Sovereign Cloud Stack
An OSB ALLIANCE project

https://scs.community

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

gaia-x

ALASCA

ALASCA Tech Talk 2023-02-23

Standardization in the Sovereign Cloud Stack Community

Kurt Garloff
scs@osb-alliance.com

Vision

Sovereign Cloud Stack:
One platform - standardised, built and operated by many.

SCS combines the best of Cloud Computing in one unified standard. SCS is built, backed, and operated by an active open-source community worldwide. Together we put users in control of their data by enabling cloud operators through a decentralised and federated cloud stack- leveraging true digital sovereignty to foster trust in clouds.

Sovereign Cloud Stack Deliverables

Certifiable Standards

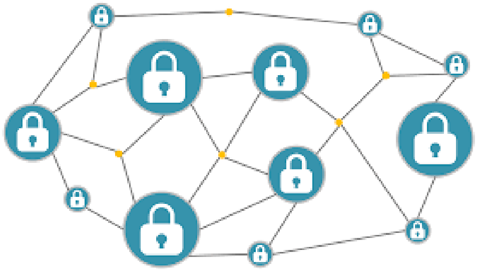
Modular Open Source
Reference Implementation

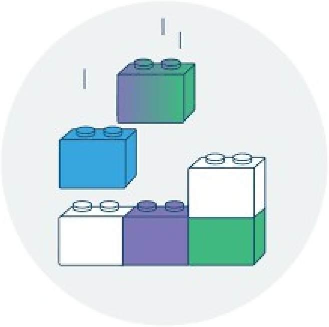
Operational
Knowledge

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Mission

1. Simplify operating modern cloud infrastructure
2. Enable federation and x-operator scaling
3. Create and adopt certifiable standards
4. Create transparency
5. Enable choice for users

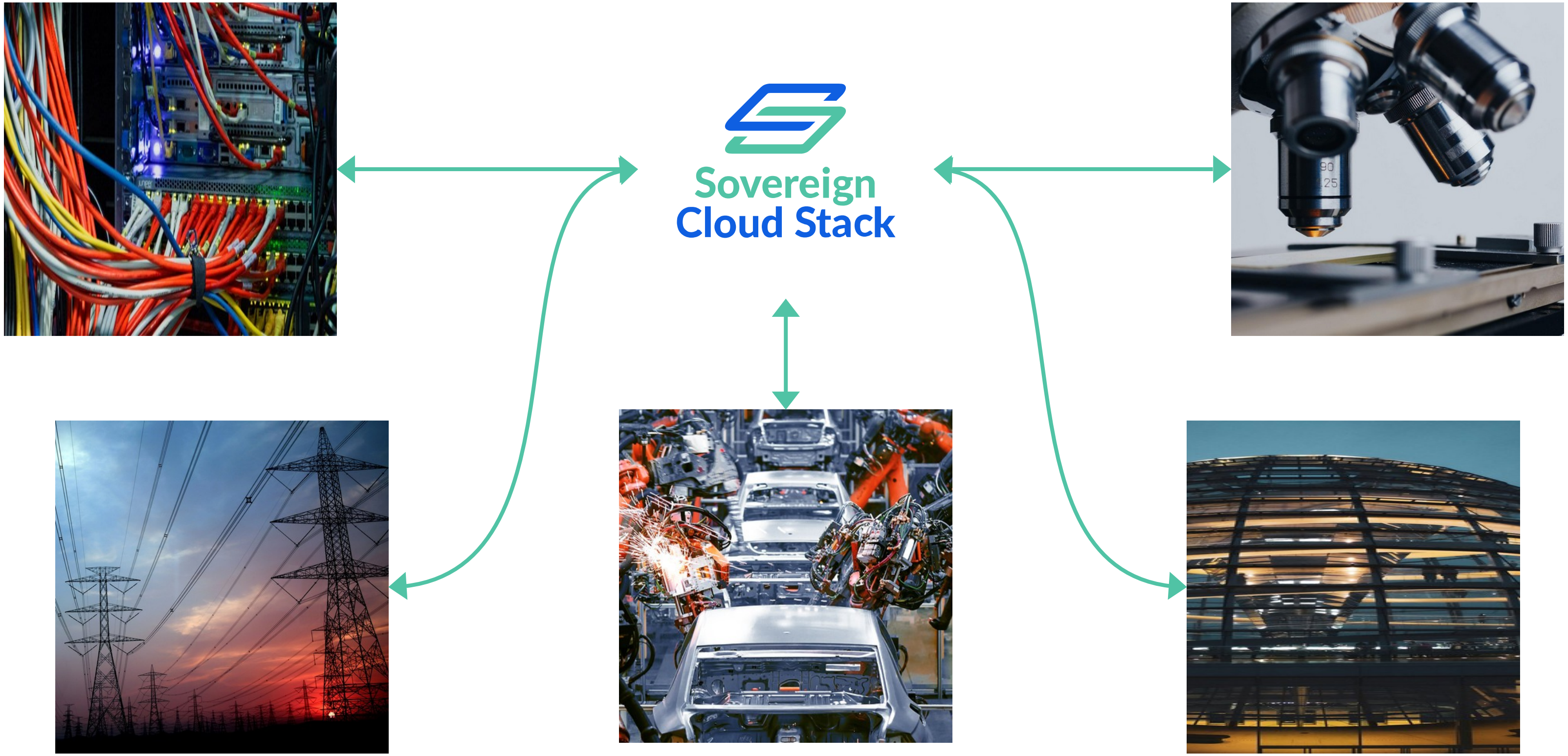




CERTIFIED

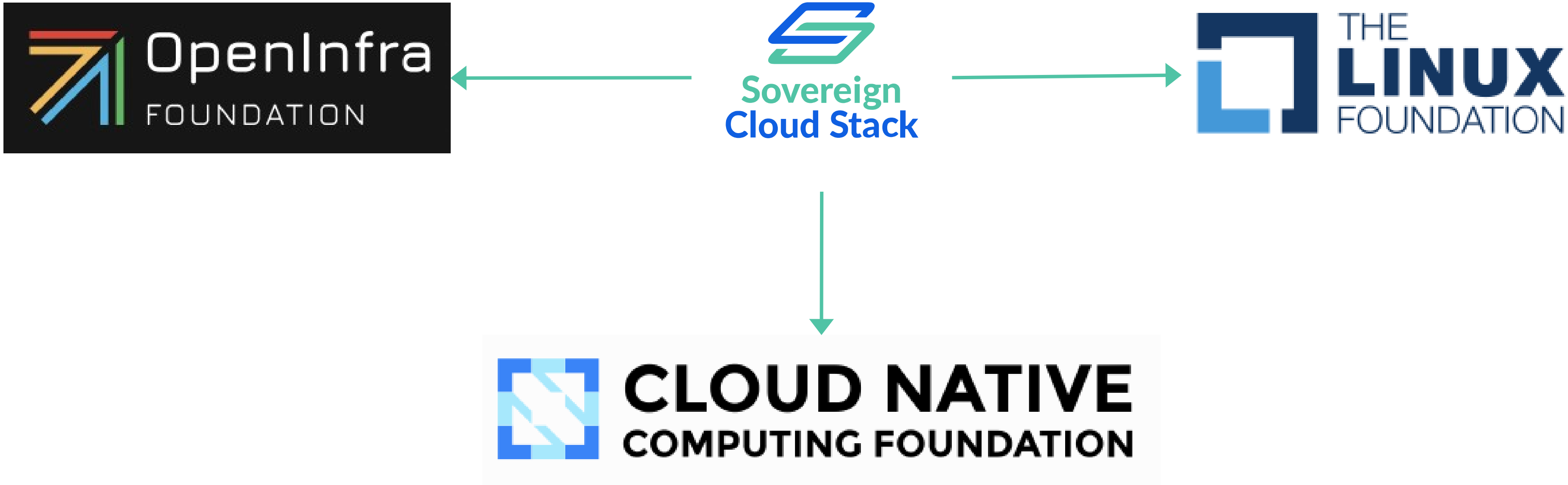
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Open, federated infrastructure for industry, science, administration

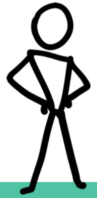


Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Upstream first!



SCS: Realize Digital Sovereignty



Competence (esp. Operations)

Ability to shape technology

Choice / Switching / Interoperability

Legal Compliance (GDPR ...)

the cloud report
Digital Sovereignty
Additional: Sovereign Technology - Open Source - Data Residency - New Work - Open Policy Agent - Container Days

https://rdcu.be/cWdBJ

SCS Certification

Dimensions of Digital Sovereignty

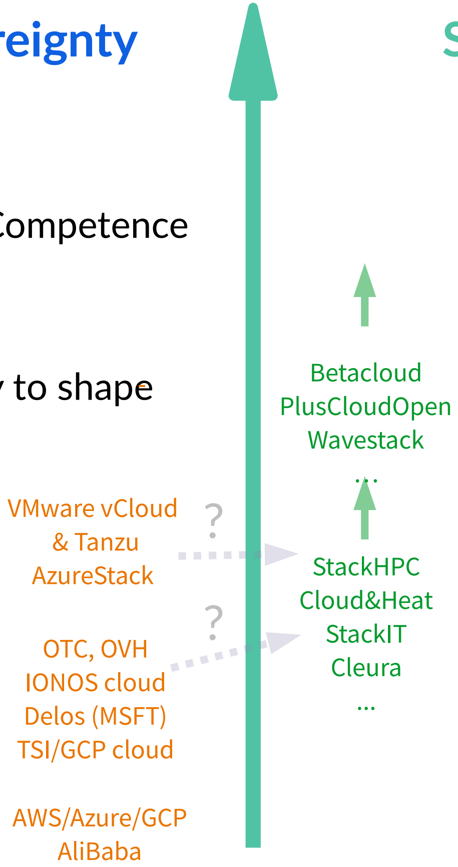
4: Operational Transparency and Competence

3: Technology transparency, ability to shape

2: Choice, Interoperability, Portability

1: Legal Compliance

0: None



VMware vCloud & Tanzu AzureStack ?

OTC, OVH IONOS cloud Delos (MSFT) TSI/GCP cloud ?

AWS/Azure/GCP AliBaba

StackHPC Cloud&Heat StackIT Cleura …

Betacloud PlusCloudOpen Wavestack …

SCS Certification Levels

CERTIFIED

4: "**SCS-Sovereign**" – Ops/IAM Stacks also fully open, transparency w.r.t monitoring, incidents, … Contribution to "Open Operation" (5x Open)

3: "**SCS-Open**" – SBOM for functional stack available, fully open (4x open acc. OpenInfra)

2: "**SCS-Compatible**" – Technical Compatibility, interoperable (Conformance tests pass: CNCF, OIF, SCS)

1: ENISA / Gaia-X labels / GDPR (no extra SCS-Cert)

Sovereign Cloud Stack
An OSB ALLIANCE project

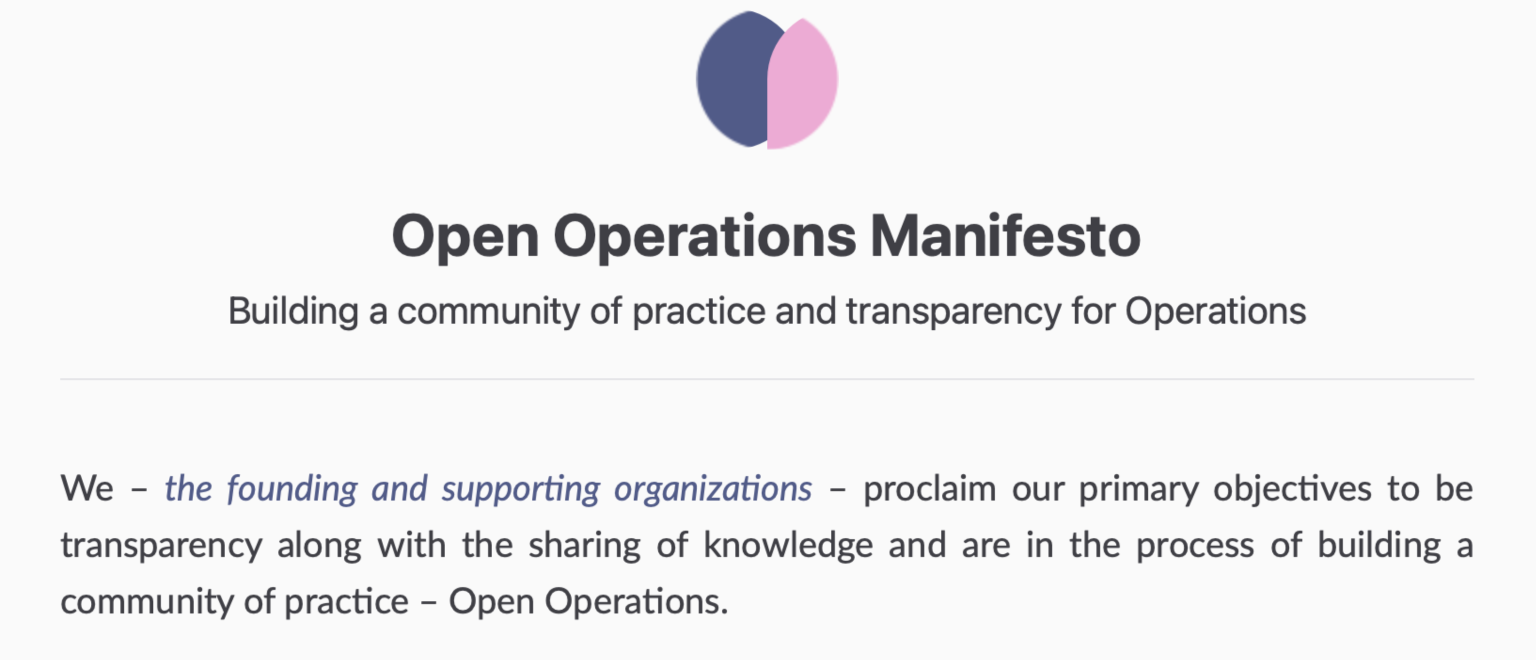
ALASCA

https://scs.community

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

gaia-x

Open Operations



Open Operations Manifesto

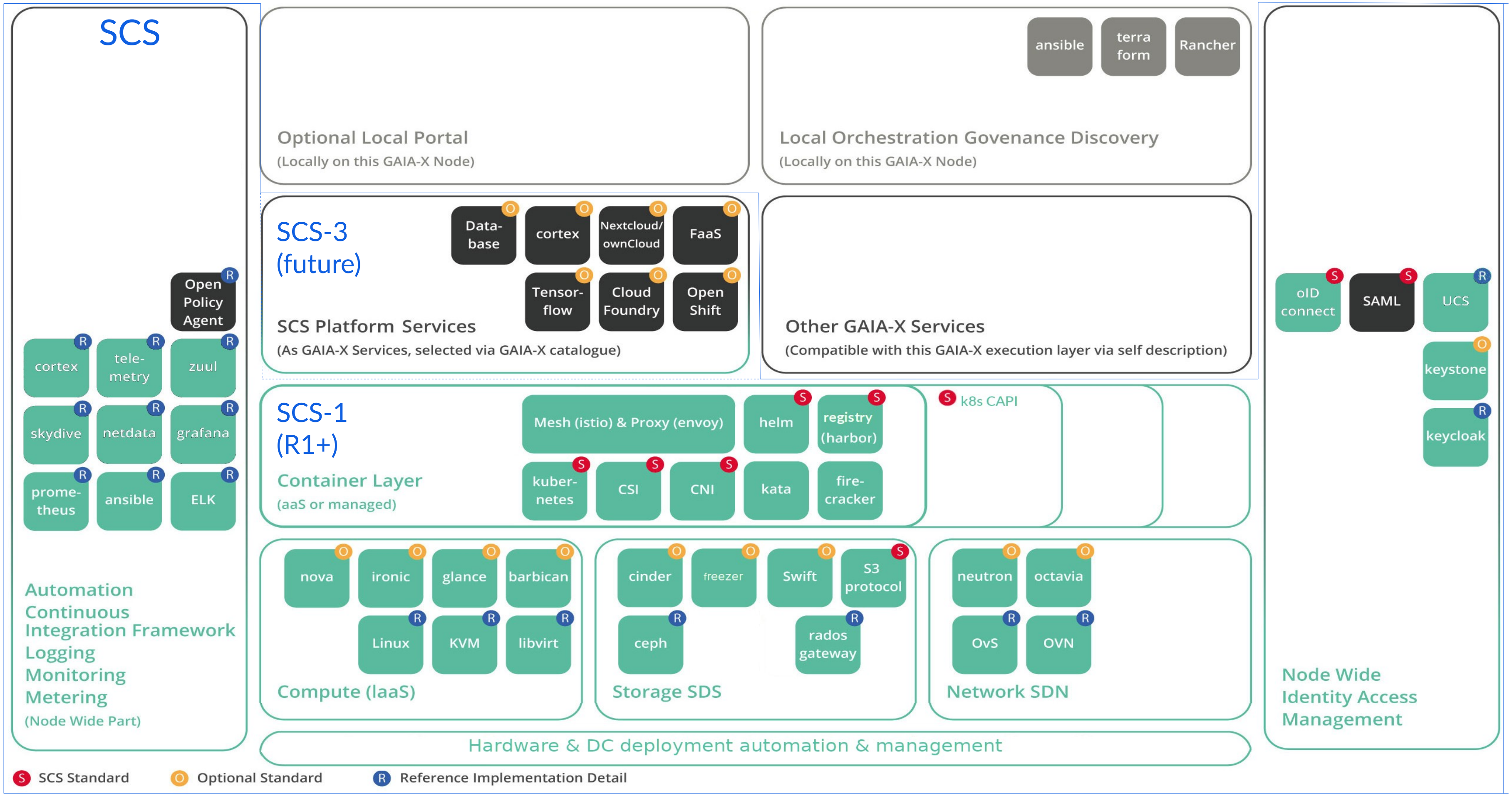
Building a community of practice and transparency for Operations

We – *the founding and supporting organizations* – proclaim our primary objectives to be transparency along with the sharing of knowledge and are in the process of building a community of practice – Open Operations.

https://openoperations.org

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

SCS Ref. Architecture (current status)



SCS

Open Policy Agent R

cortex R

tele-metry R

zuul R

skydive R

netdata R

grafana R

prome-theus R

ansible R

ELK R

Automation
Continuous Integration Framework
Logging
Monitoring
Metering
(Node Wide Part)

Optional Local Portal
(Locally on this GAIA-X Node)

ansible

terra form

Rancher

Local Orchestration Govenance Discovery
(Locally on this GAIA-X Node)

SCS-3 (future)

Data-base O

cortex O

Nextcloud/ ownCloud O

FaaS O

Tensor-flow O

Cloud Foundry O

Open Shift O

SCS Platform Services
(As GAIA-X Services, selected via GAIA-X catalogue)

Other GAIA-X Services
(Compatible with this GAIA-X execution layer via self description)

SCS-1 (R1+)

Mesh (istio) & Proxy (envoy)

helm S

registry (harbor) S

S k8s CAPI

kuber-netes S

CSI S

CNI S

kata

fire-cracker

Container Layer
(aaS or managed)

nova O

ironic O

glance O

barbican O

Linux R

KVM R

libvirt R

Compute (IaaS)

cinder O

freezer O

Swift O

S3 protocol S

ceph R

rados gateway R

Storage SDS

neutron O

octavia O

OvS R

OVN R

Network SDN

oID connect S

SAML S

UCS R

keystone O

keycloak R

Node Wide
Identity Access
Management

Hardware & DC deployment automation & management

S SCS Standard   O Optional Standard   R Reference Implementation Detail

Dark squares:
future

SCS: Achievements

- Public Cloud offerings built with SCS reference implementation:

BETACLOUD wavestack OPEN+

- Bundesamt für Sicherheit in der Informationstechnik BSI C5-Certification of *pluscloud open*
- Release 3 (2022-09-21), Release 4 (2023-03-22)
- Infrastructure layer for Gaia-X FEDERATION SERVICES GXFS created
- In evaluation or built up in various organizations (industry, administration, science)
- Building block of the Deutsche Verwaltungscloud-Strategie of the IT-Planungsrat
- Proof of Concept with dataport
- Active & growing community

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Active & growing community (companies)

23 | Technologies

B1 SYSTEMS

SPRIN-D

Bundesministerium für Wirtschaft und Klimaschutz

cleura

CLOUD & HEAT

[C] CLOUDICAL

dataport

_dilossacon

GONICUS PIONEERS OF OPEN SOURCE

gridscale

LEITWERK Die Zukunft Ihrer IT

noris network

Open Infrastructure FOUNDATION

OSB Open Source Business ALLIANCE Bundesverband für digitale Souveränität e.V.

T

OX Stay Open.

OSISM

OVHcloud

plusserver

Stackable

StackHPC

Syself

univention be open

WAVECON

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

gaia-x

SCS standards

SCS: Why standardization?

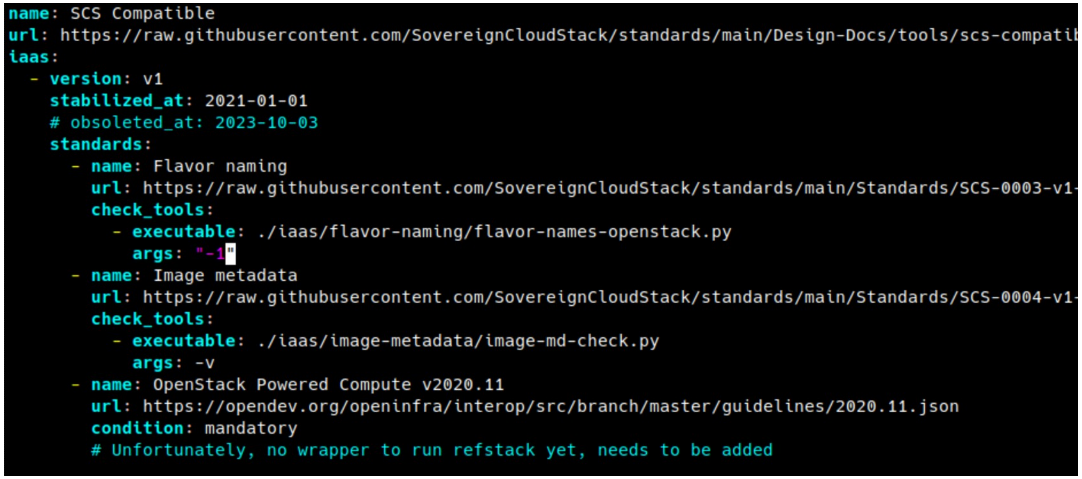
- Real choice (2nd dimension DigiSov) requires lock-in-less choice
  - Technically fully technically compatible providers available
  - Self-Hosting fully compatible infrastructure must be realistic
- „Virtual Hyperscaler“ vision
  - Users can leverage many clouds as one
  - Requires common feature set, common APIs, common system behavior (baseline)
  - Requires user federation
- Enables joint development, joint operational practices

SCS: Standardization process

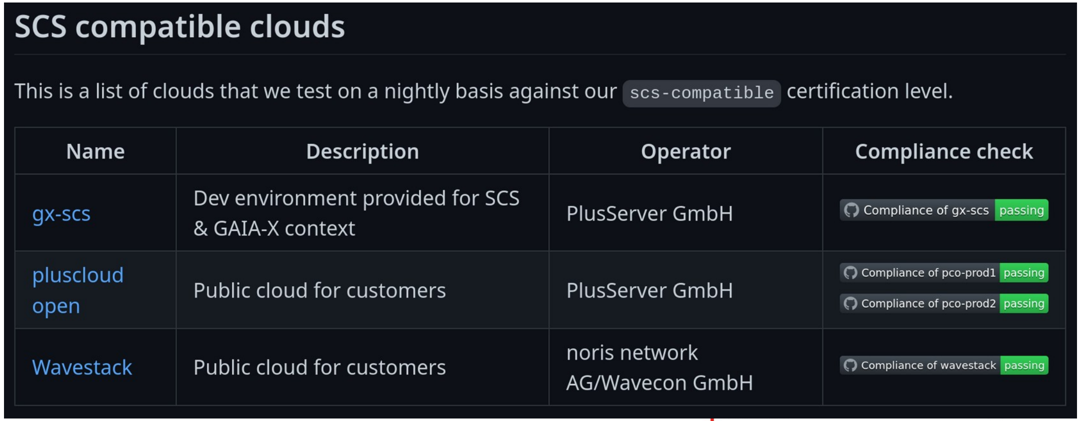
- Preference to leverage/reference/contribute to existing upstream standards
- Process: Described in gh:SCS/standards/Standards/SCS-0001-v1
  - Lifecycle: Pre-merge Draft → Merged Draft → Stabilized (or Rejection) → Deprecation (all via github PRs)
  - Standards are versioned
  - Discussed in SCS technical teams, reach out to broader communities when useful, get operator feedback
  - Standards should come with compliance check tools
- Driven by interoperability needs from users (DevOps teams that operate workloads on SCS infra)
  - Internal needs: Container layer creates InterOp requirements to Infra layer, platform services to container layer
- Standards are extensible
  - Common baseline, growing over time, overdelivery allowed
- IaaS and KaaS layers currently (both also requiring IAM Federation), Platform services in the future
- Current focus on SCS-compatible, openness checks (SBOM) and open operations standards in the future

SCS certification testing framework

- Defined in gh:SCS/standards/Standards/scs-0003-v1
- YAML file, defining a version X of certification requirements valid in a timespan for a layer (currently iaas or kaas), listing all needed (mandatory and optional) standards (SCS and upstream) along with compliance tests
- Test tool gh:SCS/standards/Tests/scs-compliance-check.py that can be run (with normal customer privileges!) against IaaS or KaaS under test
- Available as docker container
- Continuous compliance monitoring (github action)



```yaml
name: SCS Compatible
url: https://raw.githubusercontent.com/SovereignCloudStack/standards/main/Design-Docs/tools/scs-compatib
iaas:
  - version: v1
    stabilized_at: 2021-01-01
    # obsoleted_at: 2023-10-03
    standards:
      - name: Flavor naming
        url: https://raw.githubusercontent.com/SovereignCloudStack/standards/main/Standards/SCS-0003-v1-
        check_tools:
          - executable: ./iaas/flavor-naming/flavor-names-openstack.py
            args: "-1"
      - name: Image metadata
        url: https://raw.githubusercontent.com/SovereignCloudStack/standards/main/Standards/SCS-0004-v1-
        check_tools:
          - executable: ./iaas/image-metadata/image-md-check.py
            args: -v
      - name: OpenStack Powered Compute v2020.11
        url: https://opendev.org/openinfra/interop/src/branch/master/guidelines/2020.11.json
        condition: mandatory
        # Unfortunately, no wrapper to run refstack yet, needs to be added
```



SCS compatible clouds

This is a list of clouds that we test on a nightly basis against our `scs-compatible` certification level.

Name	Description	Operator	Compliance check
gx-scs	Dev environment provided for SCS & GAIA-X context	PlusServer GmbH	Compliance of gx-scs passing
pluscloud open	Public cloud for customers	PlusServer GmbH	Compliance of pco-prod1 passing Compliance of pco-prod2 passing
Wavestack	Public cloud for customers	noris network AG/Wavecon GmbH	Compliance of wavestack passing

SCS compatible on IaaS layer (1)

What	Why	Status	Tests	References	
Systematic Flavor-naming	Allow IaC to work across clouds (incl. k8s-capi-provider)	V1 done (mandatory) V2 draft (mandatory?)	Done Done	flavor-naming scs-0100-v2	R
Mandatory flavors	Allow IaC to work across clouds (incl. k8s-capi-provider)	V1 done (mandatory) V2 draft (mandatory?) V3 ADR for SSD flavors	Done Done Implicit	flavor-naming scs-0100-v2 scs-0110-v1	R
Flavor discoverability	IaC: Discover properties beyond vCPU/RAM/ Disk	TBD (extend and standardize extra_specs)	TBD		
Image metadata	Transparency on image properties (e.g. login, build date) and update promises	V1 done (mandatory)	Done	Image-Properties	R

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

SCS compatible on IaaS layer (2)

What	Why	Status	Tests	References	
Entropy for VMs	Workloads (encryption) expect there to be enough ...	Draft	TBD	standards/#210	R
IPv4 networking: Local networks FIPs for public net	Common source of divergence	Idea		issues/#167	R
IPv6 networking: Local networks Public Prov. network	ditto	Idea		issues/#166	
Metadata source (w/ user-data, vendor-data)	Required for customization of VMs	Idea			R

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

SCS compatible on IaaS layer (3)

What	Why	Status	Tests	References
DNS and NTP for VMs	Working DNS without outgoing internet access, correct system time	Draft Draft	TBD TBD	issues/#229 issues/#230 issues/#231
Domain admin role	Allow project creation, user management as self-service (resellers)	Idea – various workarounds (policies, APIs exist), upstream disucssions started	TBD	issues/#184
Identity federation via OIDC	Federate users from federated clouds	Blog post (device auth grant flow needed)	TBD	Blog
OpenStack powered Compute 2022.11	Baseline	Done (Upstream)	Refstack in Ref.Impl. but not generic	Guidelines

r

R

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

SCS compatible on IaaS layer (4)

What	Why	Status	Tests	References
L3 loadbalancer (OVN)	Needed for good externalTrafficPolicy: Local support	WIP	TBD	issues/#251
Definition of AZ	Availability expectations when spreading over AZs	Idea: Meaningful level of independence (power, net, fire, cooling, …)	TBD	
Definition of Region	What is shared?	Idea: Share identities, replicate images	TBD	

r

r

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

SCS compatible on KaaS layer (1)

What	Why	Status	Tests	References	
CNCF conformance tests	Baseline	Done	sonobuoy	Test driver	R
Offered K8s version recency	Security baseline	ADR Done	TBD	SCS-0210-v1	R
K8s version support period	Avoid enforcing unneeded churn	Idea: (Support minor version at least as long upstream does)	TBD		R
Default storage class properties	Reasonable default storage always available	ADR Done	TBD	SCS-0211-v1	R
Additional storage classes (IOPS, RWX)	RWX needed by some workloads; IOPS to allow for storage performance	WIP	TBD	issues/#214	
Anti-affinity (soft for workers)	Availability expectations from deployed workloads	WIP	TBD	issues/#226	R

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

SCS compatible on KaaS layer (2)

What	Why	Status	Tests	References
CNI with network policies	Network controls needed for security	TBW	TBD	issues/#211
Ingress / Gateway service (opt-in) with client IPs	Allow customers to do access control	WIP	TBD	
Identity federation via OIDC	Allow to reuse identities from underlying cloud or external IdP	Research	TBD	issues/#194
Machine identities	The controlling infra knows who you are … Avoid complexity.	Idea	TBD	issues/#163

R

R

SCS compatible on KaaS layer (3)

What	Why	Status	Tests	References
Control plane backup/ maintenance	Avoid losing cluster status	TBW	TBD	k8s-capi/#258
Kube API access controls	Customer requests	WIP	TBD	k8s-capi/#246
Metrics service (opt-out)	Standardized service needs to be available	WIP	TBD	issues/#224
Container registry (opt-in)	Very popular demand	WIP	TBD	issues/#263

r

r

R

r

SCS compatible on KaaS layer (4)

What	Why	Status	Tests	References
Cluster management API	Unified cluster lifecycle management (capi / Gardener style)	Research	TBD	issues/#181
Gitops controller for Cluster Mmgt	Vision	Research	TBD	

SCS Standardization: Present and Future

- 2022 focus was on reference implementation, 2023 focus is on standards
  - Tender package finally awarded (waiting for release of funds)
- SCS standards are meant to be implementable in more than one way
- Most of the above mentioned standards are already implemented (R) or partially implemented (r) in the Ref. Impl. - normally a prerequisite for finalizing a standard
- Not every above mentioned discussion necessarily ends up being a mandatory standard
- The more operators join the more useful the standards
- Standardization just started – largest part ahead of us
- Join us if you agree with the fundamental approach
  - Team meets, github (standards and issue repos: issues, PRs)

Sovereign Cloud Stack

An OSB ALLIANCE project

https://scs.community

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

gaia-x

https://scs.community/

//