Sovereign Cloud Stack

gaia-x

Sovereign Cloud Stack

Open Source Cloud & Container Stack for Federated Sovereign Infrastructure (Gaia-X)

Using Sovereign Cloud Stack to Achieve Digital Sovereignty

Dr. Manuela Urban, **Kurt Garloff**, Dirk Loßack, Eduard Itrich,
Felix Kronlage-Dammers, Bianca Hollery-Pfister (OSB Alliance e.V.)

project@scs.sovereignit.de

Cloud Expo Europe, 2022-05-11

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

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Digital Sovereignty … What?

Sovereign Cloud Stack
An OSB ALLIANCE project

aws

HETZNER

IONOS

Google Cloud

T-Systems Sovereign Cloud powered by Google Cloud
Volle Public Cloud Funktionalität für die Digitalisierung – volle Souveränität inklusive

Open Telekom Cloud

STACKIT
CLOUD & HEAT

Azure

Kick Start for the First Sovereign Cloud Platform for the Public Sector in Germany: SAP and Arvato Systems Announce Partnership
February 3, 2022 by SAP News

OVH.com

Stack HPC

Alibaba Cloud

vmware vCloud

cleura

gridscale

plusserver

HUAWEI

ORACLE CLOUD

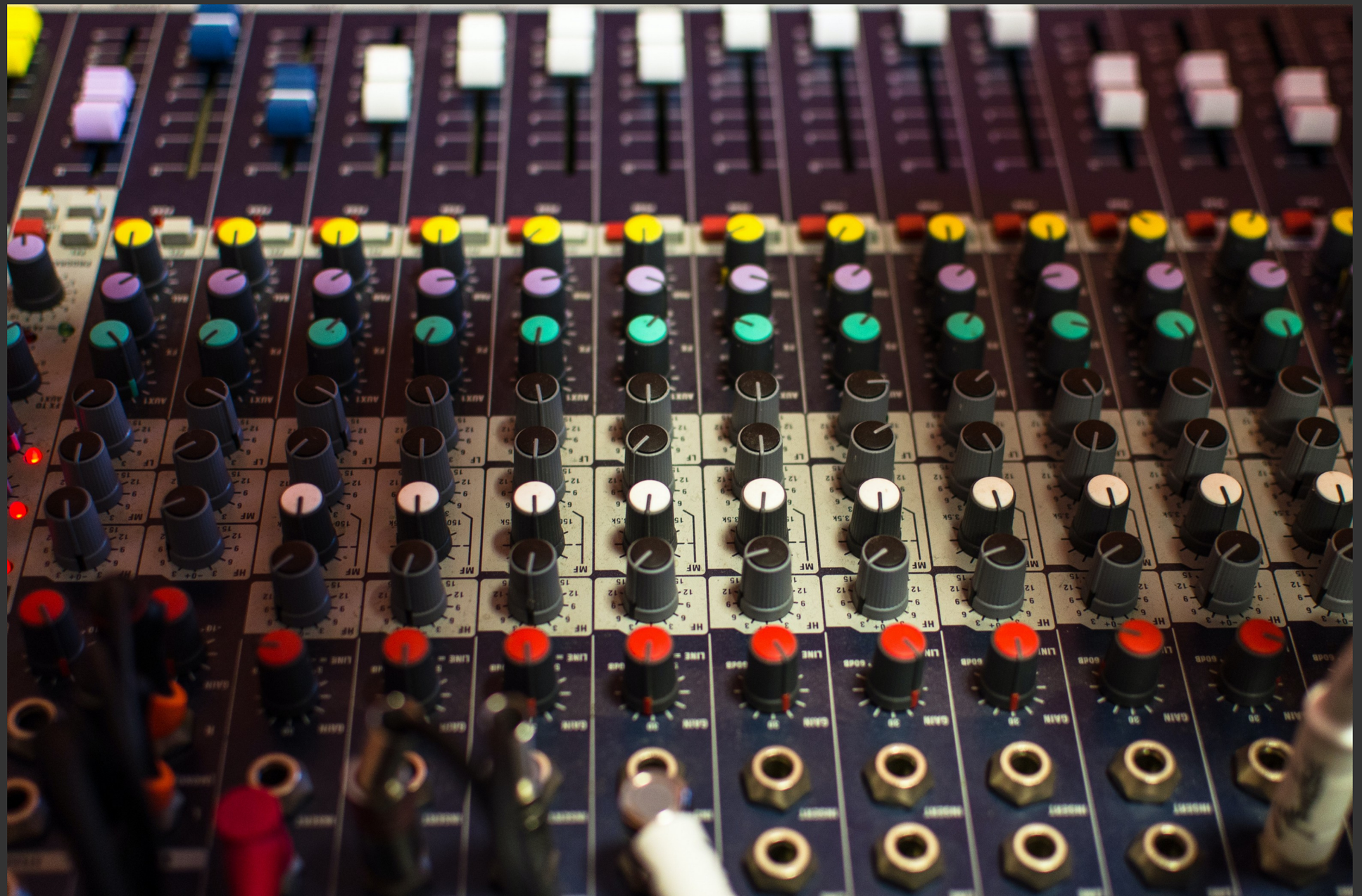
NUTANIX

DigitalOcean

VEXXHOST

gaia-x

Who is in control?



Levels of sovereignty

Sovereign Cloud Stack
An OSB ALLIANCE project

None	Data protection	Choice	Shape Technology	Operational Skills
	GDPR	Strong Interoperability	Software Transparency	Operational Transparency
	ENISA		*Fully* Open Source	Education
	Gaia-X labels	Many Vendors / Operators	Open Development	Open Operations
	Confid. Computing		Open Community	

Recommendation: Thu, 11:15, Digi Trans Keynote Theatre:
Peter Ganten: Digital Sovereignty and the Cloud: Everything is at stake

gaia-x

Sovereign Cloud Stack

An OSB ALLIANCE project

Openness?

Transparency?

gaia-x

Sovereign Data requires ...

… sovereign infrastructure …

2010

and it‘d better be solid

2018

Sovereign Cloud Stack vision

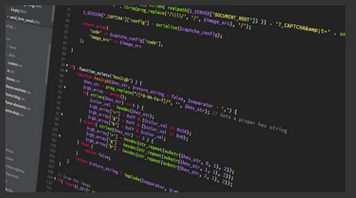
Sovereign Cloud Stack
An OSB ALLIANCE project

None | Data protection | Choice | Shape Technology | Operational Skills

Achieve all levels of digital sovereignty

1) GDPR / Data protection / Data security

2) Real choice by many (collaborating!) providers with strong interoperability: Standardization & Certification



3) Fully open functional stack (Four Opens, OSS Health Check) as reference implementation

4) Full transparency over operations stack, operational practices (Open Operations)

gaia-x

Sovereign Cloud Stack project

Started end of 2019

Funded by BMWK (German Fed. Min. for Economic Affairs & Climate Action) since summer 2021

Run by Open Source Business Alliance e.V. with half a dozen employees (growing to a dozen)

Open Community contributions

Paid contractor work (awarded via public tenders)

Closely working with Gaia-X

SCS project is neutral orchestrator within the SCS ecosystem, partners do business as CSP, services providers, etc.

Project page: https://scs.community/

1 - Security by Design

Using strong isolation for container clusters

- Different tenants receive their own Kubernetes clusters; by default, no cluster sharing happens
- Underlaying VMs, network, storage are separated by strong virtualization barriers

Private registry for users

- Make it easy for DevOps teams to enforce their own security vetting processes and control their supply chain
- Vulnerability scanning included in regristry solution

Daily patching supported

- The architecture is built for daily patching (or redeployment) without noticable customer impact
- This creates a practice of keeping the systems up to date especially with respect to security patches

Secure Operational practices

- Document updating, patching, security response, … processes to help with secure operations

Air gap mode supported

- Deploying and updating without internet connection possible
- Leveraging an internal registry and patch distribution mechanism (includes vulnerability scanning)

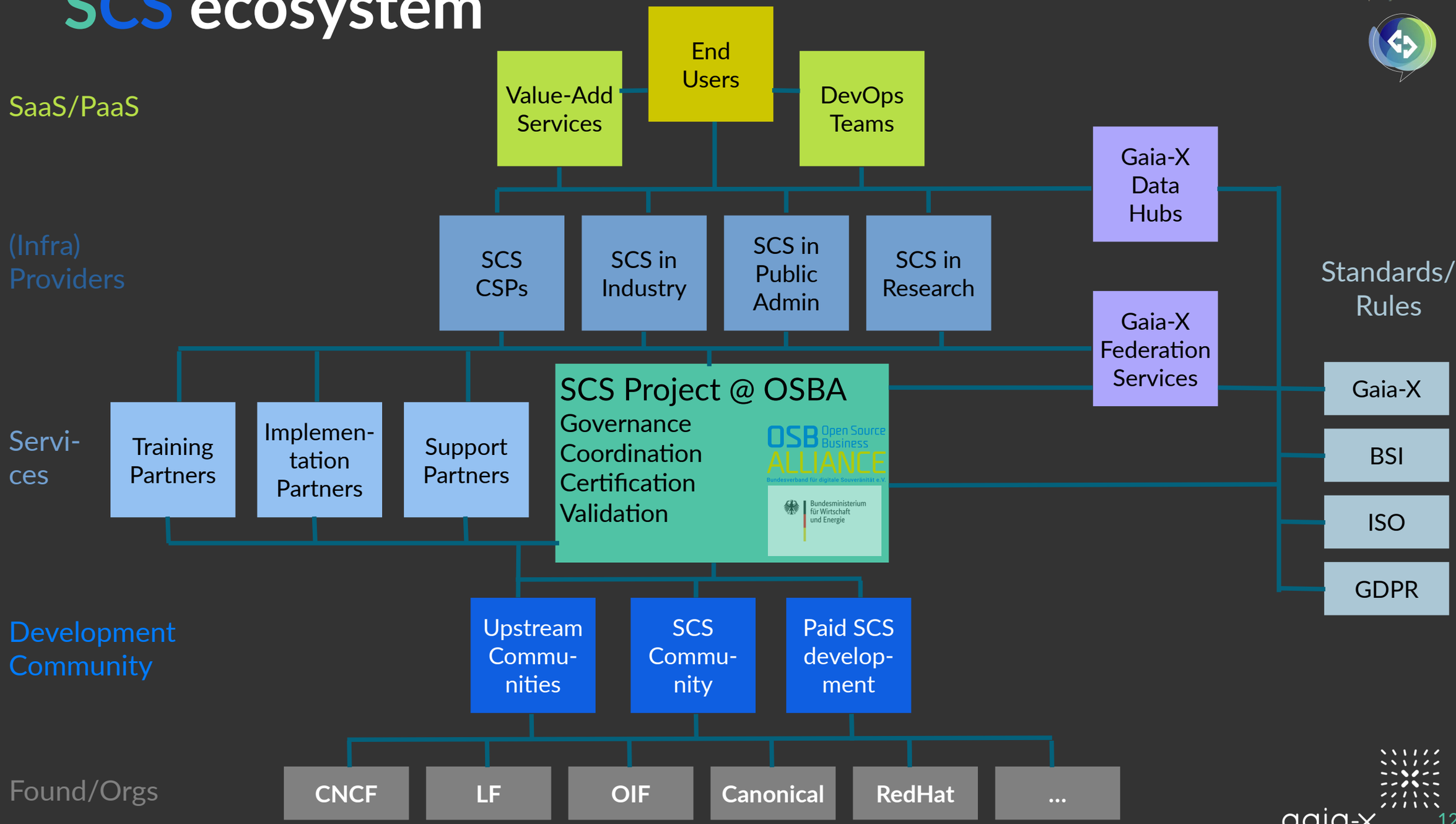
Certification

- Budget for security certifications (BSI) with partners – SCS based PlusCloud Open achieved BSI C5 in Nov 2021
- Pen testing planned (and budget allocated)

Supply chain security

- Work with researchers on further improving supply chain security (reproducible builds, scanning, ...)

SCS ecosystem



2 - SCS choice ...

Sovereign Cloud Stack
An OSB ALLIANCE project

SCS

aws

HETZNER

IONOS

Google Cloud

Open Telekom Cloud

STACKIT
CLOUD & HEAT

Azure

OVH.com

Stack HPC

Alibaba Cloud

vmware vCloud

cleura

gridscale

plusserver

HUAWEI

ORACLE CLOUD

NUTANIX

DigitalOcean

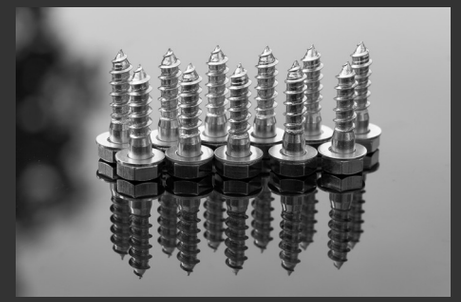
VEXXHOST

gaia-x

2 - SCS standards & certification

Reuse existing Open Standards

- Must have a fully open and capable (reference) implementation
- Ideally with conformance tests
- Examples: CNCF conformance tests, S3, OIDC, OpenStack powered trademark tests
- Contribute improvements (e.g. tests) back upstream
- Gaia-X self-descriptions (in development)



SCS: Fill gaps (for PaaS/SaaS DevOps teams)

- Done: IaaS flavor naming and standard flavors
- Done: Image metadata
- WIP: Definition of regions, availability zones, ...
- WIP: k8s cluster management (k8s cluster-API)

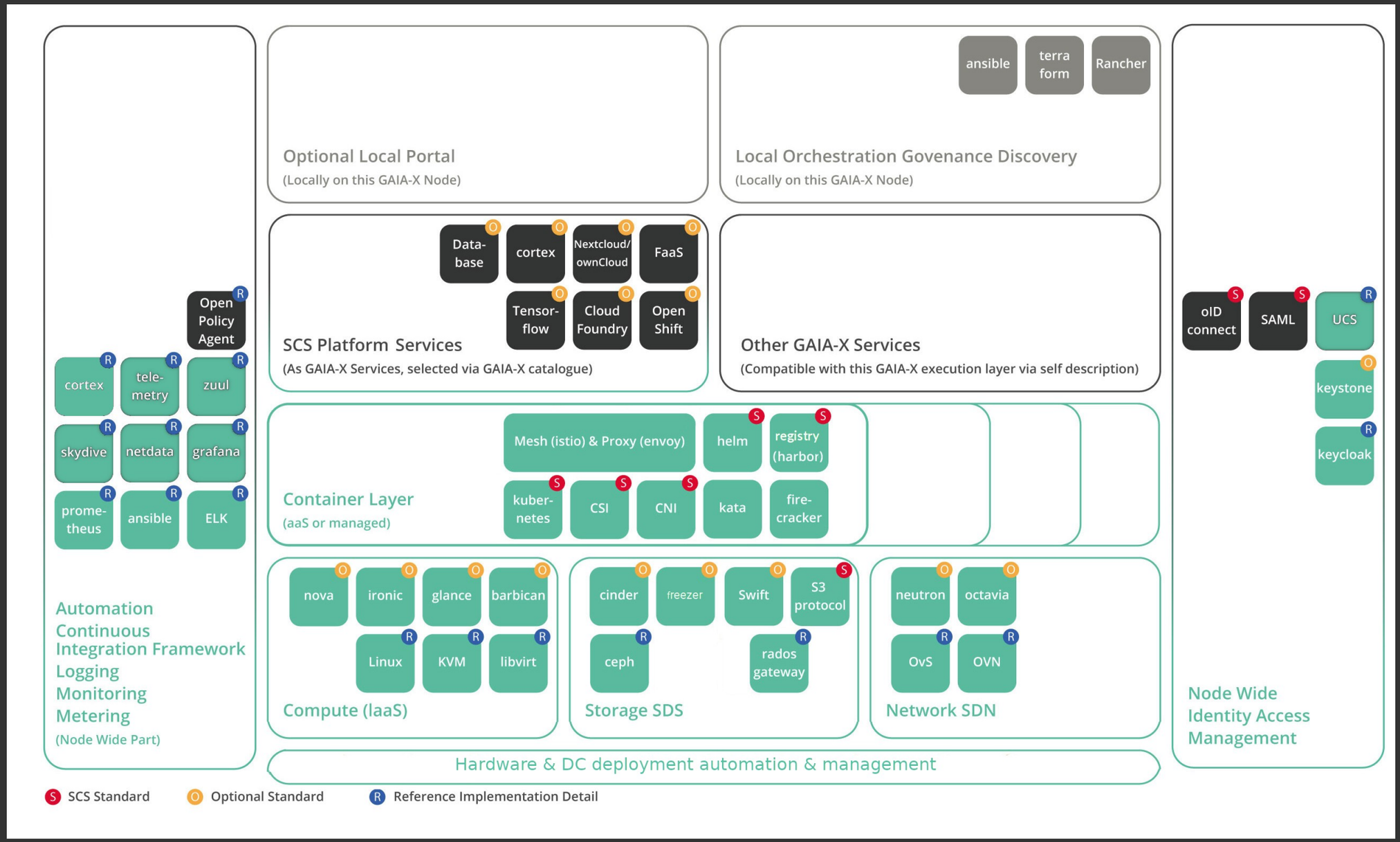
Federation

- Allow OIDC user federation

Formal SCS certification program to be launched this summer for CSPs

- SCS compatible: Compatibility / Interoperability testing
- SCS open: Technological transparency (fully open functional stack)
- SCS sovereign (later): Operational transparency

3 - SCS reference implementation architecture



3 - SCS reference implementation status

Sovereign Cloud Stack
An OSB ALLIANCE project

Consists of OSI compliant (OSS helath check surviving) upstream components

- Participating in & contributing to upstream communities

All SCS work fully OSS (github.com/SovereignCloudStack)

- Modular code, developed by growing community in an agile way

Release R2 (v3.0.0) from 2022-03-23

- Secure, Stable & sustainable base layer (OSISM) w/ Bare Metal automation
- Complete IaaS stack (includes OpenStack Xena)
- Ready for federation (OIDC) & GXFS
- Operational stack (Lifecycle Management, Monitoring, Alerting, ...) included
- K8s Cluster-API based container cluster management (KaaS) – API/CLI only

Roadmap for R3 (Sept 2022)

- Encrypt all data at rest (opt-out possible)
- Standardize k8s cluster management across providers (also for non-SCS IaaS)
- Strengthen CI framework and coverage
- Conformance tests (IaaS)
- Document and validate a set of IAM federation use cases
- Later: PaaS, Edge setups, Network encryption, ...

GREEN IT CIS

gaia-x

3 - SCS reference implementation adoption

Two public clouds in production with complete SCS stacks since > 1 year

BETACLOUD

OPEN

PlusCloud achieved a BSI C5 certification in Nov ‘21

SCS validated in Gaia-X Hackathons and Betacloud & PlusCloud customers

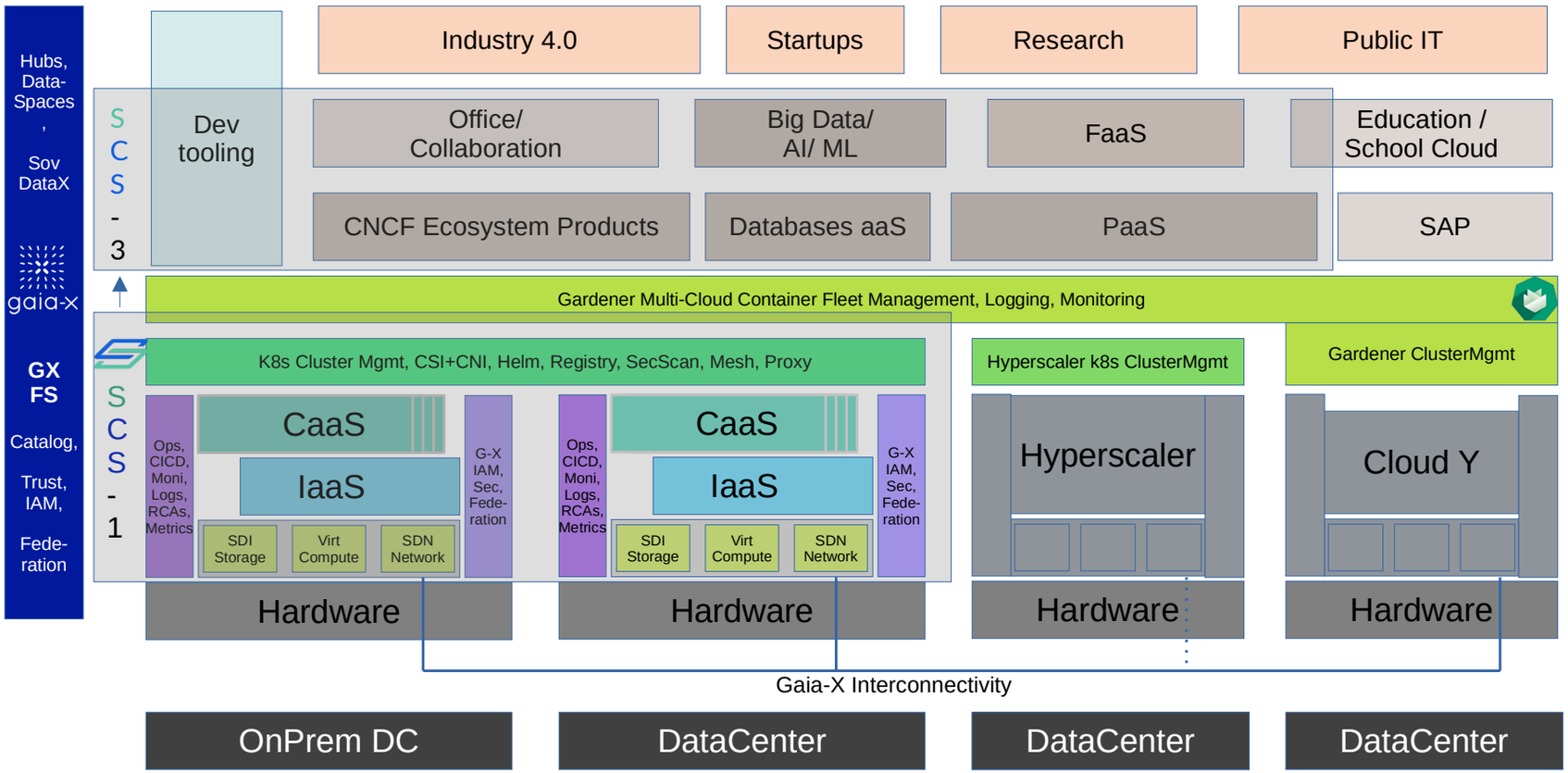
Adoption continues...

- Soon: Third public cloud (with full SCS)
- PoCs in industry and with public sector IT providers (DE)
- Modules used by various partners (see logos on homepage)
- Ecosystem of service companies emerging (training, consulting, implementation, support, ...)
- Standards adoption via certification program

Gaia-X

- Collaboration with Gaia-X Federation Services
- Usage in Gaia-X projects

2/3 - Building federated clouds

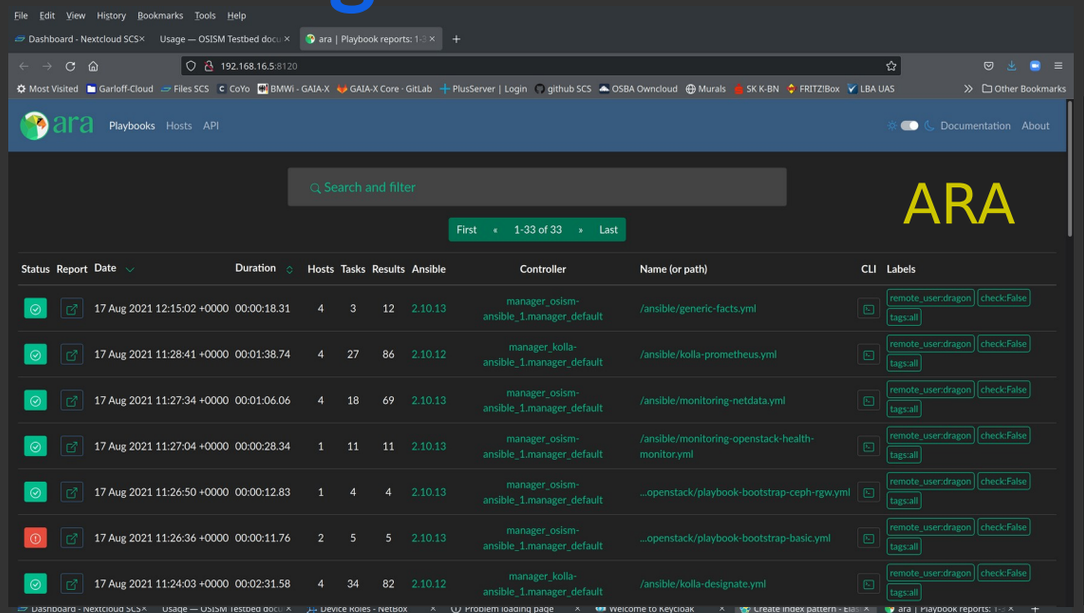


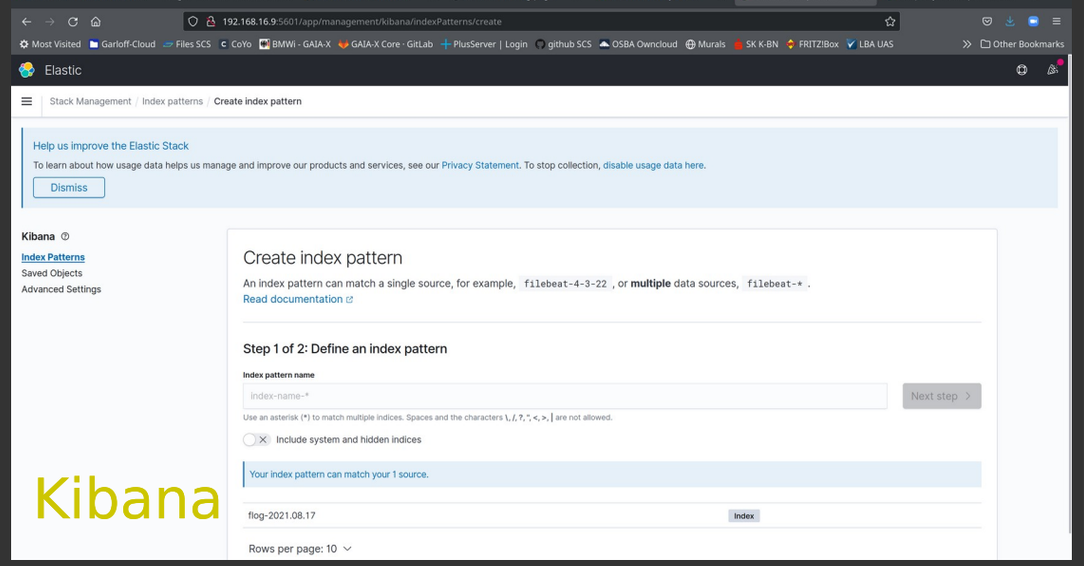
Adapted from Acatech Whitepaper on Digital Sovereignty (3/2021)

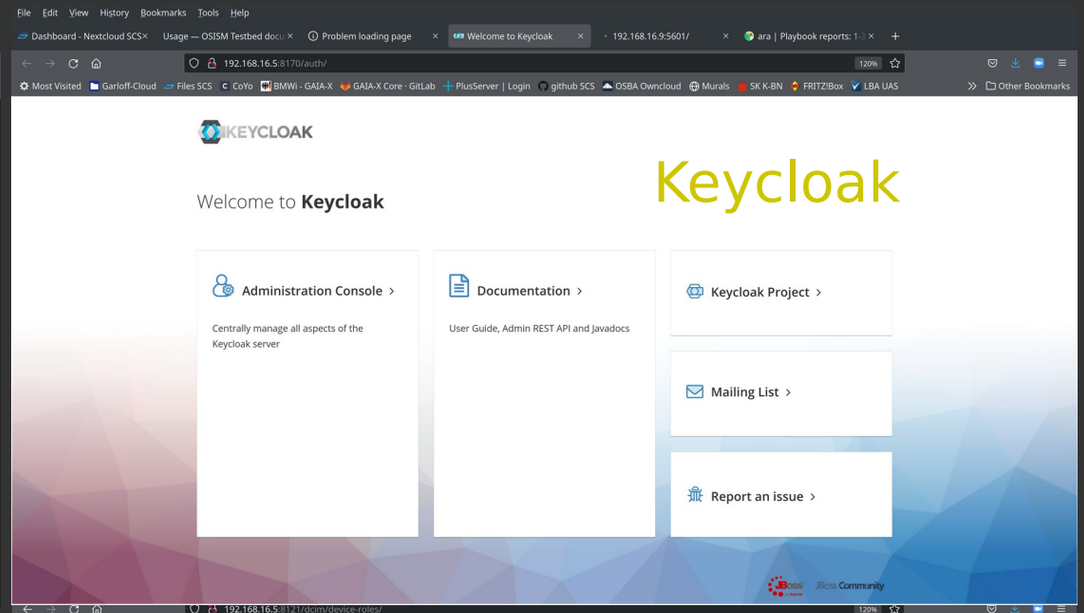
4 - Addressing the Operations challenge:

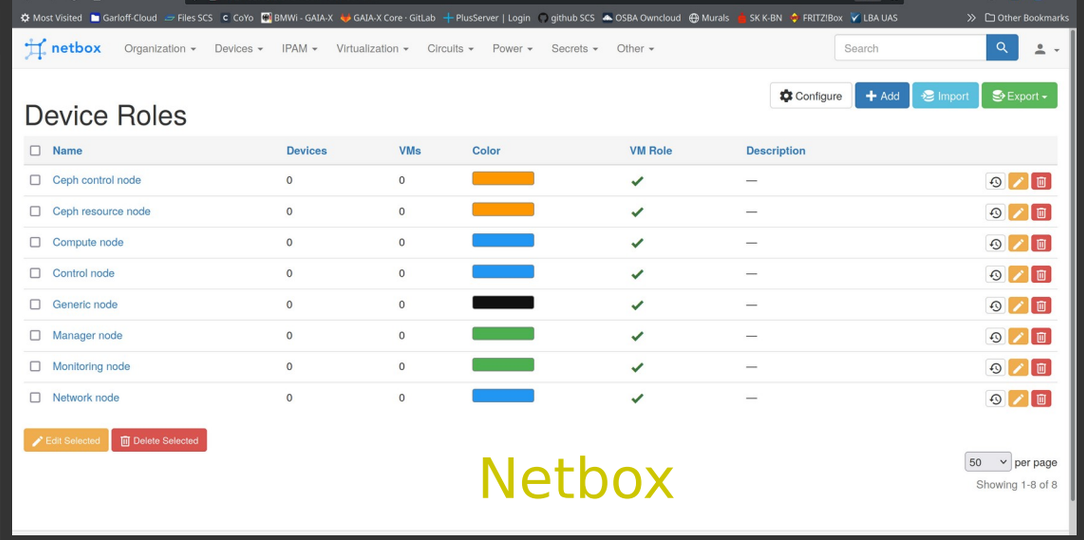
Tooling

Sovereign Cloud Stack
An OSB ALLIANCE project









gaia-x

4 - Operations:

Measure what you want to manage ...

openstack-health-monitor: Black-box monitoring

4 - Addressing the Operations challenge: Towards fully Open Operations

Sovereign Cloud Stack
An OSB ALLIANCE project

More tooling (well documented and configured)

- Monitoring, Alerting, Trending
- Patching (LCM) & CI/CD

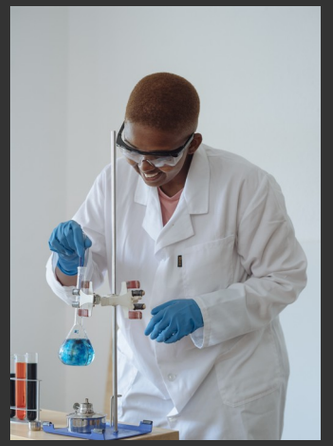
Documenting and sharing best practices

Transparent Issue resolution

- Public RCAs

Public dashboard / status page

- e.g. OpenStack Health Monitor (or successor from TSI)



gaia-x

Join the growing SCS community!

Sovereign Cloud Stack
An OSB ALLIANCE project

As CSP or industry IT department
- Join discussions / community
- Adopt standards
- Adopt technology (code)

As OSS infrastructure software developer
- Contribute / Participate in community
- Apply for a job in our OSB Alliance team

As interested company
- Build SCS expertise
- Respond to tenders
- Build business model around SCS expertise

As PaaS/SaaS developer
- Develop / Test against SCS standards

As IT consumer
- Request true sovereignty from your platform

More information:

Homepage:
https://scs.community/
Github:
https://github.com/SovereignCloudStack

Booth E155 (3.1) at CEE
(Other Confs: OIF summit, CloudLand, ...)

Gaia-X: MVG OWP, Hackathons,
WGs FS/OSS, Svc. Char.

Email: project@scs.sovereignit.de
Matrix: SCS rooms