REVYCORE

WHITE PAPER

Sovereignty & Audit Evidence.

Data, keys and decisions, in your jurisdiction.

REVYCORE RESEARCH

DECEMBER 2026

EXECUTIVE SUMMARY

Sovereignty is a requirement. It must be demonstrated, too.

Ministries, agencies, local authorities, operators of essential services and regulated industries share a requirement, whatever their jurisdiction: keep the data, the keys and the decisions at home, and be able to prove it.

Access certification touches all three. It processes identities and entitlements, seals evidence with cryptographic keys, and records human decisions that may be examined years later.

This paper describes the properties a certification platform needs to meet sovereignty requirements by design: regional isolation, keys per tenant, no implicit vendor access, evidence that stands without the vendor, and humans who always decide.

01 **A region you choose**
And nothing leaves it.

02 **Keys per tenant**
No platform-wide secret to steal.

03 **No implicit vendor access**
Support access is explicit and consented.

04 **Evidence without the vendor**
Verifiable, exportable, in open formats.

CONTENTS

01 Three things to keep at home
02 A region, and nothing leaves it
03 Keys that belong to you
04 The vendor does not see your data
05 Evidence that stands without the vendor
06 Where to start

01

Three things to keep at home

Sovereignty is often reduced to data location. For access certification, it has three components. The data: identities, entitlements and observations. The keys: those that seal the evidence. And the decision: the human judgement recorded in each attestation.

Each can escape jurisdiction in a different way: data replicated abroad, keys held by a vendor, decisions taken or altered by a system outside the organisation's control.

Sovereignty by design. requirements met by the architecture itself, rather than by contractual commitments added afterwards.

> **The data, the keys and the decision.**

02

A region, and nothing leaves it

In a sovereign design, authentication, the sealing authority, secrets, mail and the audit trail all run in the region of the subscription. A central control plane, if any, holds only metadata and never reads inside a region.

Larger organisations may need more: a dedicated silo for a single client, or a deployment on their own servers when the regulator requires it. Moving between these models should be a migration, never a copy.

01

Shared cell

Isolated per subscription, in the chosen region.

02

Dedicated silo

One client, one silo, never two.

03

On-premises

For isolated or classified environments.

04

Metadata only

Nothing from inside a region leaves it.

> **Every service runs where your law applies.**

03

Keys that belong to you

Evidence is only as trustworthy as the keys that seal it. Each subscription should seal with its own key, held in a vault that application hosts cannot open, with the possibility of importing the organisation's own signing key.

One authentication application per client removes the platform-wide secret whose theft would compromise everyone.

> **One key per tenant. No platform secret.**

04

The vendor does not see your data

Vendor staff should have no implicit access to client data. Where support requires access, it should be explicit, time-bound, consented to by the client, and written into the client's own audit trail.

The same structural rule that prevents administrators from recording decisions should prevent the vendor from reading, so that both are enforced by the system rather than by policy.

- **Explicit.** Requested for a stated reason.
- **Time-bound.** Expires on its own.
- **Consented.** Approved by the client.
- **Traced.** Written into the client's own trail.

> **The rule that stops administrators deciding stops the vendor reading.**

05

Evidence that stands without the vendor

Sovereignty also means independence over the long term. Evidence, audit trail and configuration should be exportable in open formats; the verifier and the keyring of the sealing authority should be published, so that an auditor can verify a package with no account and without contacting the vendor.

And humans should decide, always: no system signature, no delegated signatory, no decision action available to an assistant. Facing the AI Act or a works council, the answer is structural, not a policy.

> **Leave with everything. Verify without us.**

06

Where to start

Assessing sovereignty starts with three questions about data, keys and decisions, asked of every tool that processes access and evidence.

1 **Locate every service** that processes identities, entitlements and evidence.

2 **Identify who holds the sealing keys** and who can open the vault.

3 **Check how vendor access works:** implicit, or explicit and consented.

4 **Test independence:** export the evidence and verify it without the vendor.

5 **Confirm that only humans decide,** by design.

> **Ask the three questions of every tool that touches access.**

REVYCORE

Your jurisdiction, by design.

Human decisions. Verifiable evidence.

Request a demonstration in your context: your solutions, your scopes, your agents.

revycore.com

This paper describes sovereignty principles and the corresponding capabilities of REVYCORE for information purposes; it is not legal advice. Deployment options depend on the edition chosen. © 2026 REVYCORE SAS.