

# 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](mailto:project@scs.sovereignit.de)

ParlDigi Dinner, Bern (CH), 2022-06-15

Gefördert durch:

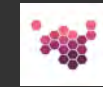
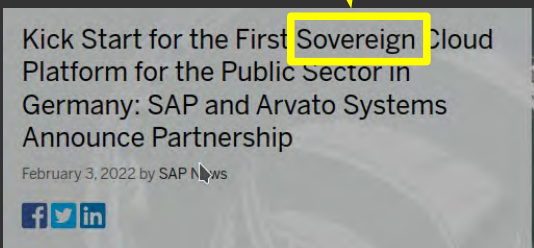
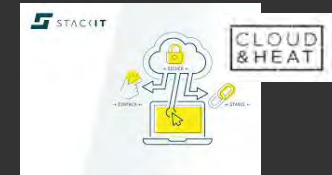


Bundesministerium  
für Wirtschaft  
und Klimaschutz

aufgrund eines Beschlusses  
des Deutschen Bundestages



# Digital Sovereignty ... What?





# Digital Sovereignty

„There must [...] be a sovereign government. Sovereignty is supreme authority, an authority which is independent of any other earthly authority. Sovereignty in the strict and narrowest sense of the term includes, therefore, independence all around, within and without the borders of the country.“

- LFL Oppenheim, 1905

“Digitale Souveränität eines Staates oder einer Organisation umfasst zwingend die vollständige Kontrolle über gespeicherte und verarbeitete Daten sowie die unabhängige Entscheidung darüber, wer darauf zugreifen darf. Sie umfasst weiterhin die Fähigkeit, technologische Komponenten und Systeme eigenständig zu entwickeln, zu verändern, zu kontrollieren und durch andere Komponenten zu ergänzen.

- Digitale Souveränität und Künstliche Intelligenz, Digitalgipfel 2018





# Digital Sovereignty – Open Source



“Digital Technology and Digital Sovereignty [...] and we define it as the capacity to be able to act and to reduce vulnerabilities. So it’s twofold. The one is really to reduce your weaknesses, where others can attack you.

And the other side is to be able to innovate, to develop by yourself, to set your own standards, to define the values you want to see in technology.

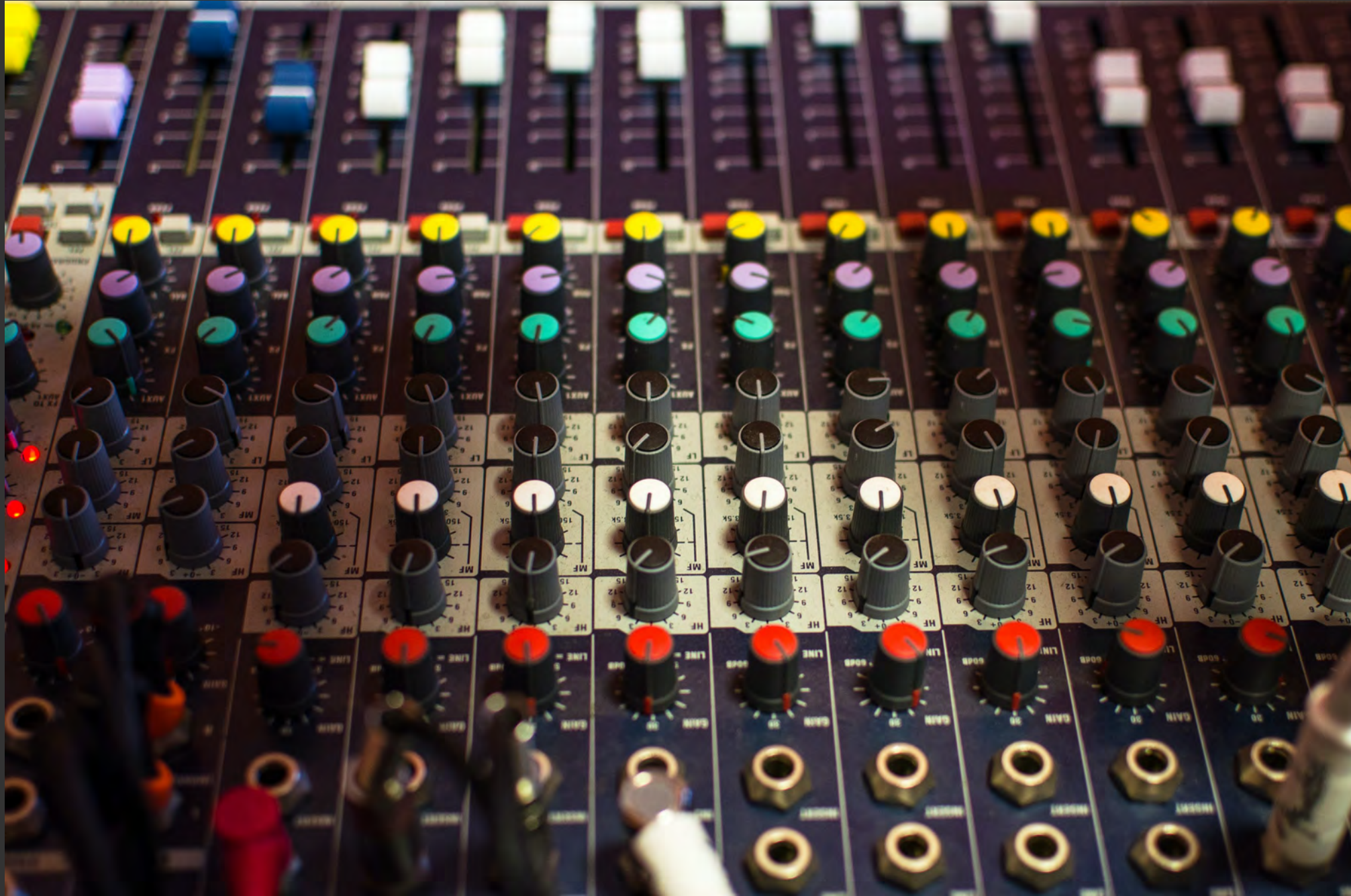
[...]

[Sovereign Tech Fund is specifically for open source software?] Only!”



Parldigi

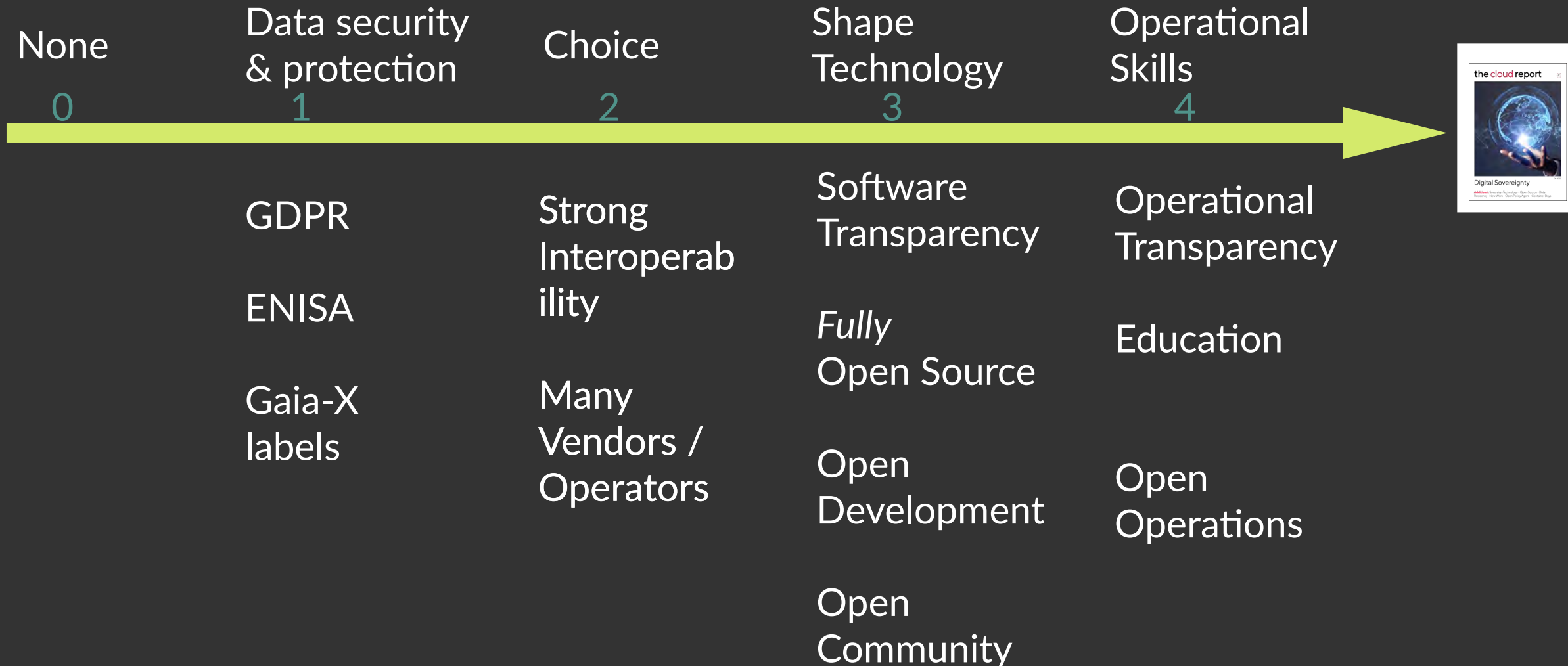
# Who is in control? Who can act?





Parldigi

# Levels of sovereignty



The Cloud Report 1/2022 <https://the-report.cloud/>  
<https://scs.community/de/2022/03/18/digital-sovereignty-whitepaper/>



# A pig with a lipstick ...



Local data centres of non-EU platforms

Cloud Act

Confidential Computing

Data decrypted for processing (exc homomorphic)

Availability issue remains

Local operations (with partner)

Availability issue only partially solved

No choice, no ability to shape

“Open”

Open Standards w/o Open Ref Implementation

Open Core / partial Open Source

Closed communities

No Operational knowledge sharing

“Transparent”

No public Root Cause Analysis

Very filtered public monitoring / status

# Sovereign Data requires ...





# ... sovereign infrastructure ...



# and it'd better be solid



Parldigi



2018

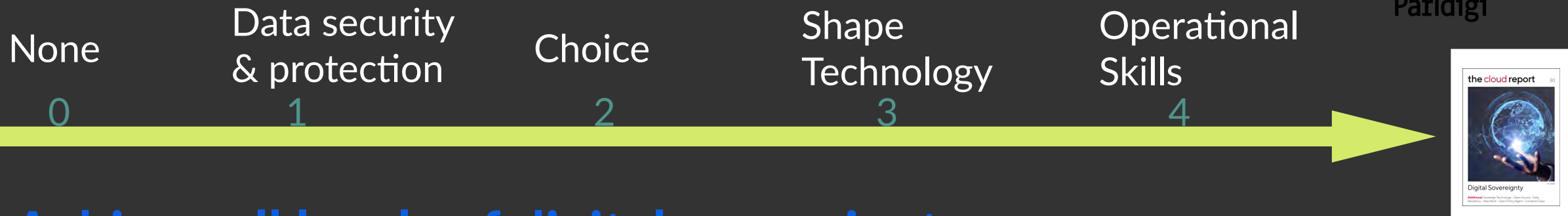
gaia-x





Parldigi

# Sovereign Cloud Stack vision



## Achieve all levels of digital sovereignty

- 1) GDPR / Data protection / Data security / availability
- 2) Real choice by many (collaborating!) providers with strong interoperability: Standardization, Certification, Federation
- 3) Fully open functional stack (Four Opens, OSS Health Check) as modular reference implementation
- 4) Full transparency over operations stack, operational practices, status, RCAs (Open Operations)



Avoiding fragmentation



# Sovereign Cloud Stack project



Parldigi

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/>





# Sovereign Cloud Stack and Gaia-X

## Gaia-X in One (Big) Figure

### Advanced Smart Services

(Cross-) Sector Innovation/ Marketplaces/ Applications

### Data Ecosystem



### Data Spaces

Interoperable & portable (Cross-) sector data-sets and services

### GAIA-X Federation services

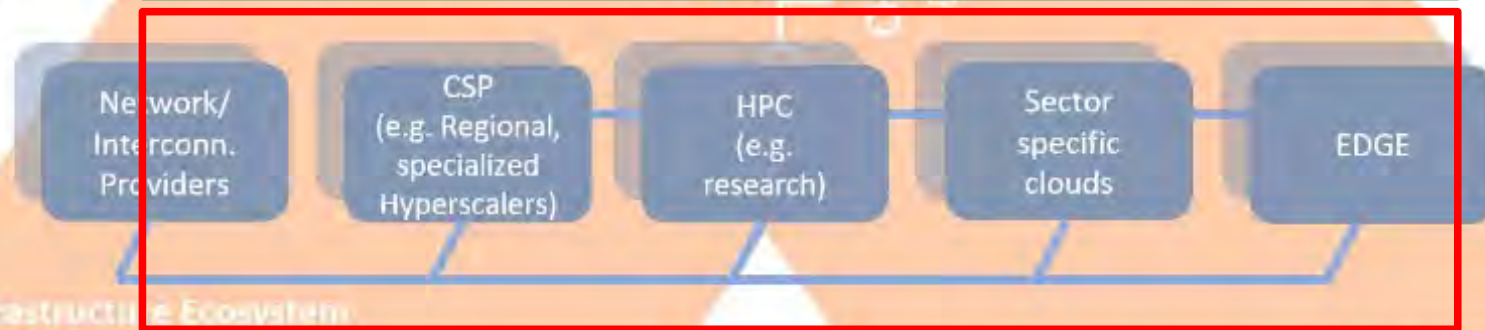
Federated & distributed for interoperability, trust & sovereignty services



GXFS

### Portability, Interoperability & Interconnectivity

Technical: Architecture of Standards  
Commercial: Policies



SCS

### Compliance

Legal: Regulation & Policies



# 1 - Security by Design

## Using strong isolation for container clusters

- Different tenants receive their own Kubernetes clusters; by default, no cluster sharing happens
- Underlying 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 registry solution

## Daily patching supported

- The architecture is built for daily patching (or redeployment) without noticeable 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

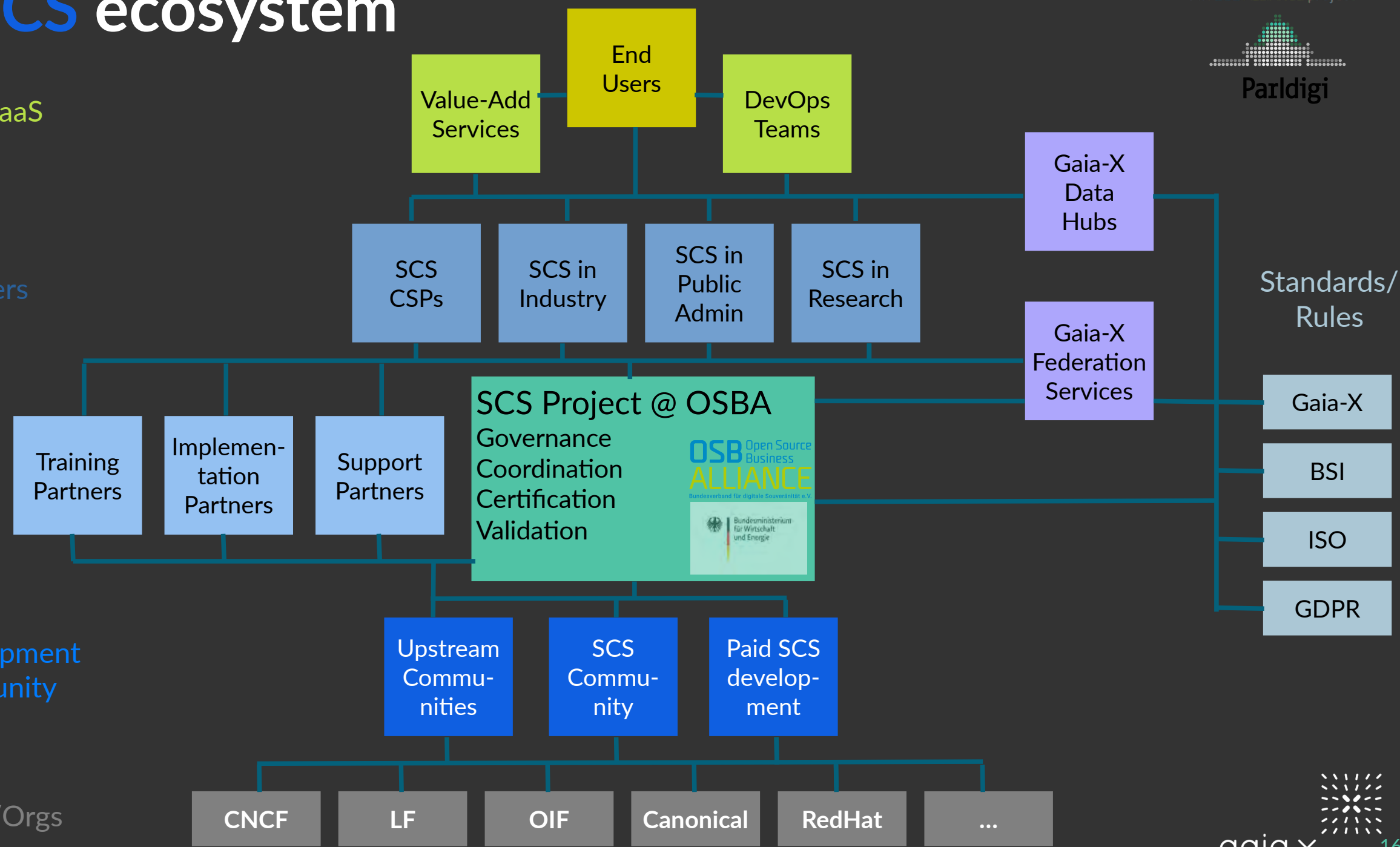
SaaS/PaaS

(Infra) Providers

Services

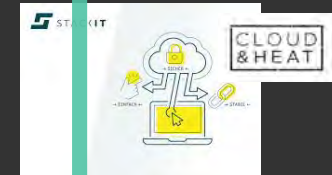
Development Community

Found/Orgs

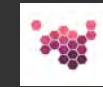




# 2 - SCS choice ...



SCS







# 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)

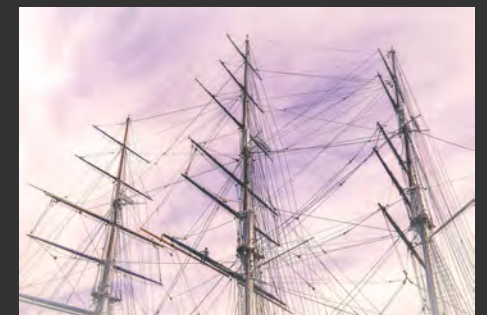
- Done: IaaS flavor naming and standard flavors
- Done: Image metadata
- WIP: Definition of regions, availability zones, ...
- WIP: k8s cluster management (k8s cluster-API)

## Federation

- Allow OIDC user federation

## Formal SCS certification program to be launched this summer for CSPs

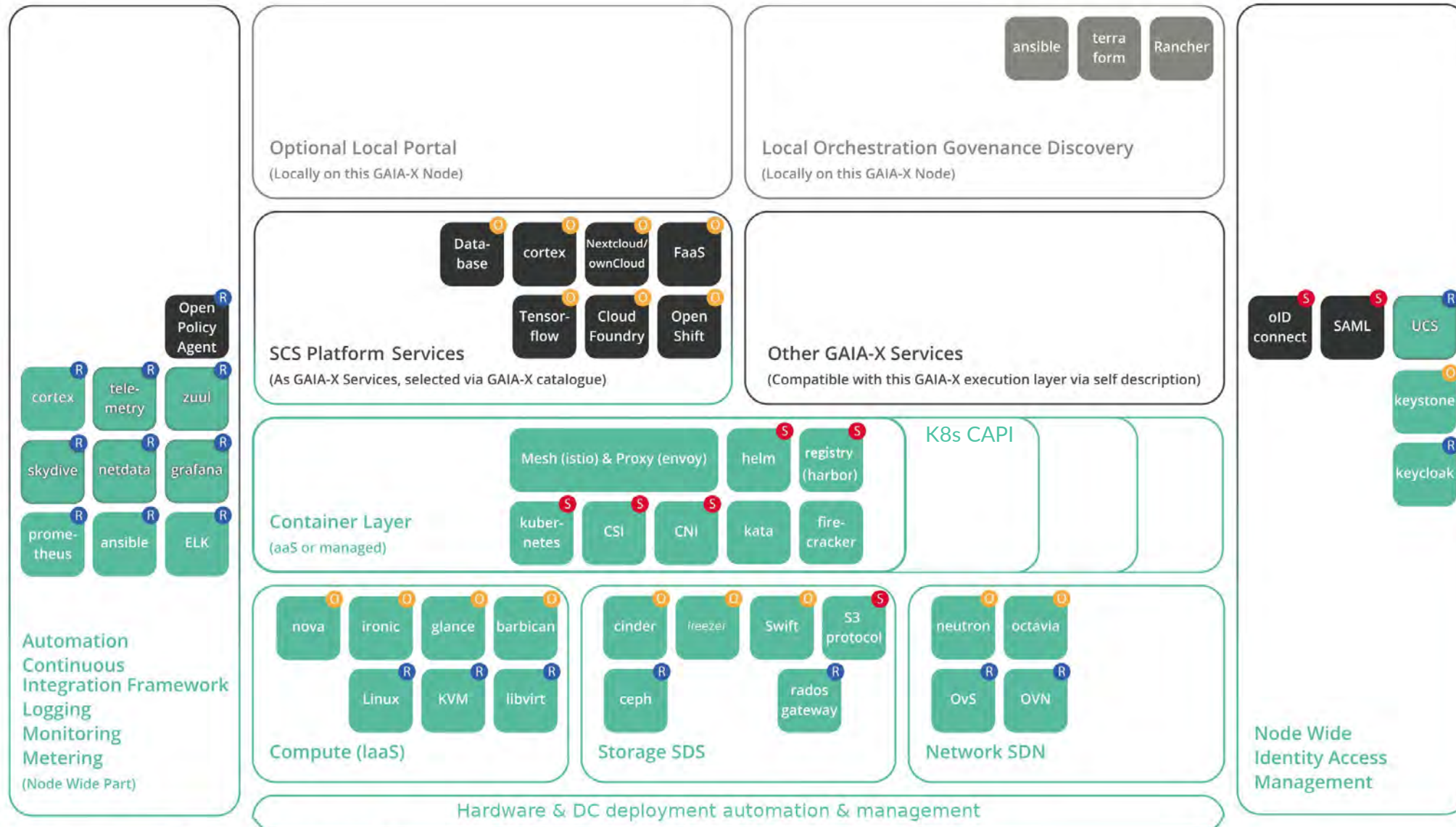
- SCS compatible: Compatibility / Interoperability testing
- SCS open: Technological transparency (fully open functional stack)
- SCS sovereign (later): Operational transparency





Parldigi

# 3 - SCS reference implementation architecture



S SCS Standard    O Optional Standard    R Reference Implementation Detail

LOKI  
=  
Linux  
OpenStack  
Kubernetes  
Infra-  
structure



# 3 - SCS reference implementation status

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

- Participating in & contributing to upstream communities

All SCS work fully OSS ([github.com/SovereignCloudStack](https://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, ...





# SCS reference implementation adoption

Two public clouds in production with complete SCS IaaS/Ops/IAM stacks since > 1 year



PlusCloud achieved BSI C5 certification in Nov '21

## Adoption continues...

- Soon (2022-08-01): Third public cloud (with full SCS)
- PoCs in industry and with public sector IT providers (DE: dataport, DVS = Deutsche Verwaltungscloud Strategie)
- Modules used by various partners (see logos on homepage)
- Ecosystem of service companies emerging (training, consulting, implementation, support, ...)
- Standards adoption via certification program (WIP)
- SCS Gitops Container Management definition also with non-SCS-IaaS providers (WIP)

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

- Gaia-X Self-Descriptions developed and provided (Srv. Char. WG / Bachelor thesis @ C&H)

## Gaia-X Federation Services

- SCS used as Dev and Validation platform for Gaia-X Federation Services, integrated offerings planned

# 4 - Operations: Measure what you want to manage ...



openstack-health-monitor: Black-box monitoring

# 4 - Addressing the Operations challenge: Towards fully Open Operations

## 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)

=> Building Open Operations community





# Join the growing SCS community!

## 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](mailto:project@scs.sovereignit.de)

Matrix: SCS rooms





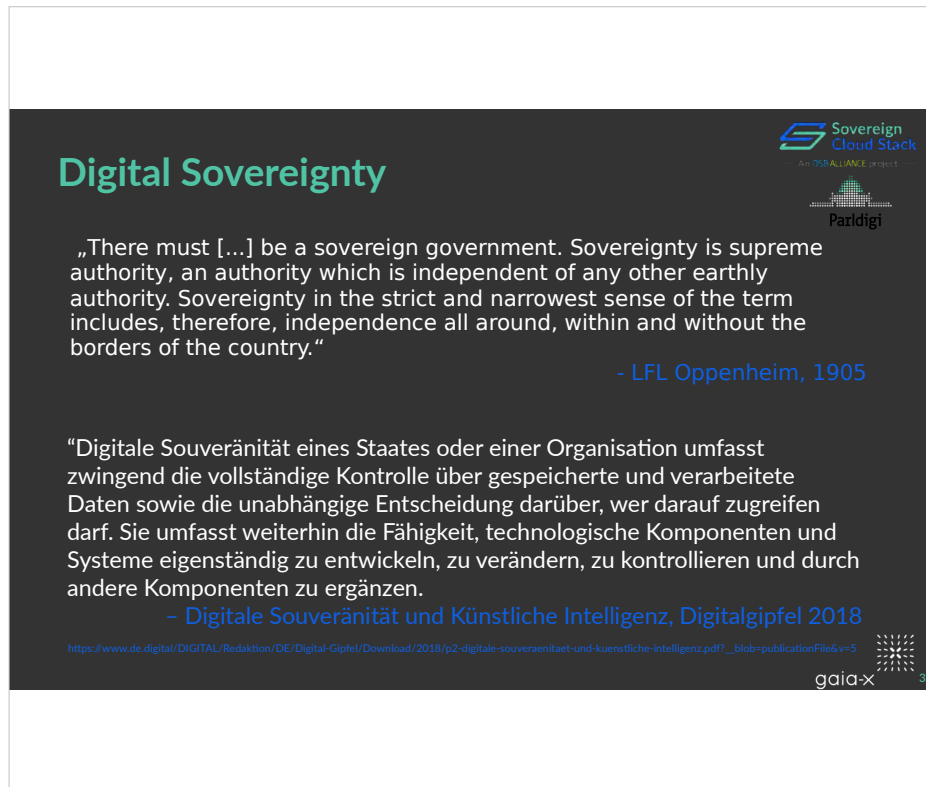


Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.



**Digital Sovereignty**

„There must [...] be a sovereign government. Sovereignty is supreme authority, an authority which is independent of any other earthly authority. Sovereignty in the strict and narrowest sense of the term includes, therefore, independence all around, within and without the borders of the country.“

- LFL Oppenheim, 1905

“Digitale Souveränität eines Staates oder einer Organisation umfasst zwingend die vollständige Kontrolle über gespeicherte und verarbeitete Daten sowie die unabhängige Entscheidung darüber, wer darauf zugreifen darf. Sie umfasst weiterhin die Fähigkeit, technologische Komponenten und Systeme eigenständig zu entwickeln, zu verändern, zu kontrollieren und durch andere Komponenten zu ergänzen.

- Digitale Souveränität und Künstliche Intelligenz, Digitalgipfel 2018

[https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche-intelligenz.pdf?\\_\\_blob=publicationFile&v=5](https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche-intelligenz.pdf?__blob=publicationFile&v=5)

gaia-x 3

“At least half of the usage of public clouds in Germany is in violation of data protection laws!”

– Kurt Garloff, 2016

**Digital Sovereignty - Open Source**

“Digital Technology and Digital Sovereignty [...] and we define it as the capacity to be able to act and to reduce vulnerabilities. So it's twofold. The one is really to reduce your weaknesses, where others can attack you. And the other side is to be able to innovate, to develop by yourself, to set your own standards, to define the values you want to see in technology. [...] [Sovereign Tech Fund is specifically for open source software?] Only!”

<https://www.youtube.com/watch?v=ZIPLGmBfaVc>

### SCS Project deliverables:

- \* Standards for IaaS, KaaS, PaaS, IAM, Monitoring, ... (some together with GAIA-X)
  - also: Standards for Ops (for providers)
- \* Complete, 4 x Open, Modular Software Stack
- \* Ecosystem for providers (internal & public)

### Building and managing a CSP Ecosystem:

- Avoid reinventing the solution to all operational challenges
- Share ops practices, tooling, ...
- OVERCOME THE OPERATABILITY PROBLEM
- Impose transparency (for some cert levels)
- Foster federation

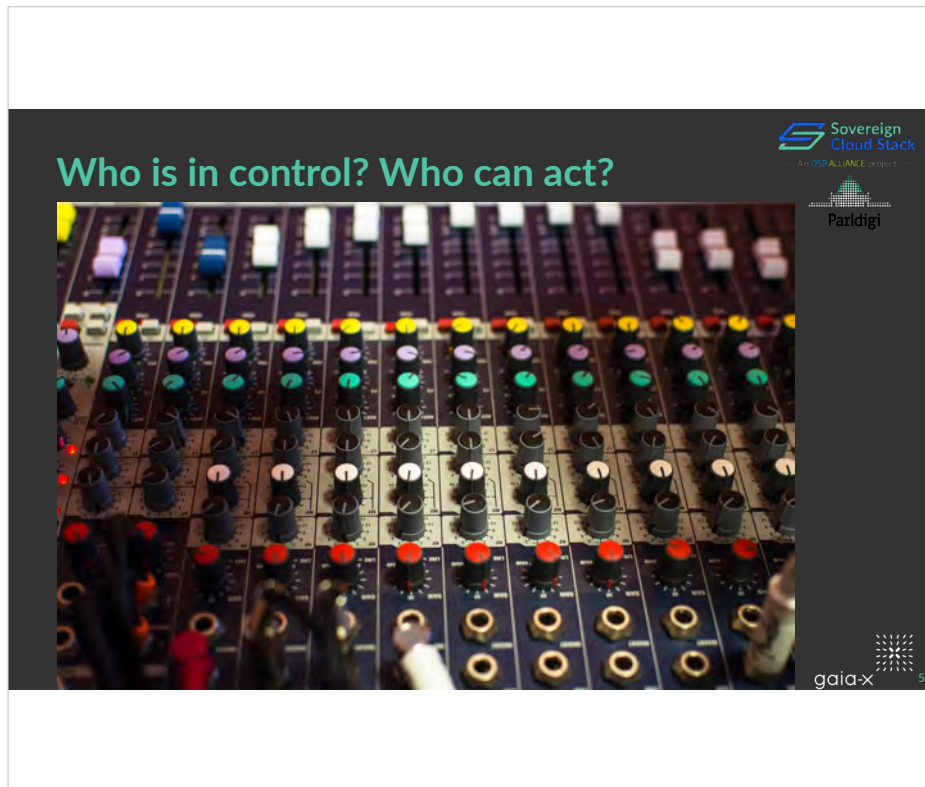
### Ensure compatibility for ISVs and users:

- Healthy app platform

### Compat for partners:

- Operators, consultants, trainers have one target platform

### OVERCOME THE FRAGMENTATION PROBLEM

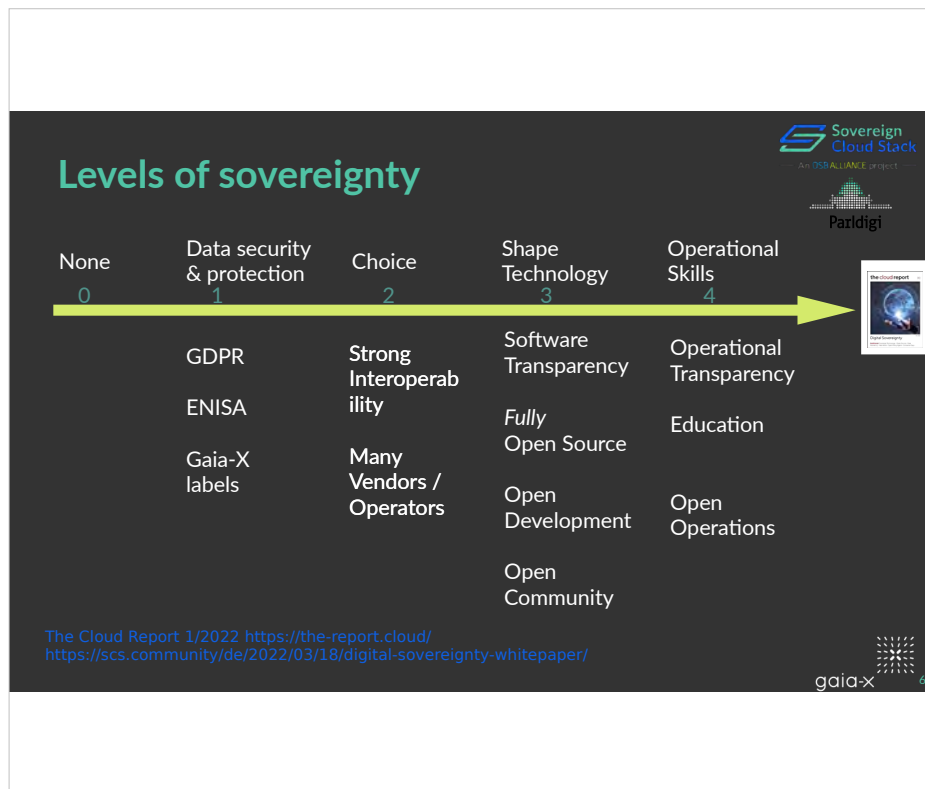


Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.



Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.

**A pig with a lipstick ...**




Image used with friendly permission from Massively Overpowered

**Sovereign Cloud Stack**  
AN OSRA ALLIANCE project

**Paridigi**

- Local data centres of non-EU platforms
- Cloud Act
- Confidential Computing**
  - Data decrypted for processing (exc homomorphic)
  - Availability issue remains
- Local operations (with partner)**
  - Availability issue only partially solved
  - No choice, no ability to shape
- "Open"**
  - Open Standards w/o Open Ref Implementation
  - Open Core / partial Open Source
  - Closed communities
  - No Operational knowledge sharing
- "Transparent"**
  - No public Root Cause Analysis
  - Very filtered public monitoring / status

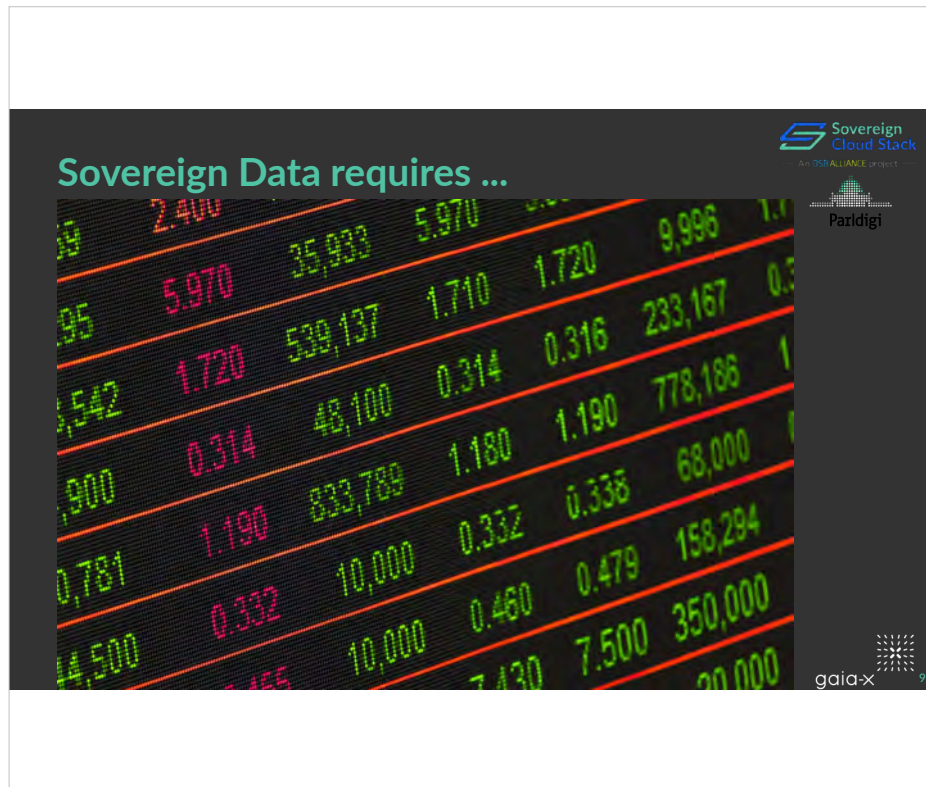
**gaia-x** 8

Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.



Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.



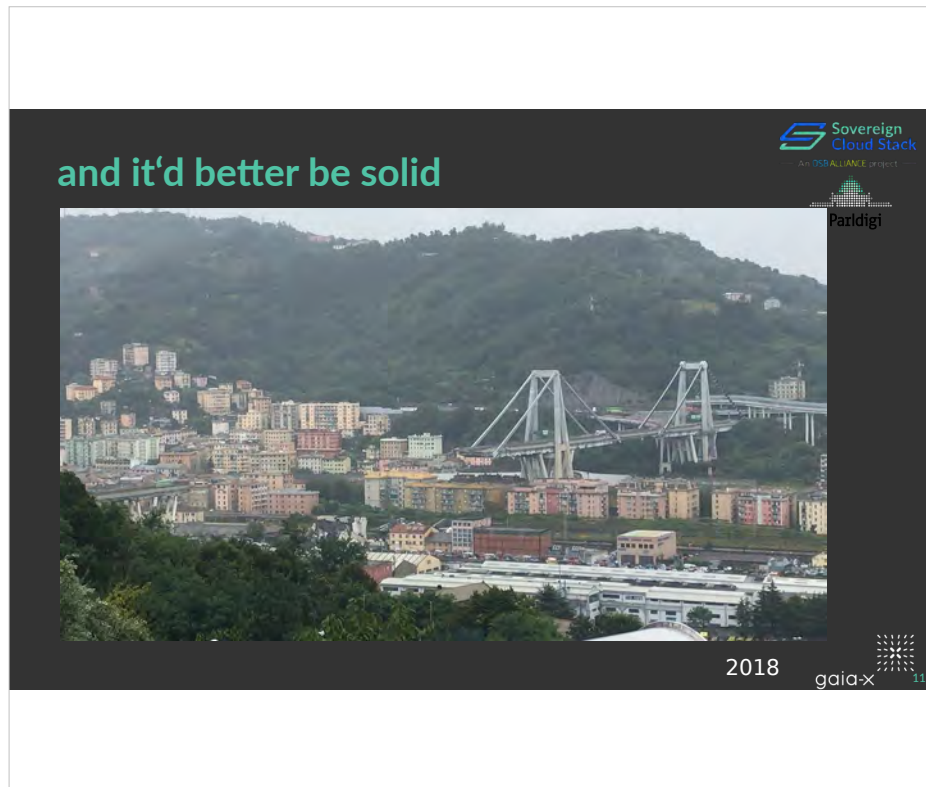
Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.





Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.

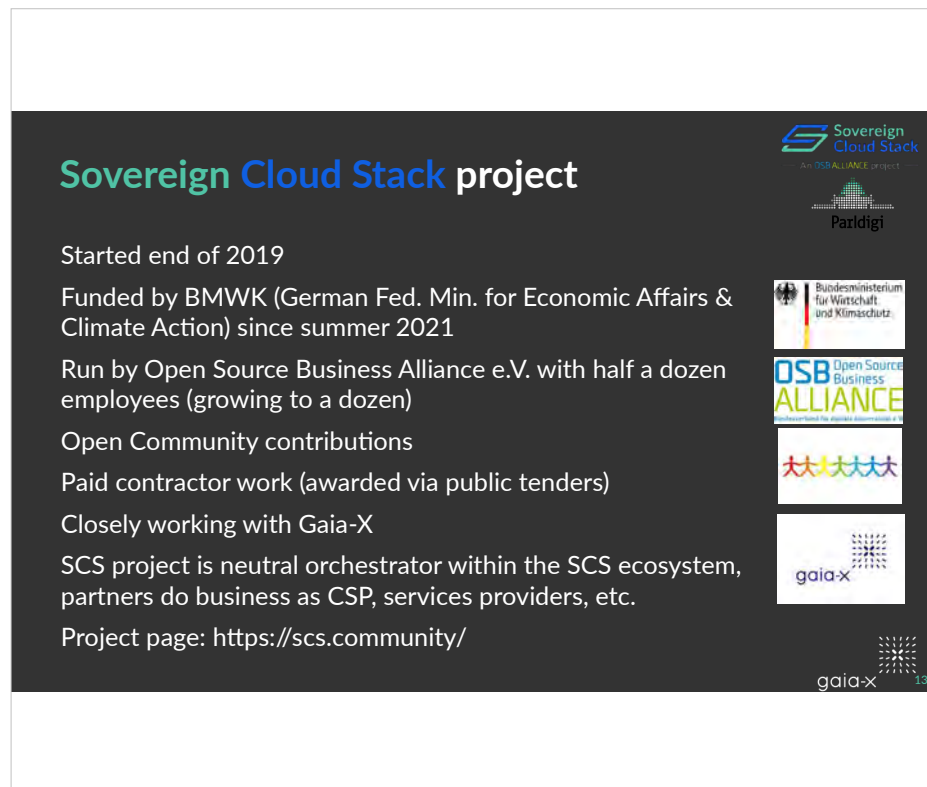


Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.



**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/>

Logos: Sovereign Cloud Stack, OSB ALLIANCE, Bundesministerium für Wirtschaft und Klimaschutz, OSB Open Source Business ALLIANCE, gaia-x, gaia-x 13

## Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

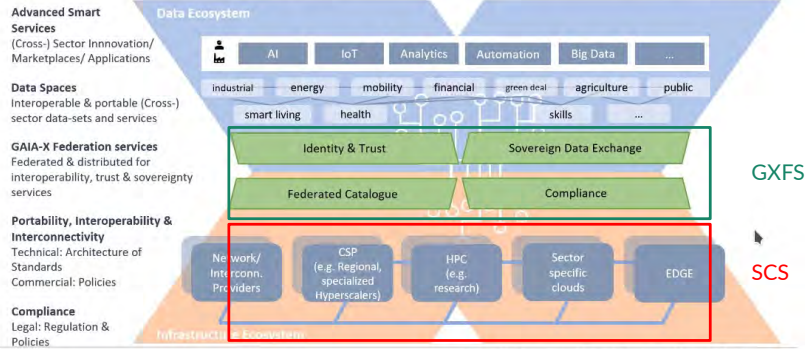
Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.

# Sovereign Cloud Stack and Gaia-X



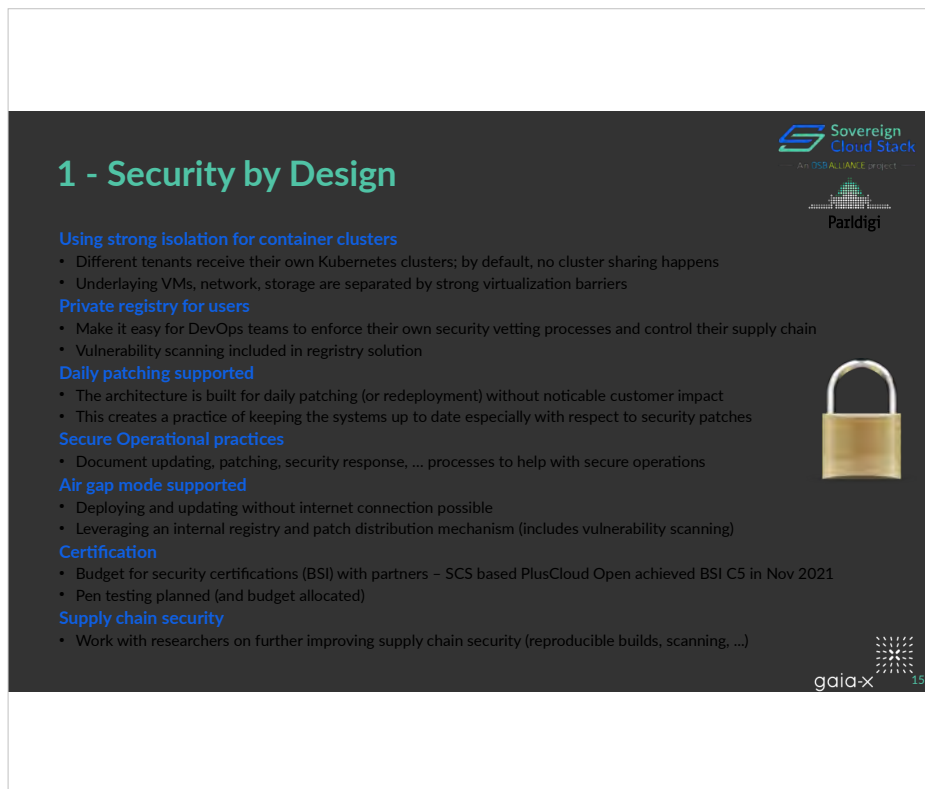
## Gaia-X in One (Big) Figure



6 6/13/2022 Dr. Sebastian Lins – Introducing Gaia-X

Applied Informatics and Formal Description Methods (AIFB)  
Critical Information Infrastructures (cii)—Prof. Dr. Sunyaev





**1 - Security by Design**

**Using strong isolation for container clusters**

- Different tenants receive their own Kubernetes clusters; by default, no cluster sharing happens
- Underlying 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 registry solution

**Daily patching supported**

- The architecture is built for daily patching (or redeployment) without noticeable 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, ...)

Logos: Sovereign Cloud Stack, AN OSRA QUINCE project, Paradigi, gaia-x 15

SCS Project deliverables:

- \* Standards for IaaS, KaaS, PaaS, IAM, Monitoring, ... (some together with GAIA-X)  
also: Standards for Ops (for providers)
- \* Complete, 4 x Open, Modular Software Stack
- \* Ecosystem for providers (internal & public)

Building and managing a CSP Ecosystem:

- Avoid reinventing the solution to all operational challenges
- Share ops practices, tooling, ...
- OVERCOME THE OPERABILITY PROBLEM
- Impose transparency (for some cert levels)
- Foster federation

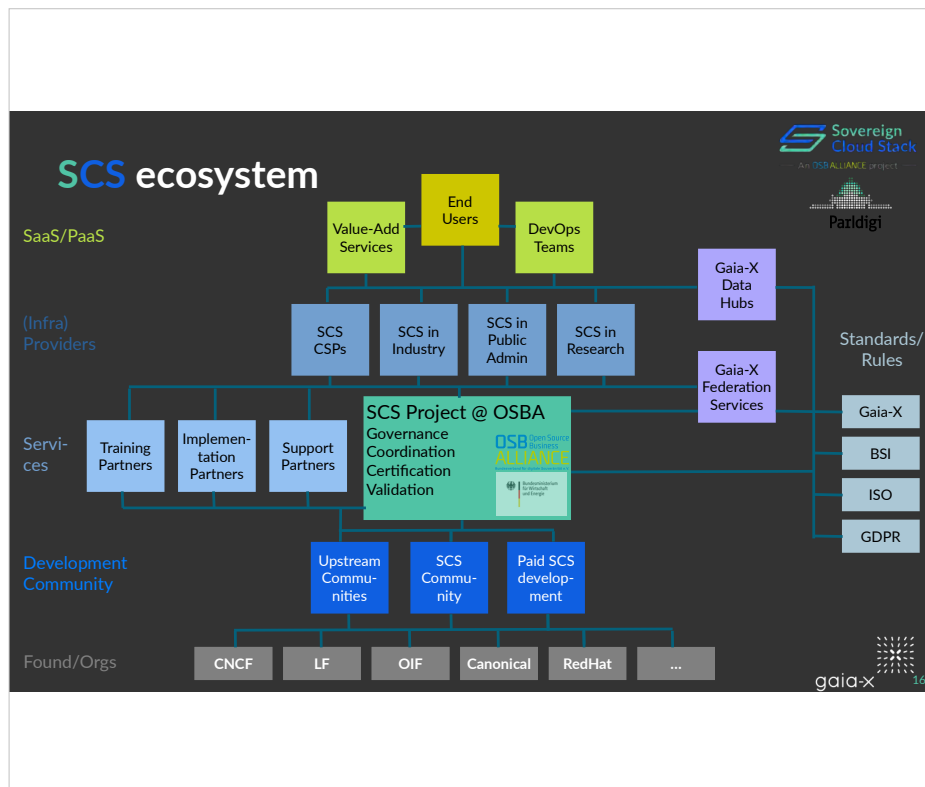
Ensure compatibility for ISVs and users:

- Healthy app platform

Compat for partners:

- Operators, consultants, trainers have one target platform

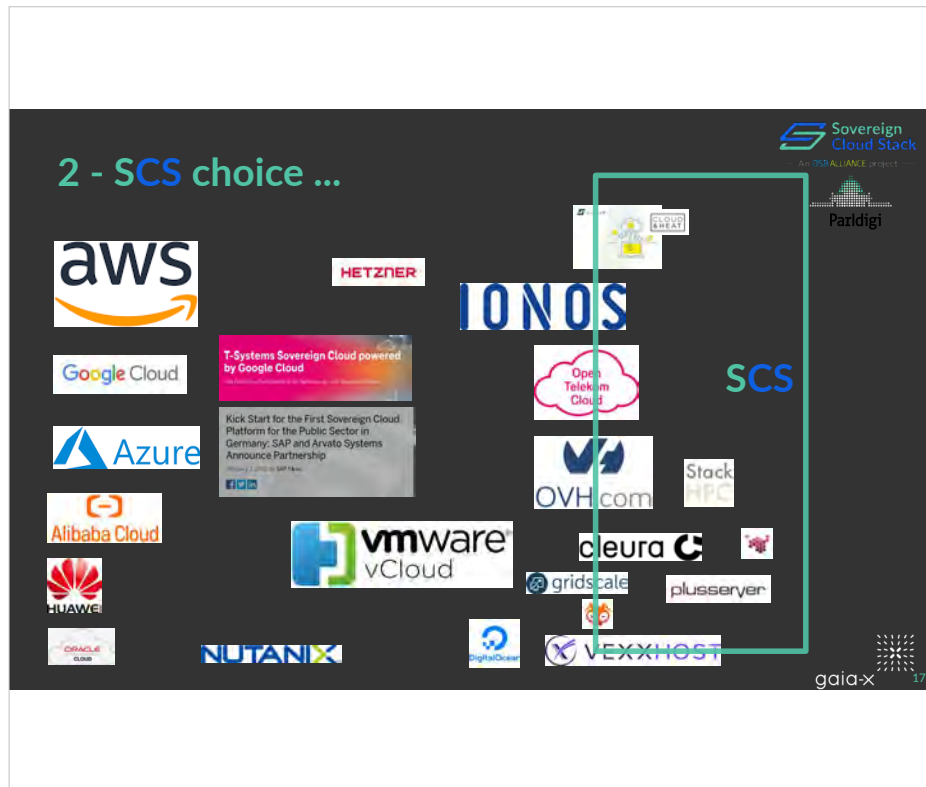
OVERCOME THE FRAGMENTATION PROBLEM



## Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this. This makes the solution sustainable, as the users are not dependent on a single provider.




Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.



## 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)**

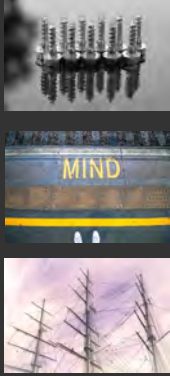

- Done: IaaS flavor naming and standard flavors
- Done: Image metadata
- WIP: Definition of regions, availability zones, ...
- WIP: k8s cluster management (k8s cluster-API)

**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

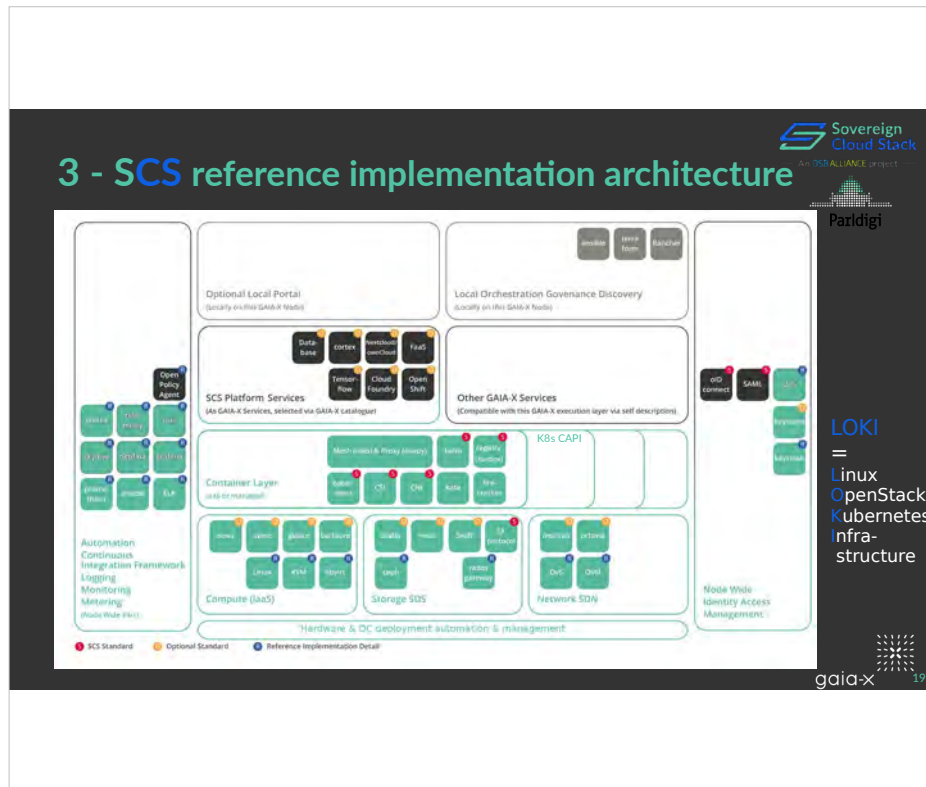
Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.





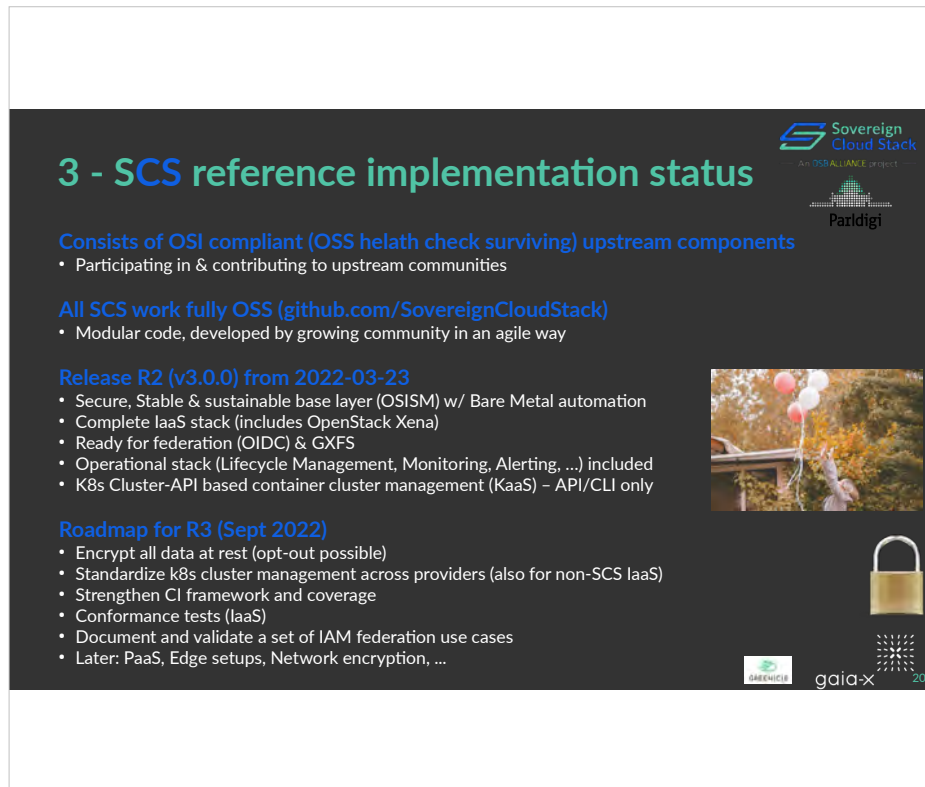
Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:

- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.



**3 - SCS reference implementation status**

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

- Participating in & contributing to upstream communities

All SCS work fully OSS ([github.com/SovereignCloudStack](https://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, ...

Logos: Sovereign Cloud Stack, AN OSS ALLIANCE project, Paradigi, GREENCLOUD, gaia-x 20

Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.

**SCS reference implementation adoption**

Two public clouds in production with complete SCS IaaS/Ops/IAM stacks since > 1 year

**BETA CLOUD**

**PlusCloud** achieved BSI C5 certification in Nov '21

**OPEN**

**Adoption continues...**

- Soon (2022-08-01): Third public cloud (with full SCS)
- PoCs in industry and with public sector IT providers (DE: dataport, DVS = Deutsche Verwaltungscloud Strategie)
- Modules used by various partners (see logos on homepage)
- Ecosystem of service companies emerging (training, consulting, implementation, support, ...)
- Standards adoption via certification program (WIP)
- SCS Gitops Container Management definition also with non-SCS-IaaS providers (WIP)

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

- Gaia-X Self-Descriptions developed and provided (Srv. Char. WG / Bachelor thesis @ C&H)

**Gaia-X Federation Services**

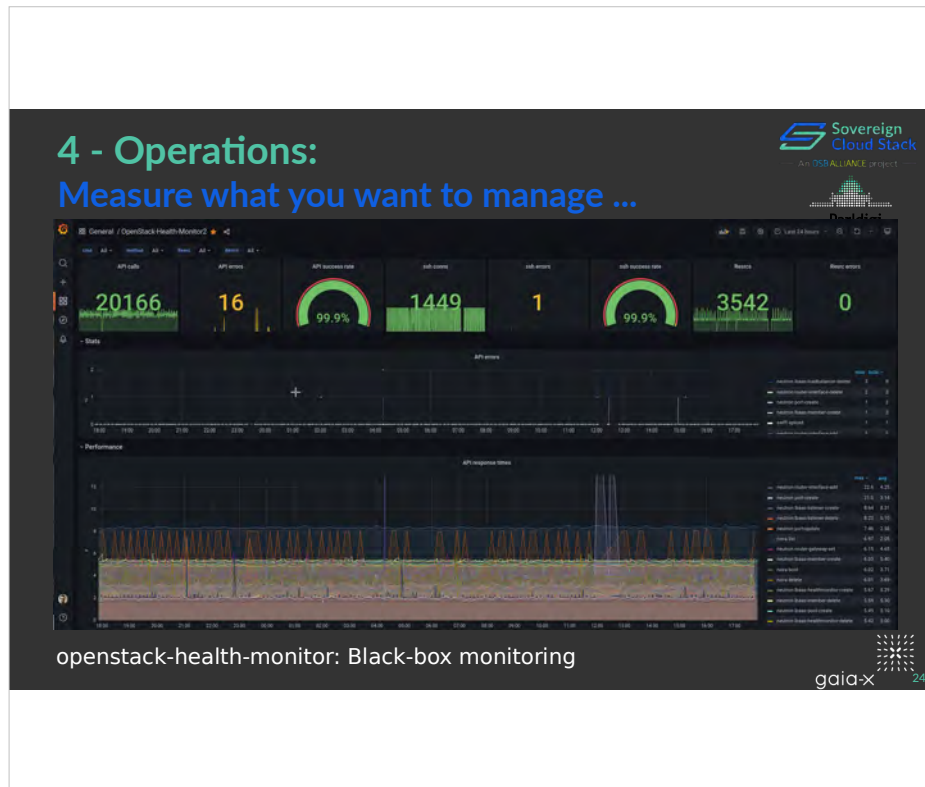
- SCS used as Dev and Validation platform for Gaia-X Federation Services, integrated offerings planned

Logos: Sovereign Cloud Stack, Paradigi, BETA CLOUD, PlusCloud, gaia-x 21

Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this. This makes the solution sustainable, as the users are not dependent on a single provider.





Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back



Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.


This makes the solution sustainable, as the users are not dependent on a single provider.

## 4 - Addressing the Operations challenge: Towards fully Open Operations

 Sovereign  
Cloud Stack  
AN OSS ALLIANCE project  
 Paridigi

- 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)
- => **Building Open Operations community**

 gaia-x <sup>25</sup>

Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.





**Join the growing SCS community!**

**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](mailto:project@scs.sovereignit.de)  
Matrix: SCS rooms

Principles how we build SCS:

- Building a network of providers (and in-house installs) requires common ground to be usable:
- Building on top of existing projects, contributing back

Common standards (helps both users & operators). We require transparency – how we build this (open source, open design, ...) and certify solutions against this.

This makes the solution sustainable, as the users are not dependent on a single provider.