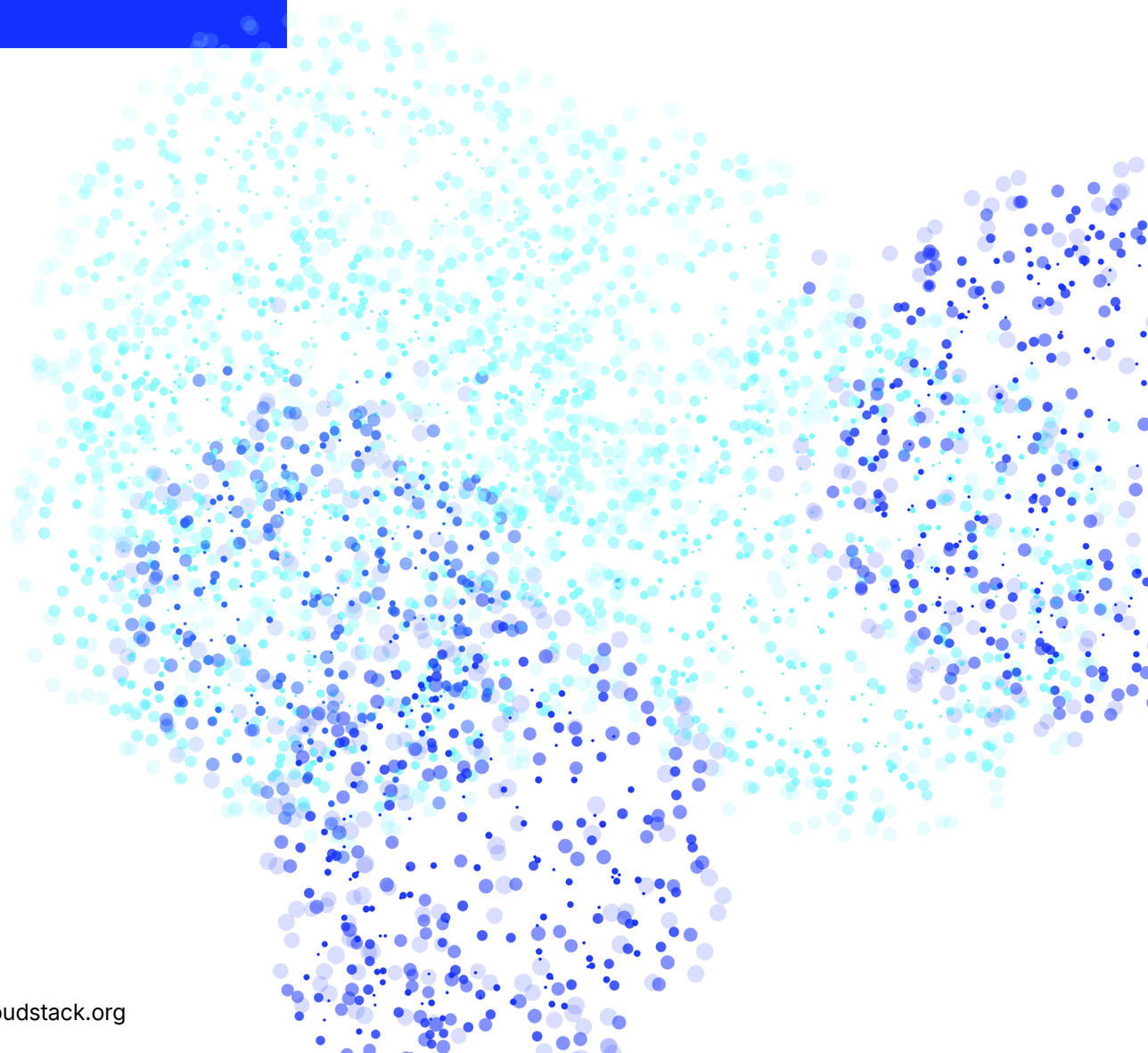
How does "a lean coffee look like"? Let's start with this quote from the original website:

> Lean Coffee is a structured, but agenda-less meeting. Participants gather, build an agenda, and begin talking. Conversations are directed and productive because the agenda for the meeting was democratically generated.

Since the SCS community is distributed a remote-friendly way of organizing the Lean SCS Operator coffee is anticipated. We chose a simple, yet useful (and open source) emulation of a kanban board: scrumblr.

While we (the SCS team) organize the lean coffee, the agenda is made by the participants and I only try to moderate the dialogue and keep the discussion going. Of course the board we use is publicly available as well.

Fragen? Kommentare? Feedback!



Felix Kronlage-Dammers – fkr@osb-alliance.com

Sovereign Cloud Stack

Danke!
Wir sehen uns auf der SCS Summit 2026!

21. Mai 2026!

Felix Kronlage-Dammers – fkr@osb-alliance.com