POSITION PAPER · FIRST EDITION · JULY 2026

A Sovereignty Test for Small-State Digital Infrastructure

Ten requirements any funder, vendor or partner should be able to meet — before the contract is signed. Three of them non-negotiable.

Engracia Sleeswijk, MBA
Architect of Digital Sovereignty for Small States

Developed for and piloted in Suriname — offered to every small state that intends to remain the owner of its own digital future.

CONTENTS

How to read this paper

This is a working instrument, not an academic study. It is written for the director, minister, permanent secretary or programme lead who signs — or advises on — digital infrastructure agreements, and who has ten minutes and one question: *how do we remain the owners of our own digital future?* Read section 3 first if you are in a negotiation this week. Read from the start if you are designing a programme.

SECTION 1

The Problem

Whoever funds it, decides the stack.

Not openly. Not in the headline of the press release. But inside every financing package for digital infrastructure sits an architecture: the hardware that arrives with the loan, the licences bundled with the grant, the hosting terms attached to the partnership, the standards that the supplier happens to use. None of these are presented as architectural decisions. All of them are.

Large states absorb this quietly. They have procurement agencies, legal departments, competing vendors and the market power to renegotiate. Small states have none of these buffers — and they are currently receiving historic investments in their digital future from development banks, bilateral partners and technology powers who each bring their own preferred stack.

The result is predictable and observable across regions: registry systems that only one foreign vendor can maintain; identity platforms whose cryptographic keys sit outside the country; e-services whose five-year costs exceed their build price several times over; and exit clauses that exist on paper but have never been tested, because testing them would switch off a public service.

The uncomfortable part

None of this requires bad intent. Funders finance what they know. Vendors sell what they build. Advisors recommend what they have seen work elsewhere. The architecture is decided by accumulation, not by conspiracy — which is precisely why it is so hard to resist after the fact. There is no single decision to appeal, no single contract to renegotiate. The stack simply *arrives*.

Small states feel this last and pay for it longest. The first years of a locked-in system look like success: services launch, ribbons are cut, reports are filed. The costs surface in year four — at renewal, at the first major change request, at the moment a second supplier is needed and cannot connect, or at the moment the country wants its own data back and discovers what "export" means in the annex.

This paper proposes a different sequence.

SECTION 2

The Principle

> *Sovereignty is not built by refusing partners. It is built by receiving every partner with the same requirements.*

A small state cannot outspend its funders, out-negotiate a global vendor, or out-lawyer a treaty partner. What it can always do — at almost no cost — is put its requirements on the table first. The same test for the biggest power and the smallest supplier. The same questions about data, exit and ownership — asked before the contract, not after the incident.

This changes the nature of every negotiation without souring any of them. A published requirements framework is not directed *against* anyone; it applies to *everyone*. It allows a director to welcome an offer warmly and test it rigorously in the same meeting. It converts "we are not sure about this vendor" — a political statement — into "this offer does not yet meet requirement 3" — a technical one. Technical statements can be fixed. Political ones start fights.

Requirements first. Contracts second.

The order matters more than the content. Requirements written after the money has arrived are read as obstruction. The same requirements, published before the first meeting, are read as professionalism — and they quietly become the standard that every subsequent offer is measured against, including offers the state has not yet received.

The ten requirements in the next section are deliberately few, deliberately plain, and deliberately answerable in one meeting. Three of them are marked as non-negotiable: they touch jurisdiction and state authority, and no discount, deadline or diplomatic warmth is worth trading them away.

SECTION 3

The Test

Score every offer — from any funder, vendor or partner — against all ten. Each requirement ends with the one question to ask in the room. An answer of "that is in the annex" counts as *unclear*, and unclear is not a yes. If any of the three non-negotiable requirements fails, the offer fails — regardless of how well the rest scores.

01 Open, published interfaces

WEIGHS HEAVILY

Interfaces follow open standards that any competent party can implement. No interface that only the supplier itself can operate.

Ask: Can a third party connect to this interface without your permission or licence?

02 Data stays under national jurisdiction

NON-NEGOTIABLE

Personal data and base registries fall under national law, wherever the technology physically runs. No foreign access rights through the back door of a contract.

Ask: Under which law does the data fall — and who can reach it without our consent?

03 Full exit within thirty days

NON-NEGOTIABLE

Complete export of data and configuration in an open, documented format, free of charge — including in conflict or early termination.

Ask: Show me what the export looks like. Now, not in the annex.

04 No black box in critical services

WEIGHS HEAVILY

For custom-built components the state holds source code or a working escrow arrangement. Standard products may be closed; critical custom logic may not.

Ask: What happens to this system if your company no longer exists in three years?

05 No exclusivity

WEIGHS HEAVILY

No offer may exclude, delay or surcharge later connections with other suppliers or institutions.

Ask: Does anything in this contract say we may not put something next to you later?

06 Identity remains state authority

NON-NEGOTIABLE

Issuing, key custody and revocation of digital identity are acts of state. Vendors supply technology — never the authority, never the keys.

Ask: Who holds the keys, and who can revoke an identity?

07 Transferable to national staff

WEIGHS HEAVILY

Operations and further development are executable by the country's own staff after delivery. Training and documentation are in scope and measurable at handover.

Ask: How many of our people can run this on the day your team flies home?

08 Works in the interior

WEIGHS HEAVILY

Citizen-facing components demonstrably function on low bandwidth and interrupted connections, including a defined degraded mode.

Ask: Has this been tested on a connection like our interior — and where is that recorded?

09 Five-year costs fully visible

WEIGHS HEAVILY

Licences, renewals, support, data traffic and migration costs stated explicitly next to the build price.

Ask: What does this cost in year four — and what does it cost to stop then?

10 Auditable by the state itself

WEIGHS HEAVILY

Logging, access control and change history are inspectable by the country itself, without depending on the supplier.

Ask: Can we see for ourselves who accessed which data, and when?

Scoring is deliberately blunt: **meets**, **does not meet**, or **unclear**. Eight or more "meets" with all three non-negotiables intact: acceptable — now move the requirements from the presentation into the contract. Anything less: keep negotiating, and let the gaps do the talking.

SECTION 4

Applying the Test

The test is designed for the room, not the archive. It takes ten minutes, requires no legal department, and works best when it is visibly on the table — literally printed, literally present — before the presentation starts.

A worked example

A director of digital government receives a strong delegation: an experienced international vendor, backed by a friendly government, offering to modernise the national registry layer at a price well below market. The demonstration is excellent. The pressure to say yes in the room is real — the delegation flies home on Friday. *(The example is a composite; every element is drawn from situations that recur across small states.)*

The director does not argue with the offer. She thanks the delegation, opens the test, and asks three questions: under which law does the data fall (02); show me the export, now (03); who holds the identity keys (06). Two answers are confident. The third — the export — is "in the technical annex".

That is the whole method. The director has not said no. She has said: *requirement 03 is unclear, and unclear is not a yes — come back with the export demonstrated and we continue.* The delegation can fix this by Friday, or it cannot. Either way, the country has lost nothing and learned everything, in ten minutes, without a single confrontational word.

Three habits that make the test work

Publish it. A test that lives in a drawer protects no one. Published — on a ministry page, in a programme document — it shapes offers before they are written.

Apply it symmetrically. The fastest way to lose the test's protection is to waive it for a friend. Its authority comes from the fact that everyone gets the same ten questions.

Move it into the contract. A requirement met in the presentation but absent from the contract was never met. The test's final step is always the same sentence: *"Excellent — let's write that down."*

SECTION 5

The Layers Behind the Test

The ten requirements are not arbitrary; they protect a target picture. Five layers, each with a single neutrality rule. A state that holds these five rules can buy technology from anyone.

Layer 1 — Channels

Counters, portals and apps through which citizens reach government.

Rule: No service may be reachable exclusively through one supplier's app or portal.

Layer 2 — Services

The service logic itself: what a citizen applies for and the steps that follow.

Rule: Service logic stands apart from the platform it runs on, and can be moved.

Layer 3 — Data & registries

Base registries as the source of truth, queried through published service contracts.

Rule: The registry is the source; consumers query it — nobody keeps a shadow copy.

Layer 4 — Identity

Establishing who someone is, with which authority, across institutions.

Rule: Issuing, key custody and revocation stay in national hands. The technology can be bought; the authority cannot.

Layer 5 — Infrastructure

Where it runs, how it is connected, how it survives outages.

Rule: Decide last. This layer stays open until a national data-sovereignty policy is in place — an infrastructure choice made before that policy is an architecture decided by accident.

Note the direction of dependency: channels change often, services sometimes, registries rarely, identity almost never — and infrastructure should be the *most* replaceable layer of all, not the least. Most lock-in does exactly the reverse: it makes the bottom layer permanent and lets it dictate everything above. The test exists to keep the pyramid the right way up.

SECTION 6

What Small States Can Do This Quarter

None of the following requires a vendor, a loan, or a large budget. Each step has value on its own; together they change the state's negotiating position permanently.

1. Publish the requirements

Adopt this test — or your own version of it — and publish it where every future partner will find it. From that day, every offer is written to meet it. Cost: an afternoon and a decision.

2. Inventory the registries

List every base registry and core service: what it is, where it runs, who owns it, who can change it, and how it is reached. Most small states discover in this exercise that nobody holds the complete list — which means, in practice, that nobody holds the architecture. Cost: weeks of asking, not months of building.

3. Name the owner of every interface

For each connection between systems, name the institution that owns it — not the vendor that built it. Interfaces without owners become vendor property by default. Cost: a decision per interface, and the authority to write it down.

Developed for and piloted in Suriname — offered to every small state that intends to remain the owner of its own digital future.

ABOUT THE AUTHOR

Engracia Sleeswijk, MBA

Engracia Sleeswijk works at the intersection of three disciplines that rarely share a room: architecture, legislation and capability. Her practice combines more than twenty years of IT leadership across complex programmes, an MBA in Strategy, Consultancy and Change Management, accredited teaching and curriculum development at professional-education level, and legislative drafting under ministerial mandate.

Her conviction is simple: most advisors bring one room, and implementations die in the other two. Technology answers *can we*; legislation answers *may we*; capability answers *can we keep doing it without help*. Small states deserve all three — in one hand, on their own terms.

She writes and speaks on digital sovereignty for small states. Invitations for keynotes, panels and advisory programmes: sovereignty.engracia.info

COLOPHON

A Sovereignty Test for Small-State Digital Infrastructure — Position paper, first edition, July 2026, The Netherlands.