IFIP EGOV 2026 · FULL RESEARCH PAPER

Tenant in your own house

The wickedness of regaining digital sovereignty over digital public infrastructures

Nitesh Bharosa [1] · Wouter Welling [2] · Mark de Reuver [1]

[1] Delft University of Technology — Faculty of Technology, Policy and Management
[2] Digicampus / Ministry of the Interior and Kingdom Relations, The Hague

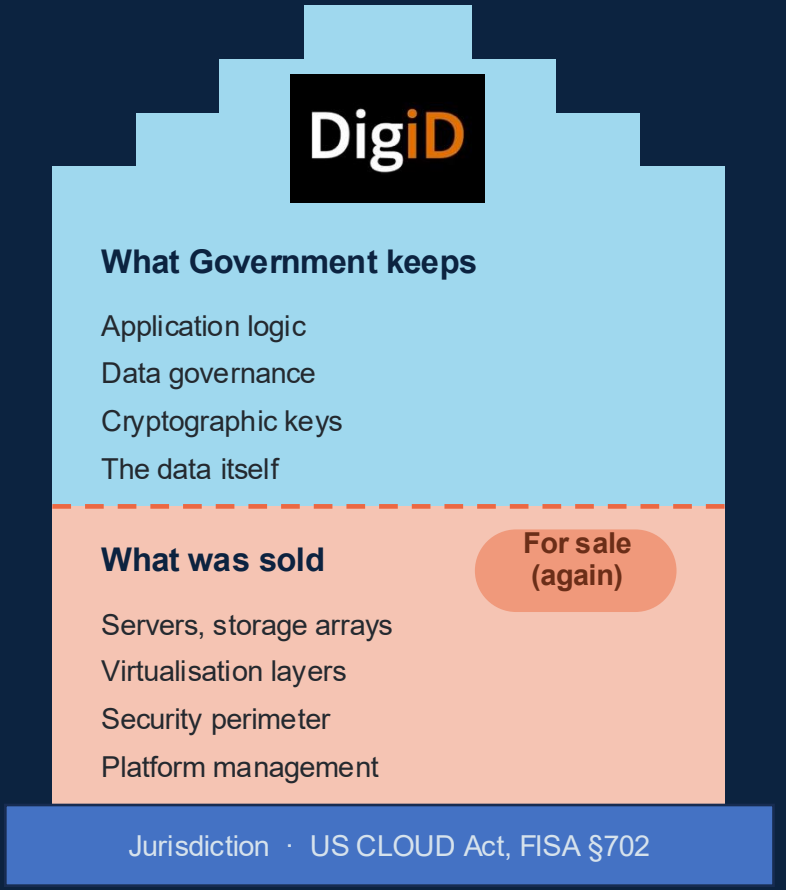
WOUTER WELLING

Declared everywhere, defined nowhere

- Digital sovereignty over digital public infrastructures is not explicitly defined — not in the Dutch coalition agreement, nor in its accompanying policy documents.
- Depending on political position, proposed measures range from nationalisation and state-owned infrastructure to market protectionism and restrictions on market access.
- This paper provides conceptual clarity and identifies the challenges and pathways for digital sovereignty in the public sector.

CENTRAL QUESTION

What are the challenges and pathways to boosting digital sovereignty over digital public infrastructures?



Not only a Dutch problem — Europe consumes the infrastructure it no longer owns

80%+

of Europe's digital infrastructure and technologies are imported and consumed as services

Bria, Timmers & Gernone (2025)

80%+

of the European cloud market is controlled by three US hyperscalers — AWS, Microsoft Azure, Google Cloud

EuroStack (2025); OECD (2025)

zero

European operating-system developers, relevant search engines, global social networks or competitive cloud infrastructures

Moerel & Timmers (2021)

THE BREAKING POINT – February 2025

The restriction of digital services for the International Criminal Court in The Hague turned an abstract dependency into a demonstrated capability — and made digital sovereignty a political question across Europe.

The Dutch breaking point — twelve months that forced the question

2025

The Dutch Tax Office decides to migrate to Microsoft Office 365, raising concerns over foreign access to sensitive financial data and a unilateral 'kill-switch'.

Nov 2025

Kyndryl, a US-based IT infrastructure provider, announces its intention to acquire Solvinity — operator of the platform on which DigiD runs.

Coalition

The new cabinet appoints the first State Secretary of Digital Economy and Digital Sovereignty. Days later, the Railway Agency outsources infrastructure to a US firm.

Jan–Feb 2026

Parliamentary roundtable on the consequences of the Solvinity takeover for DigiD; the government sends its state-of-play letter to parliament.

Yet nowhere in the coalition agreement or the accompanying policy documents is digital sovereignty over digital public infrastructures actually defined. That definitional vacuum is where our paper starts.

The ownership paradox: DigiD, Solvinity, Kyndryl

16.5 M

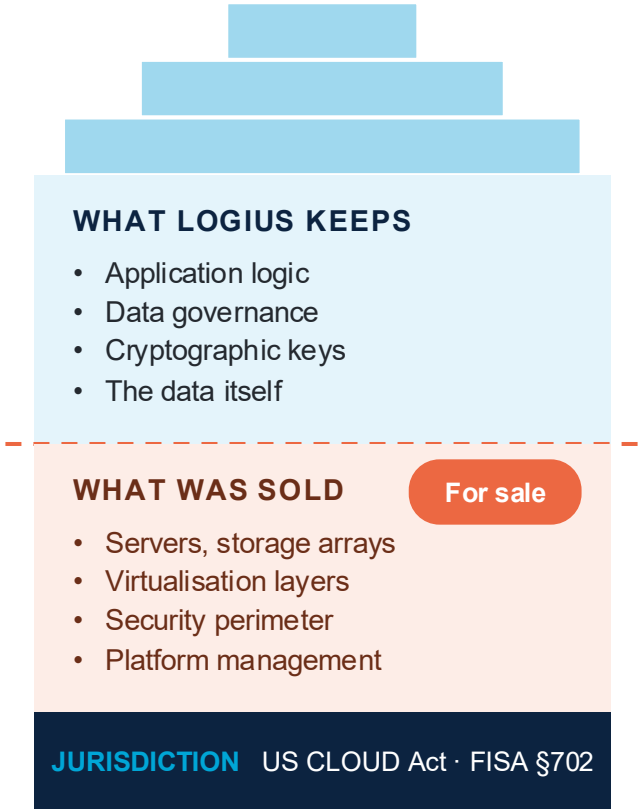
citizens for whom DigiD is the digital identity (authentication under eIDAS)

~550 M

authentications processed every year

since 2020

Solvinity has operated the secure DigiD platform, commissioned by Logius (new procurement every 5 years)



Logius (NL) — formal owner of DigiD

"DigiD is Dutch and remains Dutch" — technical briefing to parliament

The line Logius draws

Application vs infrastructure — a distinction that is coherent, and insufficient

Sold: Solvinity (NL / UK), perhaps to Kyndryl (US)

Ultimate beneficial ownership moves out of EU jurisdiction

The infrastructure now answers to another country's courts

US CLOUD Act, FISA Section 702 reach data held on US-owned providers

Mind the gap: what the paper sets out to answer

THE SOVEREIGNTY GAP

ASPIRATION
control over its own affairs

THE GAP
the disparity a state must close

REALITY
concrete digital dependencies

Moerel & Timmers (2021)

MAIN QUESTION
What are the challenges and pathways to boosting digital sovereignty over digital public infrastructures?

A What does digital sovereignty mean when the object is a digital public infrastructure?

B Which structural challenges widen the gap between aspiration and digital reality?

C Which action pathways can governments follow to close that gap over time?

Sovereignty is the what; strategic autonomy is the how

DIGITAL SOVEREIGNTY — THE WHAT

- The aspiration to independence and control (Couture & Toupin, 2019)
- Central to policy discourse over the last decade (Pohle & Thiel, 2020)
- Hard to define — and harder to operationalise in clear-cut metrics

DIGITAL STRATEGIC AUTONOMY — THE HOW

"The capabilities, capacities and control to decide and act autonomously on essential digital aspects of our economy, society and democracy." — Timmers (2023)

- **Capabilities** knowledge, skills, tools
- **Capacities** the resources available
- **Control** influence over all of the above

THE SOVEREIGNTY GAP

the disparity between aspirations for control and the reality of digital dependencies (Moerel & Timmers, 2021). Four pressures widen it:

1 BigTech dominance

Vendor lock-in to a few foreign hyperscalers

2 Geopolitical tensions

Extraterritorial claims; the US CLOUD Act reaches abroad

3 Cyber threats

Attacks without ever entering the territory

4 Declining capacity

Consumers can no longer examine their dependencies

An exploratory, qualitative single-case study

DESIGN

- Explorative qualitative case study
- DPI cannot be separated from its institutional, operational and technical context
- Many interacting challenges a quantitative design cannot do justice to

CASE & UNIT OF ANALYSIS

- The proposed 2025 acquisition of Solvinity (NL/UK) by Kyndryl (US)
- Selected because it illustrates the sovereignty gap concretely
- A critical stress test for European digital autonomy

DATA SOURCES

- Document corpus: everything the Dutch parliament made public on the takeover
- Technical briefings from Logius; formal inquiries of the House
- Factual claims verified against public sources

1

Deductive coding with PESTEL

A longlist of empirical challenges is categorised into Political, Economic, Social, Technological, Environmental and Legal factors (Andersen, 2025).

2

Mapping onto the wicked-problem lens

Categorised challenges are mapped against Head & Alford's (2015) three dimensions — social pluralism, institutional complexity, scientific uncertainty.

Six structural drivers of the sovereignty gap

P Political

- Parliament wants a line drawn; Economic Affairs wants an open investment climate
- Confronting US tech is tempered by reliance on US intelligence

E Economic

- US hyperscalers hold 80%+ of the EU cloud market
- Procurement law mandates the most economically advantageous tender

S Social

- Convenience bias: citizens expect frictionless, app-like services
- Path dependency locks in how civil servants work

T Technological

- An outsourced horizontal layer becomes a single point of failure
- Near-zero European compute for AI-driven governance

E Environmental

- The Dutch electricity grid is effectively full
- Incumbents already hold the connections hyperscalers colocate in

L Legal

- EU procurement forbids discrimination on nationality
- Screening acts exist, but their reach over cloud is contested

Regaining digital sovereignty is a wicked problem

HEAD & ALFORD'S THREE DIMENSIONS

Social pluralism

Multiple stakeholders holding diverging values and interests

Institutional complexity

Fragmented, multi-level interdependencies across organisations

Scientific uncertainty

Fragmentation and gaps in reliable knowledge; no definitive solutions

HOW THEY APPEAR IN THE CASE

There is no stopping rule

When is a state 'sovereign enough'? Complete autarky is impossible, so sovereignty is an ongoing negotiation, not a destination.

Solutions spawn new problems

Building local data centres immediately relocates the problem into another policy arena — access to the energy grid.

Opposing values, internally

Economic Affairs frames it as 'maintaining an open economy'; the Interior frames it as 'safeguarding national security'.

Stakeholders cannot even agree on the problem definition — which is why linear policy interventions are insufficient, and adaptive strategies such as ecosystem orchestration are required.

A dual imperative: fire-fighting and fire prevention

Interlinked dependencies cannot be resolved through a single intervention: governments must act to prevent the acute loss of sovereign assets while simultaneously unwinding long-term market dependencies.

PATHWAY I

Fire-fighting

Reactive legal and institutional interventions to block imminent threats to digital control, as in the Solvinity takeover.

- Block the concentration (Competition Act — ACM: no basis)
- Invoke the Vifo Act on national-security grounds
- Negotiate a carve-out — precedent: iDEAL → Wero

Holds the line — but does not, by itself, close the gap.

PATHWAY II

Fire prevention

A proactive shift from passive buyer to ecosystem orchestrator, cultivating a viable sovereign European stack over time.

- Distinguish vital components (sovereign) from service components (commercial)
- Cultivate alternative European suppliers, not winner-takes-all tenders
- Eurostack — common standards and open APIs (progressing slowly)

The mechanism that actually closes the gap.

Both pathways must be pursued simultaneously — an exercise in organisational ambidexterity, not a choice between two options.

Implications, theory, and where this paper stops

1 Policy & practice

- Stop being a passive consumer of monolithic IT, head towards market shaping competences
- Orchestrate an ecosystem; treat vital components as strategic state assets, not commodities
- Operationalise the EU Cloud Sovereignty Framework — mandate SEAL 3/4 for critical components
- Reprice the trade-off: confront the 'sovereignty premium' explicitly

2 Theoretical implications

- Bridges the wicked-problems literature with digital sovereignty
- Specifies Mazzucato: ecosystem-oriented market shaping — deliberately forming a diversified supply side
- Two pathways as organisational ambidexterity, not a binary choice

3 Limitations & future research

- Single case; first-order PESTEL analysis; the case is still ongoing
- Test adaptive governance tools (e.g. SEAL) across contexts
- Institutional design for GovTech orchestration
- Theorise relational sovereignty and the 'sovereignty premium'

Tenant in your own house

Digital sovereignty over a digital public infrastructure is an ongoing negotiation, not a final destination — and a state cannot negotiate over what it has stopped orchestrating.

The keys were never the question.

Thank you — questions welcome

Nitesh Bharosa n.bharosa@tudelft.nl
Wouter Welling wouter.welling@minbzk.nl
Mark de Reuver g.a.dereuver@tudelft.nl

Document corpus and full reference list are provided in the appendix of the paper.

TU Delft

DIGICAMPUS