
Sovereign-cloud.nl
Confidential Compute
with
Microsoft Cloud for Sovereignty
Arnold van Wijnbergen & Dinant Paardenkooper
Sovereign Cloud NL
DUTCH MICROSOFT SECURITY MEETUP

Who are we

Sovereign cloud community ---> https://sovereign-cloud.nl

Sovereign Cloud NL

Qensus

Arnold van Wijnbergen

Cloud Expert | Consultant

linkedin.com/in/**ilovit**

azurebuddy.online

github.com/**avwsolutions**

IMPRESSIVE

Dinant Paardenkooper

Cloud Native Architect | Consultant

linkedin.com/in/**dinantpaardenkooper**

Dinantpaardenkooper.nl

github.com/**dpaardenkooper**

Microsoft Most Valuable Professional

What, why and how

What Is a Sovereign Cloud? Why Is It Important? How can you leverage it?

Sovereign Cloud NL

What: Cloud computing architecture that's designed and built to provide data access in compliance with local laws and regulations.

Why: Ensuring localized infrastructure, isolated support teams and tools that ensure data does not leave the country.

How: Provide best practices, references, and other guidance based local regulations to

- **Provide data residence options**
- **Always enforce private connectivity**
- **Ensure granular control/restrictions on data access**
- **Force data in transit, use and rest is encrypted**
- **Apply policies to implement sovereign controls**

Overview of Data & Technology Sovereignty

Digital Sovereignty types explained

Sovereign Cloud NL

	Data	Technology	
Geographical	*Where is data stored and processed?*	*Where is data deployed & made resilient?*	
Operate	*Who can consume the data?*	*Who designs, develops and operations the technology?*	
Regulatory	*What laws & regulations apply?*	*How can a technology be forbidden or used by law?*	

Various Sovereign Cloud Approaches

Various approaches Hyperscalers offer to implement a Sovereign Cloud

Sovereign Cloud NL

AWS European Sovereign Cloud

Key features

- ✓ Launched first region in Germany.
- ✓ In-region billing and usage metering systems.
- ✓ Promising, yet to start.
- ✓ Currently not available in the Netherlands.

Microsoft Cloud for Sovereignty

Key features

- ✓ Available in various regions like North & West Europe.
- ✓ Leverages existing Azure services to build the product.
- ✓ Flexible to extend.
- ✓ Either customer or managed through a service provider.

Sovereign Cloud Powered by Google Cloud

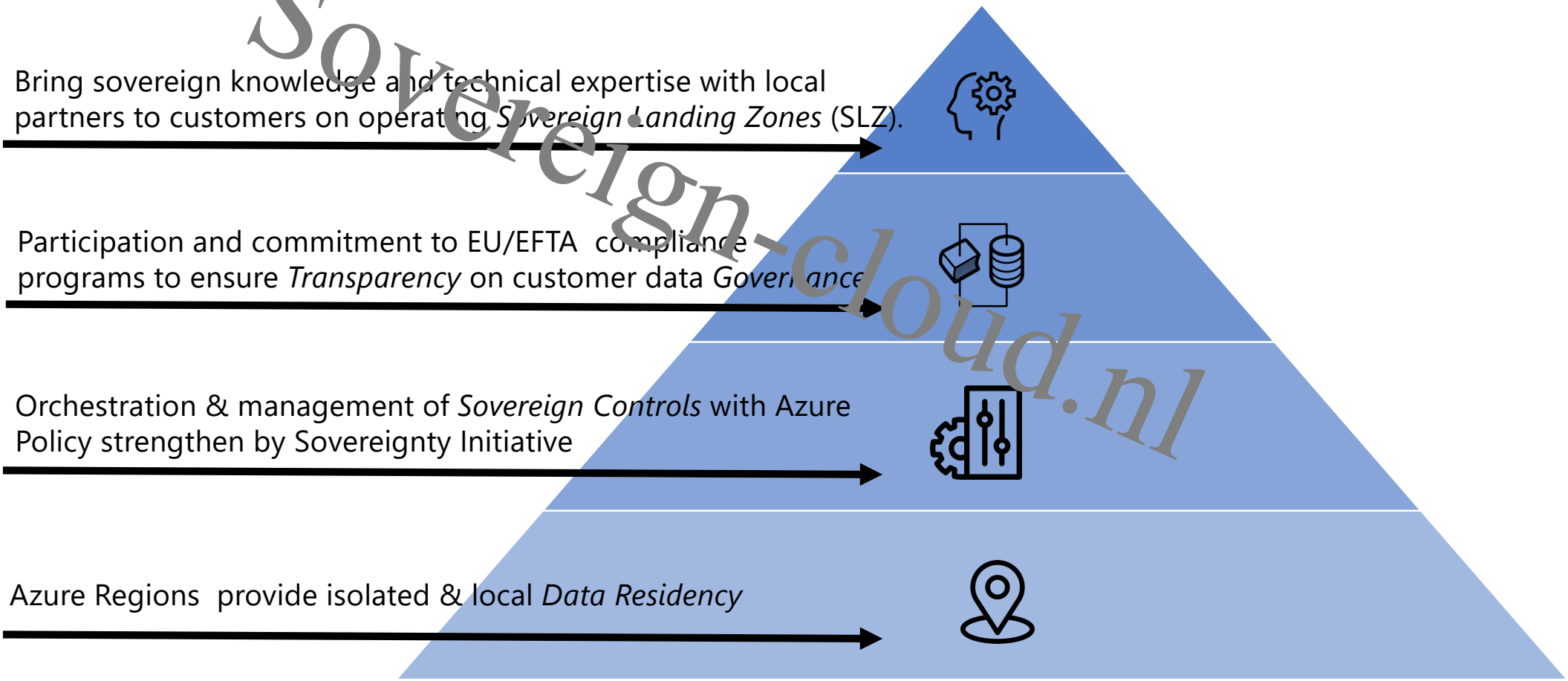
Key features

- ✓ Available only in Germany and France.
- ✓ Limited products available.
- ✓ Less flexible to extend.
- ✓ Exclusively managed by a partner like T-Systems, S3NS.

Microsoft approach didn't reinvent the wheel

Benefits of a customer centric approach by leveraging proven technology

Sovereign Cloud NL



Sovereign Landing Zone

Ingredients that provide digital sovereignty controls

Sovereign Cloud NL

Sovereign Landing Zone

Infrastructure-as-Code (IaC)

Automate infrastructure deployment, configuration, and management using code for efficiency, consistency, scalability and enforce regulatory compliance in Azure using Bicep.

Policy-as-Code (PaC)

Define, enforce, and manage policies through code for consistent governance and compliance of Azure Landing Zones by setting policy-driven guardrails for Azure resources like Management Groups, Subscriptions and VMs.

Workload Templates (Accelerators)

Collection of SLZ compatible templates to learn, validate and properly design workload resources for confidential compute and accelerate the actual deployments by using Bicep.

Sovereign Controls

Strong Encryption
At-Rest, Transit, in-Use

Key Management
Manage cryptographic materials with KV or HSM

CMK
Customer not only brings, but also takes full responsibility

Confidential Computing
Minimize trust, maximize protection during computation

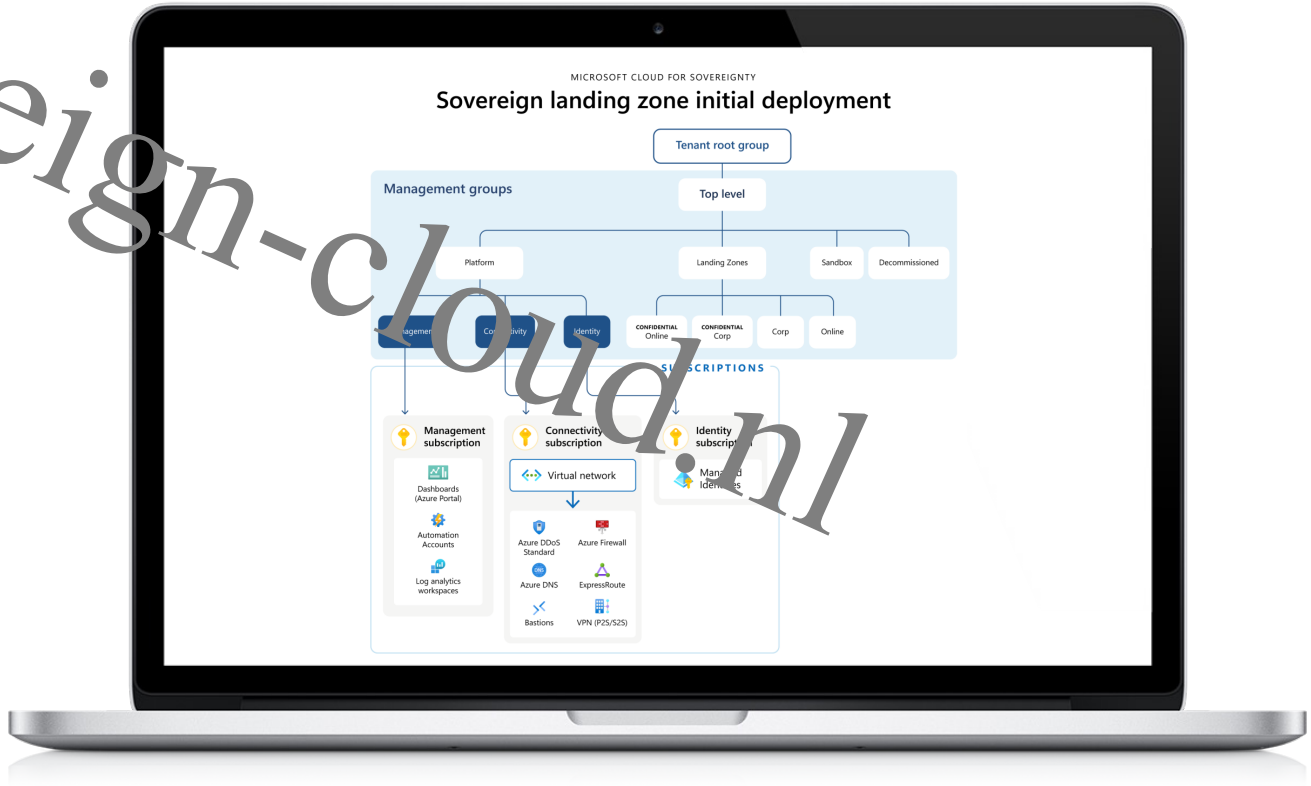
Sovereign Landing Zone

Architecture of the Sovereign Landing Zone (SLZ)

Sovereign Cloud NL

Management group structure with common platform resources to facilitate connectivity, identity and management.

- **Corp**
- **Online**
- **Confidential Corp**
- **Confidential Online**



GitHub repo: https://github.com/Azure/sovereign-landing-zone

Demo Sovereign Landing Zone

Time to dive into a demonstration of a SLZ deployment and structure

Sovereign Cloud NL

Strong Encryption evolvement

How to Secure the 3 States of Data: At Rest, In Transit, In Use

Sovereign Cloud NL

Common States to when Securing Data

At-Rest Encryption

Encrypt data when it's stored in a database, operating system, object store or on Azure disk storage.

In-Transit/Motion Encryption

Encrypt data when it's stored in a database, operating system, object store or on Azure disk storage.

Additional state for Confidential Computing

In-Use/Computation Encryption

Encrypt data when it's in memory and during processing.

Confidential Computing around the corner

Common scenarios when high level of confidentiality and trust is needed

Sovereign Cloud NL

Trusted local entity solutions

Ensuring to protect cloud computing solutions provided by government, healthcare or finance

Enhanced customer data privacy

Maximizing protection for customer data and their privacy matters.

Legal requirements

Ensuring compliance with local regulations and protection of national interests.

Secure blockchain

Focusing on data confidentiality and secure computations to safeguard data access.

Secure multi-party computation

Sharing confidential data sets like medical records by spreading as combined transactions.

Confidential Compute

Enclaves, Attestation, evidence and all about online trust

Sovereign Cloud NL

Confidential Computing

Confidential Computing is the protection of data in use by performing computation in a hardware-based, attested Trusted Execution Environment like an Enclave.

Enclave or Trusted Execution Environment (TEE) differences

Most of the time interchangeable terms. It provides a dedicated subsystem that is isolated and encrypted region for code and data. Decryption takes place inside the processor, so it is even safe from the RAM being read directly.

Attestation

Literally it's the evidence by which something is attested. Important part that helps to establish trust between systems. Using an API parties can verify or claim the authentication of the component or configuration.

CONFIDENTIAL COMPUTING CONSORTIUM

CCF Confidential Consortium Framework

Companies like Microsoft that brings together hardware vendors, cloud providers, and software developers to accelerate the adoption of Trusted Execution Environment (TEE) technologies and standards.

Security enclaves to ensure trusted execution

Hardware and software isolation technologies for cryptographic protection

Sovereign Cloud NL

Intel Software Guard Extensions (SGX)	Intel Trust Domain Extensions (TDX)	AMD Secure Encrypted Virtualization (SEV)	ARM TrustZone for Cortex-A (CCA)
Pioneer in Confidential Computing hardware-based enclaves. Matured over the years, but has prerequisites on the application programming model, since it requires code adjustments using an additional SDK or abstraction like Gramine.	Newest virtualization-based enclave from Intel. Improved isolation and performance comparing With SGX. Biggest benefit is no coupling with programming model, which makes it easy to implement.	AMD answer to Intel, which is a virtualization-based Enclave. First enclave with no dependency on the actual application or requiring any SDK. Ensures protection from the hypervisor layer, which is some cases is not sufficient.	Other vendors also provide confidential compute architectures. Like ARM hardware-based enclave. Technology is widely adopted in the embedded system space like for IoT. Important SDK is OP-TEE.
Application protection	Hypervisor protection	Hypervisor protection	Application protection
DCsv[2,3]-series	[D,E]Cesv5-series	[D,E]Ca(d)sv5-series	n/a

Security enclaves, not only for CPUs

Protect data, AI-models that are processed and guardrail for responsible AI

Sovereign Cloud NL

Protect AI Intellectual Property

Ensures the integrity of intellectual property data that is fed into AI models gets protected from being tampered or even stolen. Important when applying ML/AI in healthcare industry or processing personally identifiable information (pii).

Security for AI Training and Inference

Ensures that data like personally identifiable information cannot leak during interaction with system resources like the CPU. This way only through a secure driver can interfere with the information, which excludes OS and hypervisor.

Secure Multi-Party Collaboration

Important to establish online trust when multiple parties have responsibility and process data records. This way we ensure the confidentiality and integrity of connected data sources.

Confidential AI

Hardware based

Isolation is hardware based and available for H[1,2]00 GPU series.

Sensitive data

Protects against hypervisor and OS layer unauthorized access.

Attestation ready

Using the concept of Attested and integrates Attestation validation.

Strong partnership

Confidential AI is available on Azure, which bundles with AMD-SEV VM.

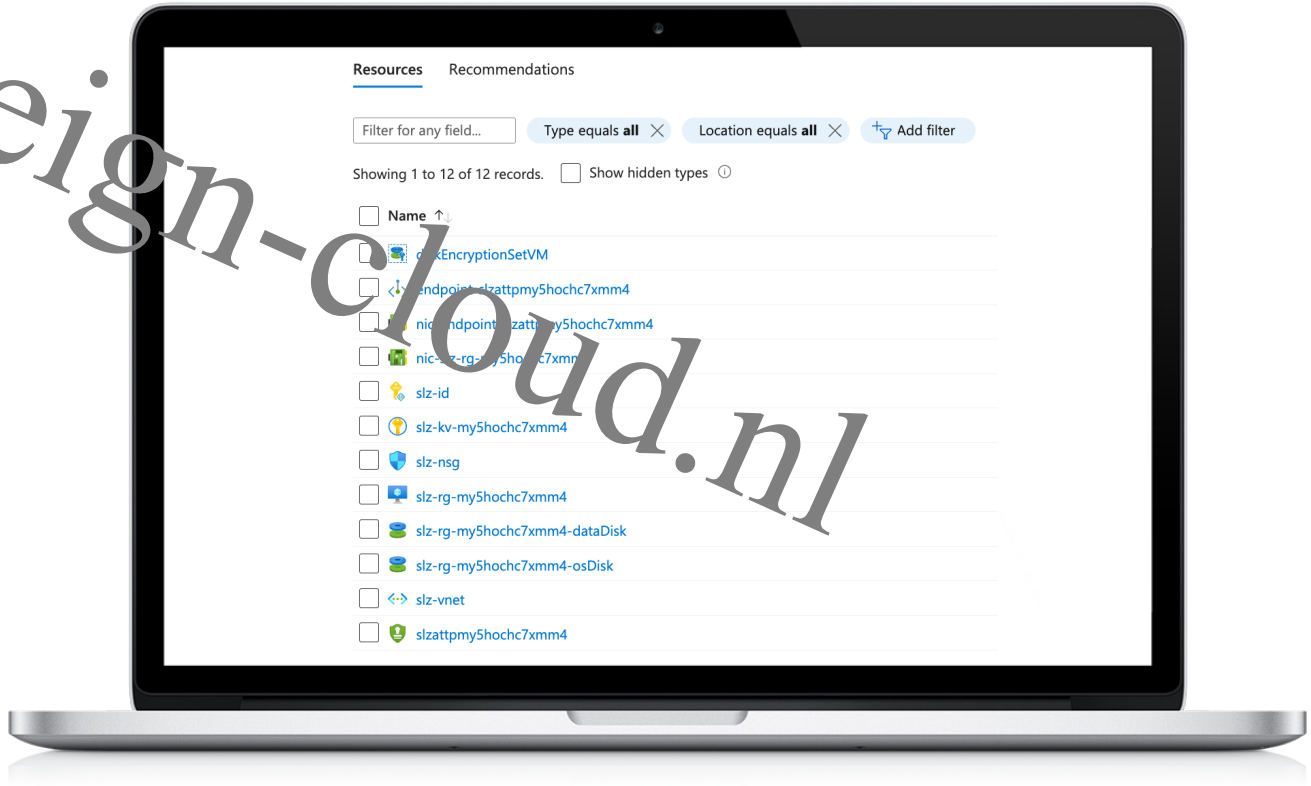
Azure Confidential Virtual Machine

Involved resources to setup an Azure Confidential workload

Sovereign Cloud NL

Workload accelerator based on the AMD-SEV template, deploying compliant resources in the SLZ landing zone.

- **Standard_DC2as_v5**
- **Ubuntu 22.04**
- **Confidential SLZ**
- **Guardrails applied**



GitHub repo: https://github.com/Azure/cloud-for-sovereignty-quickstarts

Demo Azure Confidential ACI with apps

Time to dive into a demonstration of a Confidential ACI deployment

Sovereign Cloud NL

Azure Confidential available services

Portfolio of Confidential products is rapidly growing

Sovereign Cloud NL

- ✓ Confidential VMs (AMD-SEV)
- ✓ VMs with App enclaves (SGX)
- ✓ Confidential AI VMs (GPU)
- ✓ Confidential Containers (ACI)
- ✓ Confidential Node pools (AKS)
- ✓ Confidential Databricks
- ✓ Confidential Data explorer (Public preview)
- ✓ Azure Virtual Desktop (AVD)
- ✓ SQL Always encrypt
- ✓ SQL on Confidential VMs
- ✓ Azure Confidential ledger (ACL)

Interesting Confidential Computing projects

Overview of interesting projects which are supported by the Confidential Computing Consortium

Sovereign Cloud NL

Gramine

Project originated from research which helps to easily port applications to SGX compatible and secure workloads

Occlum

Originated from Huawei to simplify running workloads a simple build OS libraries in Secure enclaves. Now everybody can run app enclave workloads.

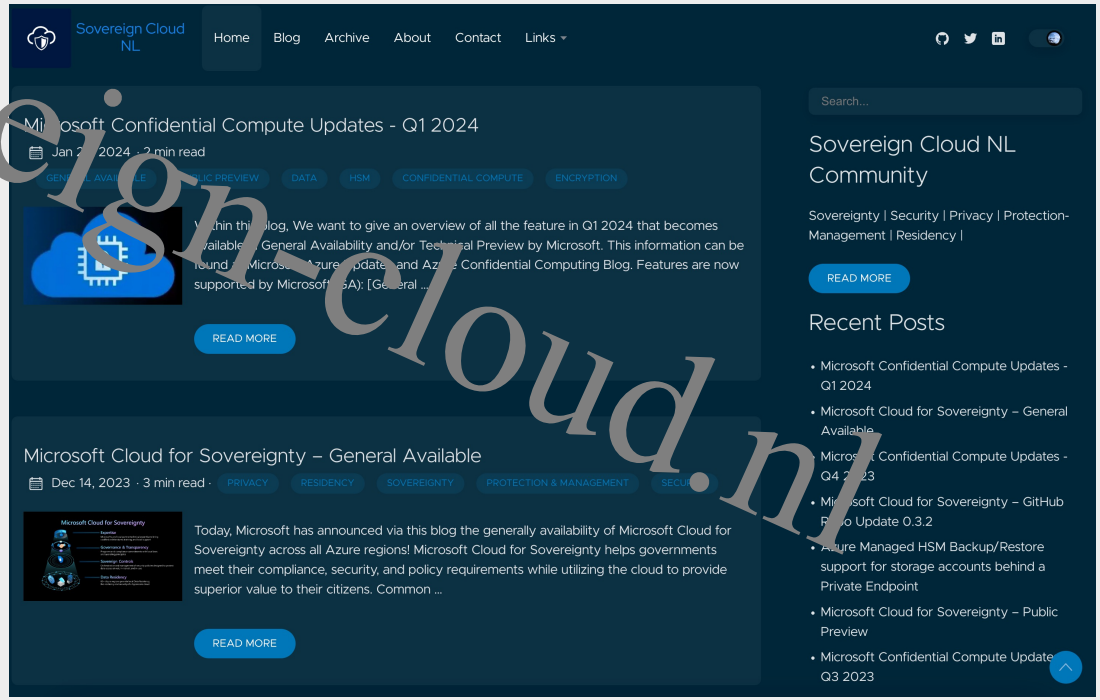
Open Enclave SDK

SDK to build your own enclave applications in C and C++ with the goal to abstract towards a single layer developer experience and create a standard, universal and pluggable eco-system.

VirTEE

OSS development community that builds tools to manage TEEs and deliver Attestation services that are used in embedded systems like IoT.

Follow us for more Sovereign Cloud updates



www.sovereign-cloud.nl