



# Cloud Security in National ID systems

Darren Lentz — Senior Manager & Digital Trust Lead

KPMG South Africa



# Digital sovereignty:

The state's ability to control

the protection of access to critical data

continuity in its critical digital systems

all times and under all conditions

# Cloud and data sovereignty caught in a paradox

We asked the hyperscalers how they would respond to US court-ordered eavesdropping on foreign citizen data – and got responses that highlight a paradoxical situation

 Help Net Security

## AWS European Sovereign Cloud puts data, operations, and oversight inside the EU

AWS European Sovereign Cloud brings EU-operated cloud infrastructure with defined sovereignty, compliance, and oversight measures.

15 Jan 2026




 Computer Weekly

<https://www.computerweekly.com> › feature › Is-cloud-... ⋮

## Is cloud data sovereignty all just a case of 'Trust me, bro'?

3 days ago — Also, the Cloud Act is considered to be “**encryption neutral**”, so companies can be compelled to hand over what they have, but it does **not** ... [Read more](#)


 Quantum Zeitgeist

## Gartner Predicts 75% Will Need Sovereign Strategies

Securing data ownership is key. IBM's Sovereign Core provides AI-ready software for true digital sovereignty, meeting Gartner's 75%...

21 Jan 2026



 The Register

## Microsoft levels up Azure Local to make it fit for large-scale sovereign clouds

Microsoft has given its Azure Local on-prem cloud a major makeover to make it fit for duty powering large-scale sovereign infrastructure.

1 week ago




 SecurityBrief Australia

## Nations race to sovereign encryption in quantum age

As quantum computing looms, nations race to build sovereign cyber and post-quantum encryption to safeguard critical digital infrastructure.

04 Feb 2026



 PRN Newswire

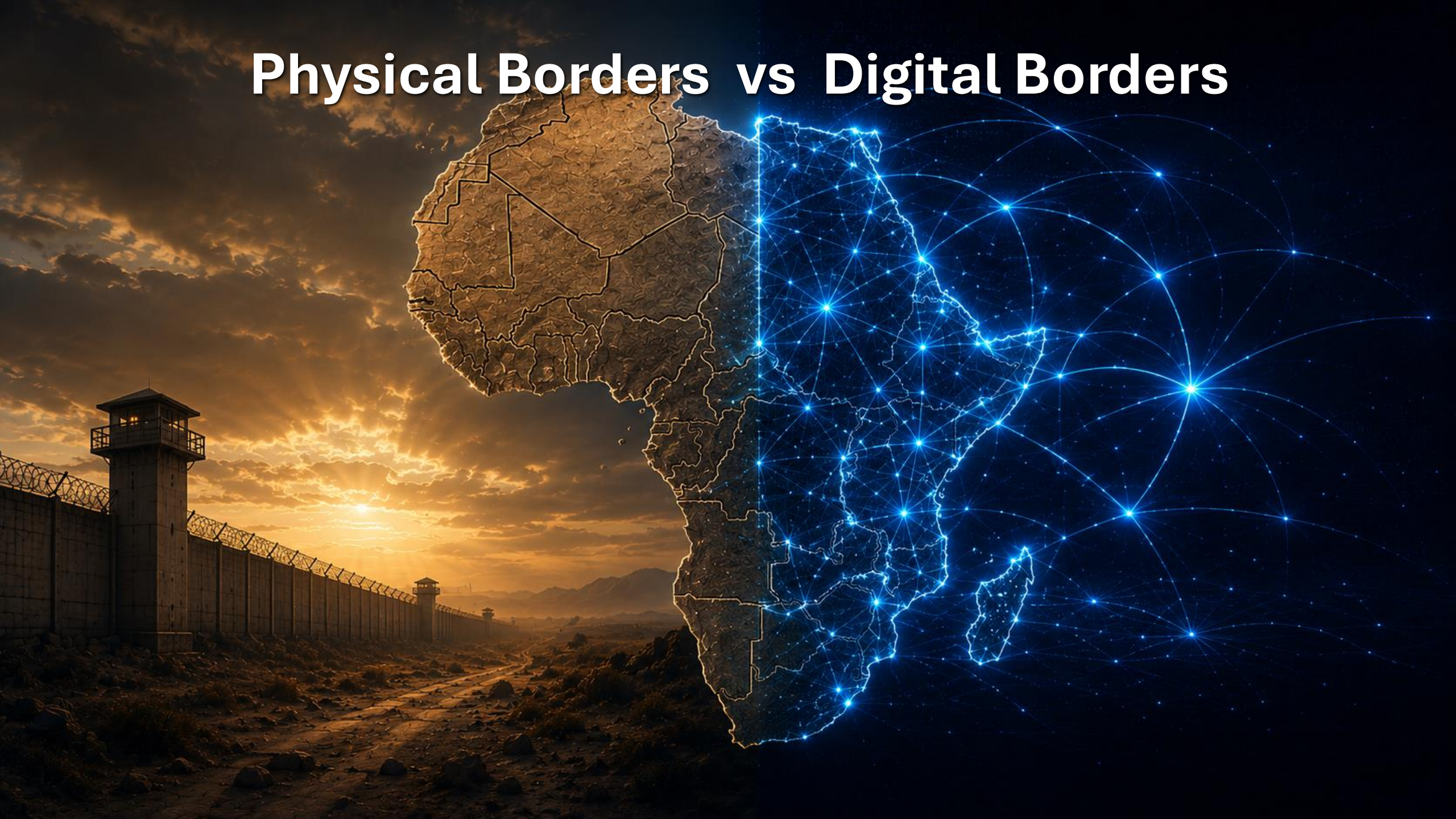
## Digital Sovereignty Push Exposes Gaps in Government Control of Cloud and AI Infrastructure, Says Info-Tech Research Group

Governments around the world are accelerating digital sovereignty mandates in response to geopolitical instability, expanding AI regulation,...

04 Mar 2026



# Physical Borders vs Digital Borders



# Sovereign Cloud ≠ Cloud Sovereignty

## Sovereign Cloud

Focus on physical location & jurisdiction

Ensures regulatory compliance

Concerned with keeping data local

Typically regionally hosted solutions only

## Cloud Sovereignty

Focus on control

Ensures strategic autonomy

Concerned with data access, even abroad

Applies to public, private, hybrid, multi-cloud

# 4 pillars that support Digital Sovereignty

## Sovereignty at Rest

Encryption at Rest

Zero-Trust of data-stores

## Sovereignty in Use

Encryption in Use

Zero-Trust of data-processors

## Sovereignty in Transit

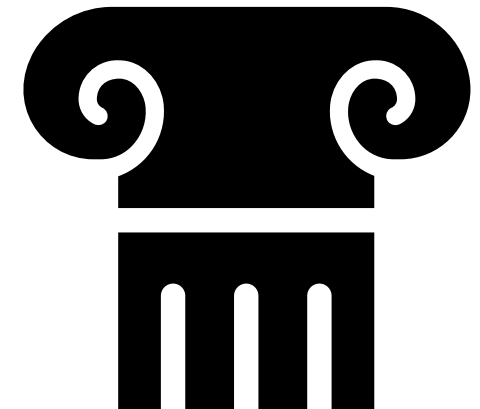
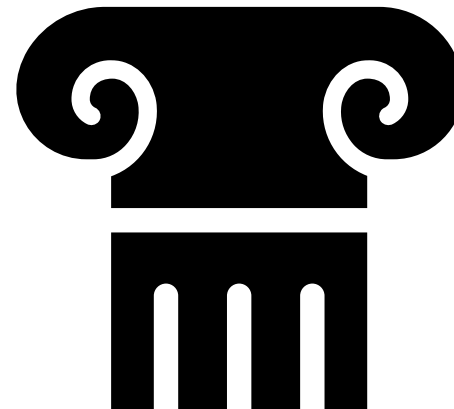
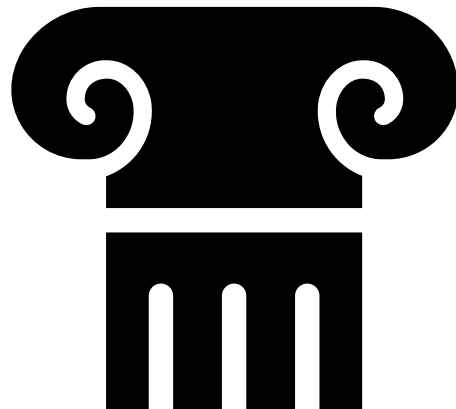
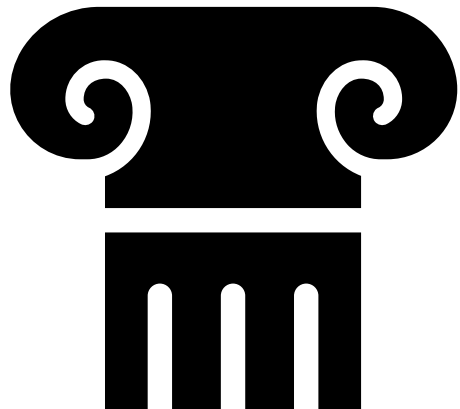
Encryption in Transit

Zero-Trust of microservices

## Sovereignty of Logic

Own the Platform

Zero-Trust of Vendors



# 4 pillars that support Digital Sovereignty

## Sovereignty at Rest

Encryption at Rest

Zero-Trust of data-stores

## Sovereignty in Use

Encryption in Use

Zero-Trust of data-processors

## Sovereignty in Transit

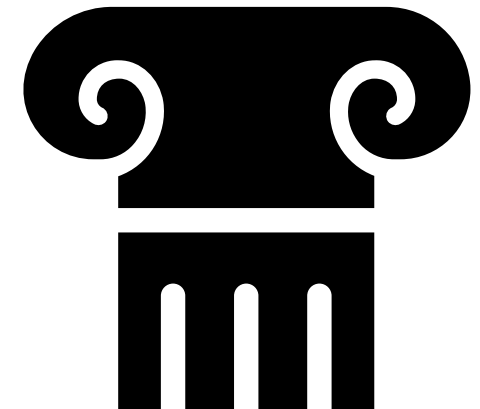
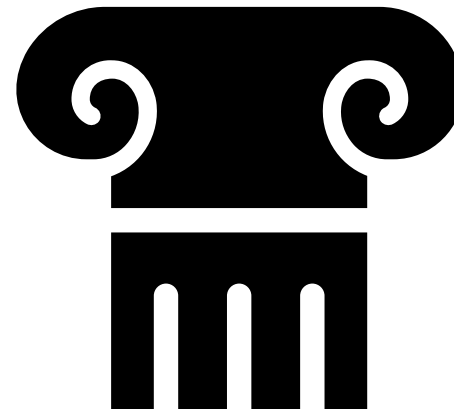
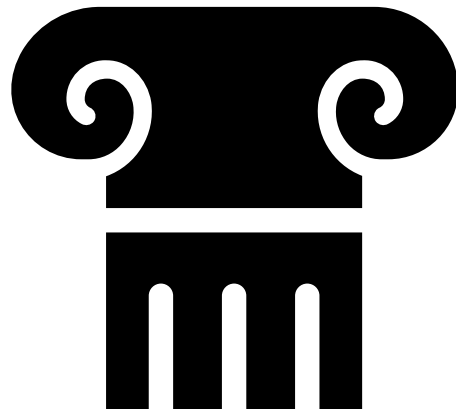
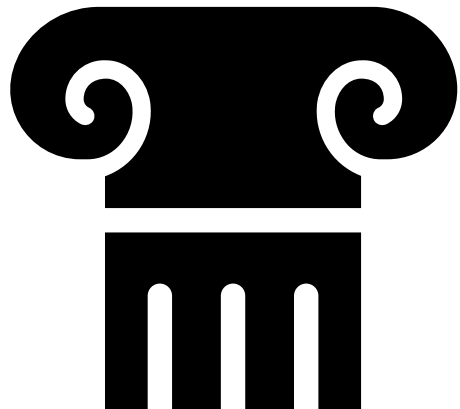
Encryption in Transit

Zero-Trust of microservices

## Sovereignty of Logic

Own the Platform

Zero-Trust of Vendors



The key to a good nights rest...

**GYOK**

**BYOK**

**HYOK**

## The key to a good nights rest...

**GYOK**

**Get Your Own Key**










**BYOK**

**Bring Your Own Key**

**HYOK**

**Host Your Own Key**

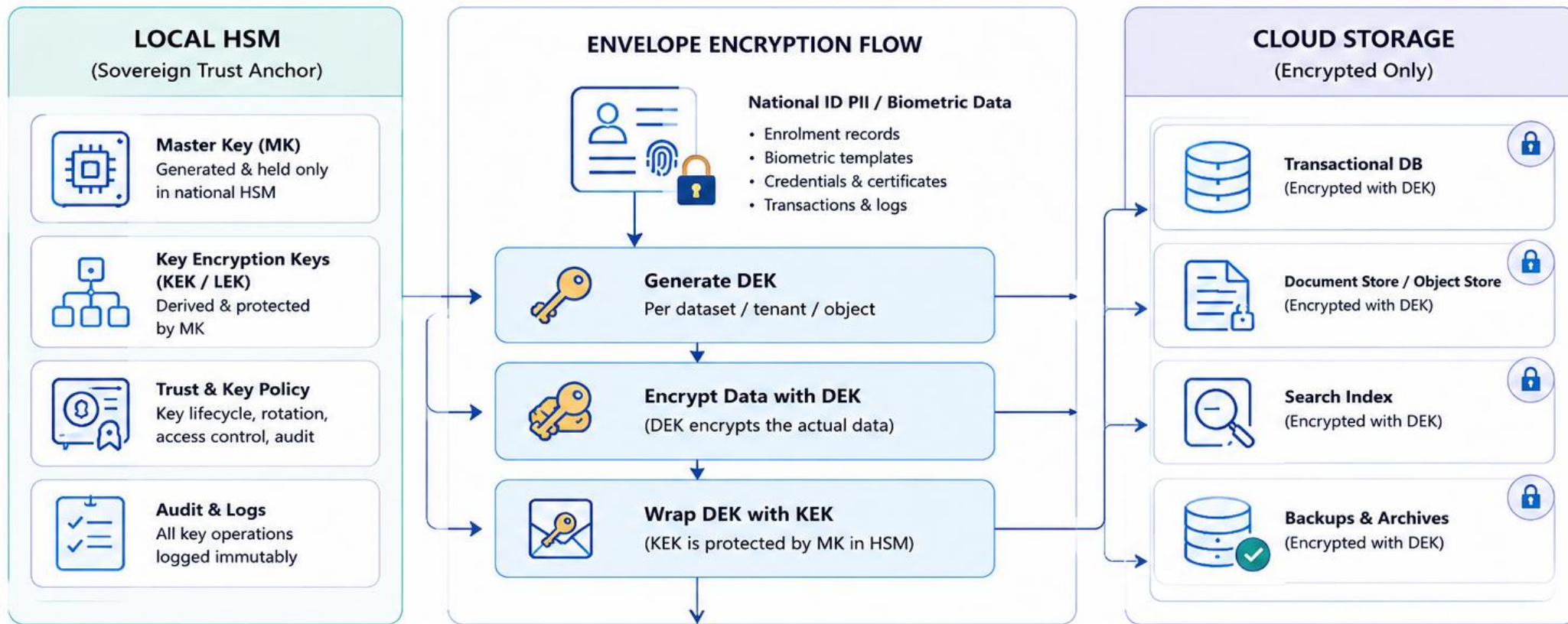
## The key to a good nights rest...

<b>GYOK</b>	<b>BYOK</b>	<b>HYOK</b>
<b>Get Your Own Key</b>	<b>Bring Your Own Key</b>	<b>Host Your Own Key</b>
Let Cloud provider (or vendor) do key generation & management for you	You generate & manage keys in your HSM, and give a copy to Cloud provider (or vendor) to use as and when they need	You generate & manage keys in your HSM, and only give “one-time use” keys to Cloud provider (or vendor)
Provider-owned keys Provider-managed keys Provider unrestricted access to keys	Customer-owned keys Customer-managed keys Provider unrestricted access to keys	Customer-owned keys Customer-managed keys Provider limited access to keys
<ul style="list-style-type: none"> <li> Full trust in vendor</li> <li> Vendor lock-in</li> <li> Virtually no sovereignty over data</li> </ul>	<ul style="list-style-type: none"> <li> Shared trust in vendor</li> <li> Mitigated vendor lock-in</li> <li> Limited sovereignty over data</li> </ul>	<ul style="list-style-type: none"> <li> Zero trust in vendor</li> <li> Vendor agnostic and PQC ready</li> <li> Complete sovereignty over data</li> </ul>

**...is in a great Host!**

# Sovereignty at Rest

## National ID System – Envelope Encryption with Local HSM



### Key Models (Simplified)



#### GYOK

##### Get your own key

Cloud provider generates and manages keys (no sovereignty)



#### BYOK

##### Bring Your Own Key

Country imports key into cloud KMS (shared control)



#### HYOK

##### Hold Your Own Key

Master Key never leaves local HSM (full sovereignty)

### Outcome

- ✓ Cloud stores only encrypted data
- ✓ Master Key never leaves the country
- ✓ Country can decrypt at any time
- ✓ **Full sovereignty at rest**

# 4 pillars that support Digital Sovereignty

## Sovereignty at Rest

Encryption at Rest

Zero-Trust of data-stores

## Sovereignty in Use

Encryption in Use

Zero-Trust of data-processors

## Sovereignty in Transit

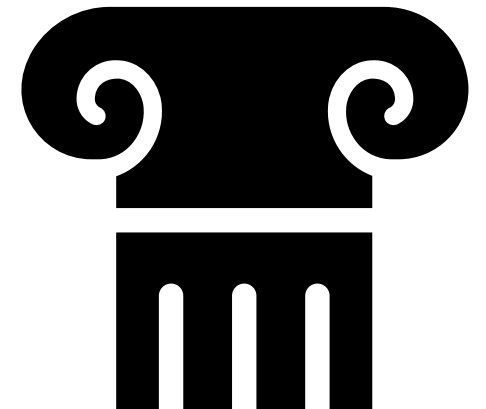
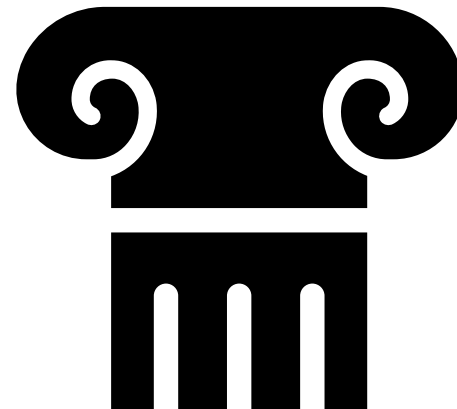
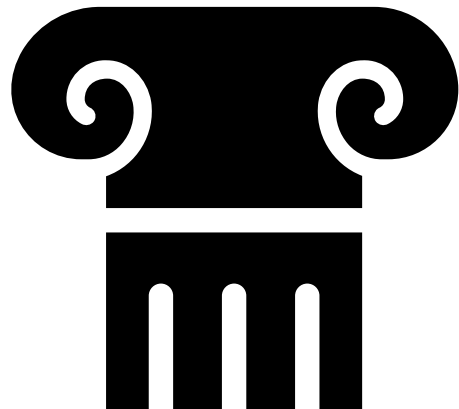
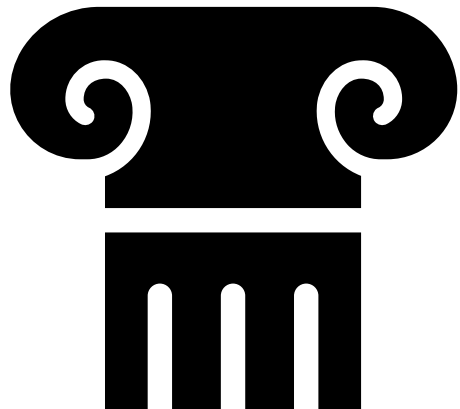
Encryption in Transit

Zero-Trust of microservices

## Sovereignty of Logic

Own the Platform

Zero-Trust of Vendors



# Confidential Computing

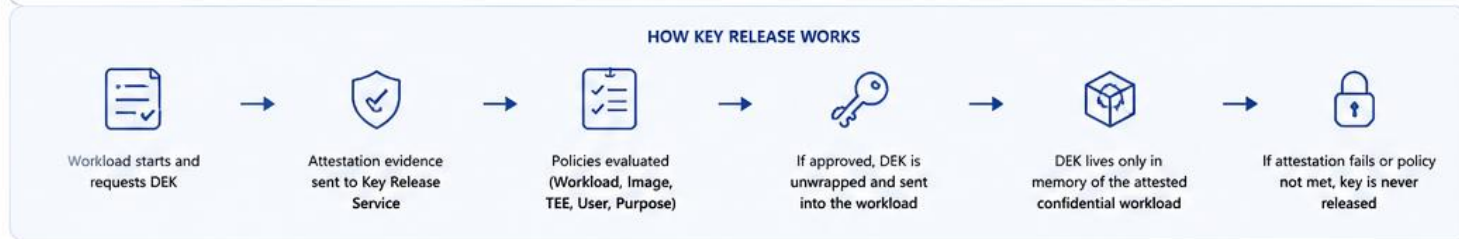
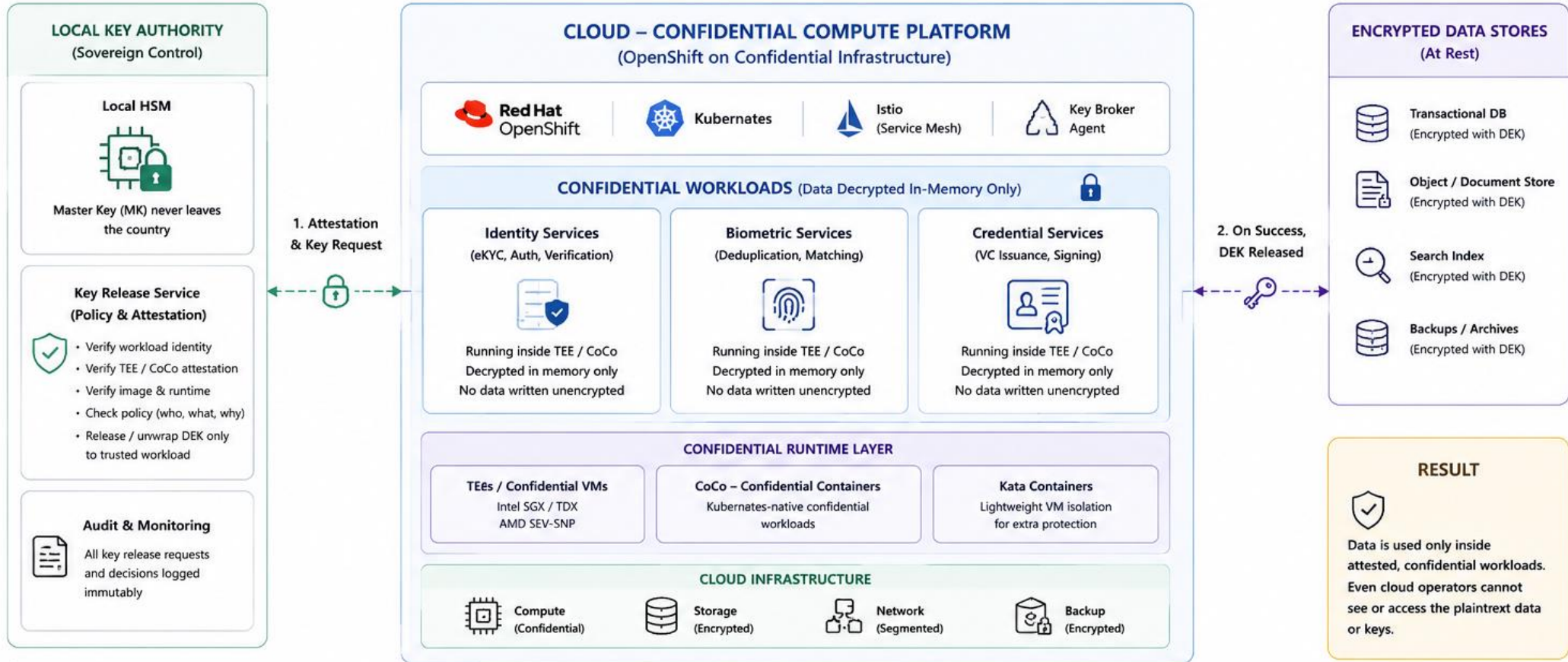
<b>Hardware</b>	Trusted Execution Environments (TEEs)	Secure Enclaves	AMD SEV SEV-SNP	Intel TDX	IBM SEL	ARM TrustZone CCA	Nvidia H100
-----------------	---------------------------------------	-----------------	-----------------	-----------	---------	-------------------	-------------

<b>VM / Containers</b>	Kata Containers	Confidential Containers (CoCo)	RedHat OpenShift	<b>Cloud</b>	AWS	Azure	GCP
------------------------	-----------------	--------------------------------	------------------	--------------	-----	-------	-----

**Hardware Root of Trust**

**Remote Attestation**

## National ID System – Confidential Computing Architecture



- KEY BENEFITS**
- ✓ Data decrypted only in trusted, attested environments
  - ✓ Keys never leave sovereign control
  - ✓ Workloads, images and operators are continuously verified
  - ✓ Strong audit trail of every key release
  - ✓ Sovereign control of data while still leveraging cloud scale

# 4 pillars that support Digital Sovereignty

## Sovereignty at Rest

Encryption at Rest

Zero-Trust of data-stores

## Sovereignty in Use

Encryption in Use

Zero-Trust of data-processors

## Sovereignty in Transit

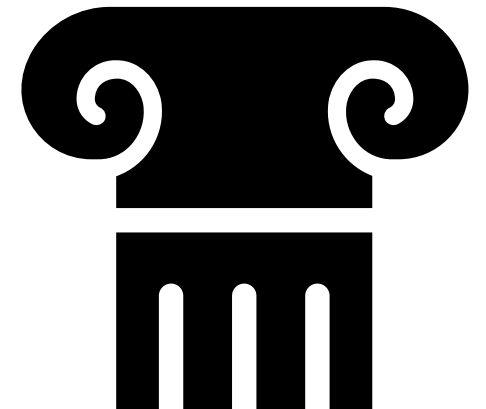
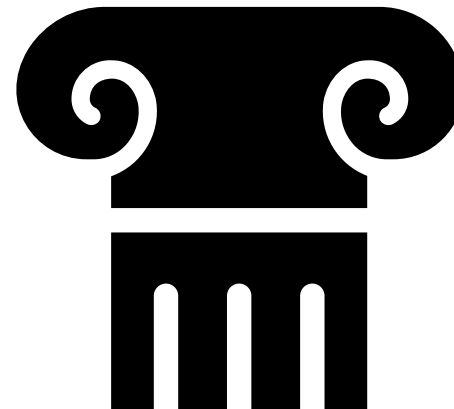
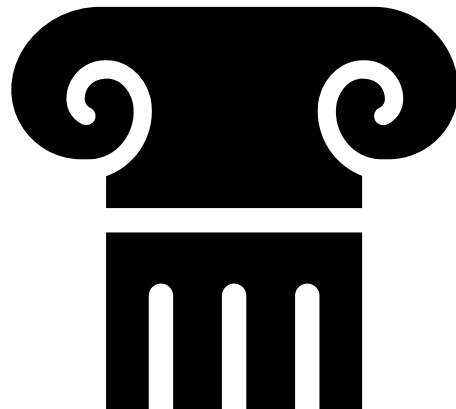
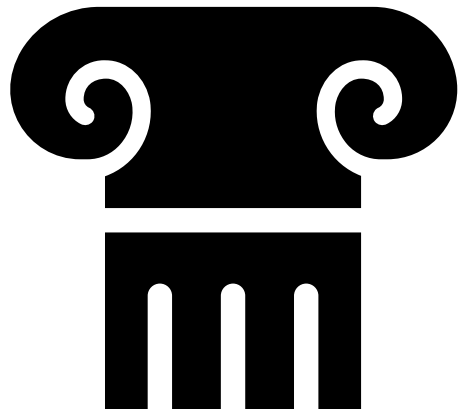
Encryption in Transit

Zero-Trust of microservices

## Sovereignty of Logic

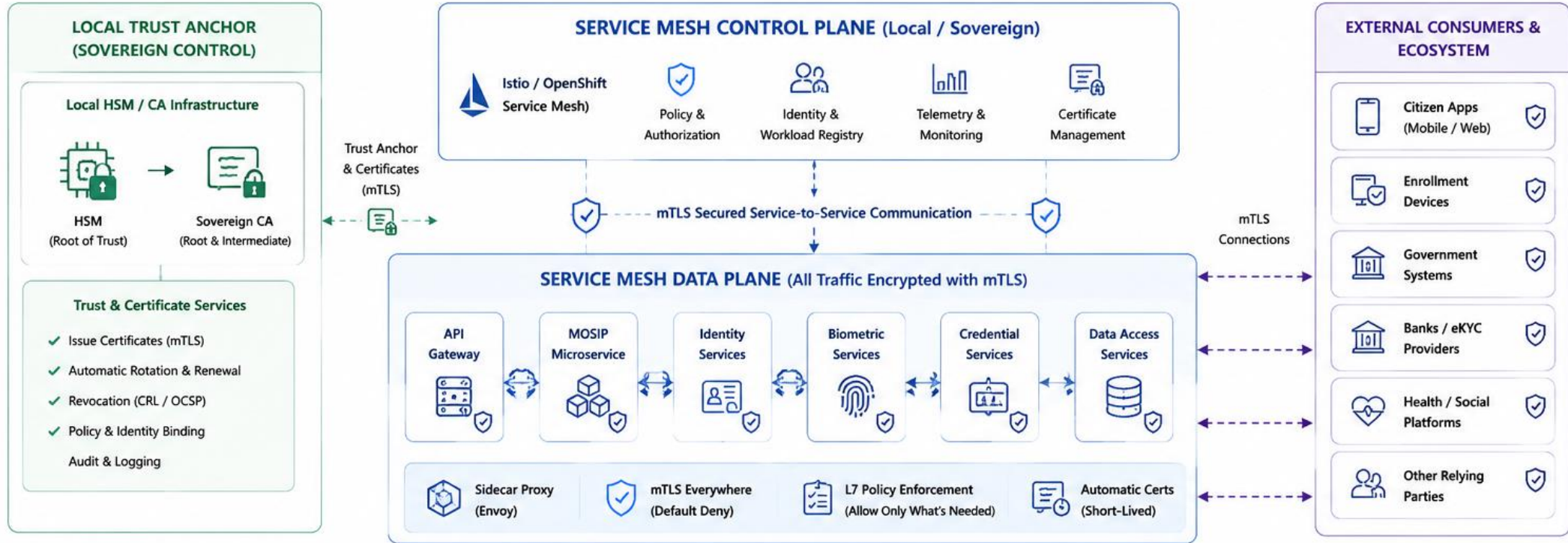
Own the Platform

Zero-Trust of Vendors



# Sovereignty in Transit

## National ID System – Zero Trust Network with mTLS & Service Mesh



### SOVEREIGN NETWORK TRUST FABRIC

- ✓ No Implicit Trust  
Verify Every Identity
- ✓ Encrypt Every Connection  
mTLS Everywhere
- ✓ Least Privilege Access  
Policy Driven
- ✓ Automatic Lifecycle  
Certificates
- ✓ Full Visibility  
Logs & Telemetry

### HOW IT WORKS (Simplified Flow)



### KEY BENEFITS

- ✓ Sovereign control of trust anchors (HSM-backed CA)
- ✓ Zero trust: no service or user is trusted by default
- ✓ mTLS protects data in transit across all workloads and networks
- ✓ Automatic certificate management reduces risk and toil
- ✓ Consistent security across on-prem and cloud environments

# 4 pillars that support Digital Sovereignty

## Sovereignty at Rest

Encryption at  
Rest

Zero-Trust of  
data-stores

## Sovereignty in Use

Encryption in  
Use

Zero-Trust of  
data-processors

## Sovereignty in Transit

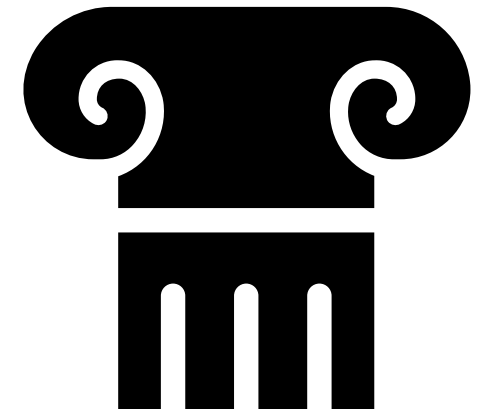
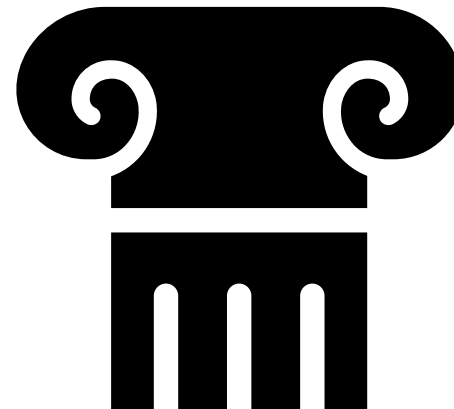
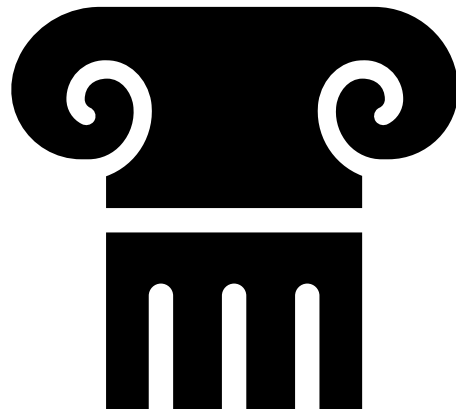
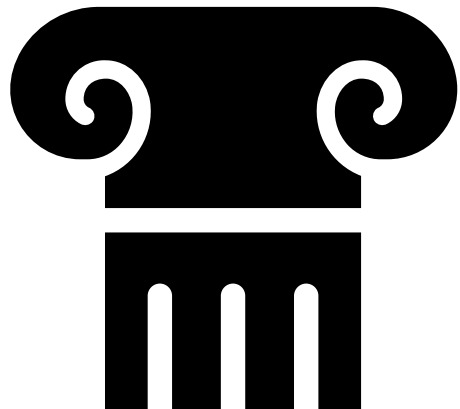
Encryption in  
Transit

Zero-Trust of  
microservices

## Sovereignty of Logic

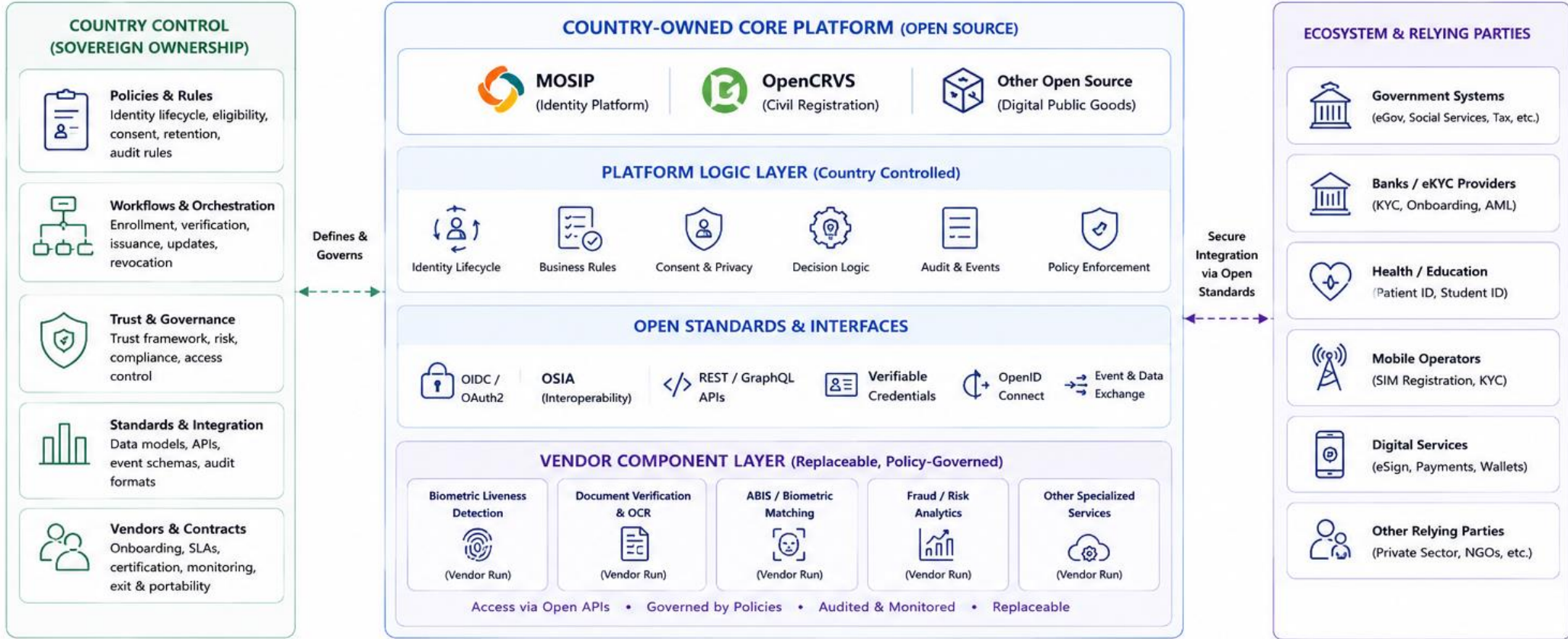
Own the  
Platform

Zero-Trust of  
Vendors



# Sovereignty of Logic

## National ID System – Open Platform, Open Standards, Controlled by the Country



LEGEND: Control / Governance    Integration via Open Standards    Policy & Governance Flow

**Sovereignty of Logic** = The country owns how the system works. Vendors may run components, but they do not control the platform.

# Digital Sovereignty is a DPI enabler...

## Sovereignty at Rest

The ecosystem may store the data resiliently,  
because it cannot read it without sovereign approval and continuous verification of trust.

## Sovereignty in Use

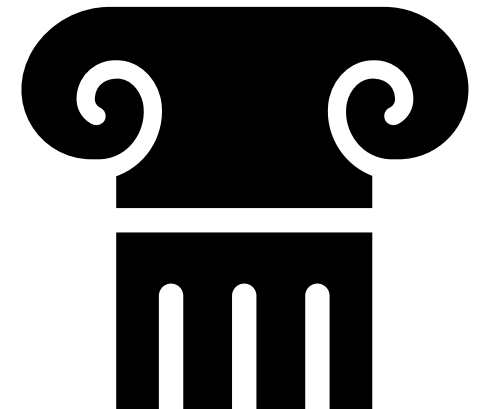
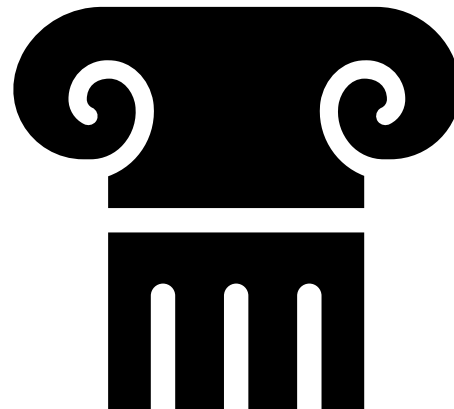
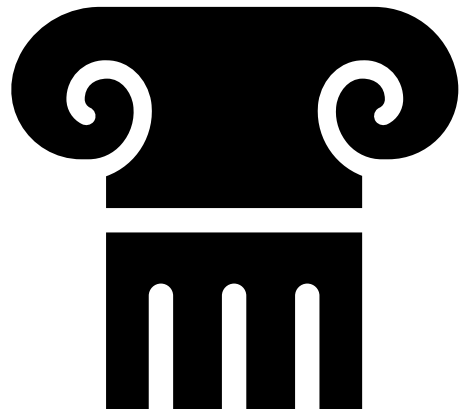
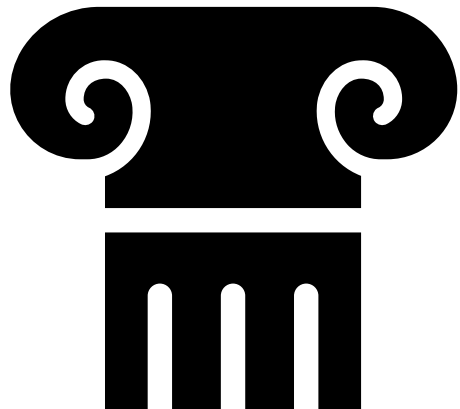
The ecosystem may process sensitive data,  
because computation is restricted to attested confidential environments.

## Sovereignty in Transit

The ecosystem may exchange data openly,  
because every interaction is authenticated, encrypted, consent driven and policy governed.

## Sovereignty of Logic

The ecosystem may innovate freely,  
because open standards and sovereign governance prevent dependency and preserve interoperability.



## Old Guard

- Perimeter firewalls
- Private networks
- Trusted insiders
- Closed infrastructure
- Centralized ownership

“Restricted access only. If you are inside the fence, you are blindly trusted.”

## New Guard

- Open APIs
- Multiple providers
- Wallets
- Banks
- Health systems
- Governments
- Cloud providers
- Regional interoperability

“Everyone is free to enter, because trust is continuously verified and cryptographically proven”

# Thank you

Darren Lentz  
Darren.Lentz@kpmg.co.za



© 2026 KPMG Services Proprietary Limited, a South African company with registration number 1999/0 12876/07 and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.