Policy Brief Summary

Digital Sovereignty Requires Verifiable Interoperability

Why Open Standards Alone Are Not Enough · Policy Brief No. 2026-002 (EN), Version 2, November 2026

Open standards are regarded as the foundation of digital sovereignty. Using documented cases, this paper shows that they are not enough on their own: what matters is whether a standard is implemented in such a way that products are demonstrably interchangeable. It expands on Section 3.2.2 of Policy Brief No. 2026-001 "Digital Sovereignty in Europe".

Formally Open, Locked In in Practice

Microsoft Office shapes the market: an estimate by Compass Lexecon commissioned by the Open Cloud Coalition puts Microsoft's share of productivity software in the EU public sector at around 77%, and at up to 90% for office applications. At such shares, the behaviour of the dominant implementation becomes the de facto benchmark – regardless of the standard or of intent.

Documents: OOXML has been ISO/IEC 29500 since 2008. To this day, Office saves by default in the Transitional variant, which was intended as a transition for existing documents – not in the cleaned-up Strict variant. Anyone who wants to exchange documents reliably with Word needs Microsoft's own specifications in addition to the standard and must replicate version-dependent product behaviour.

Calendars and contacts: CalDAV (2007) and CardDAV (2011) are open IETF standards. Outlook does not support them natively, in either the classic or the new client; a third-party extension works only in classic Outlook.

Email: In the new Outlook, IMAP accounts remain functionally restricted compared with Exchange accounts. Since an update to Outlook 2016 in 2017, new Exchange ActiveSync accounts can only be set up by a detour; the new Outlook does not support them at all.

Interfaces: Exchange Web Services, on which third-party vendors built for years, has been gradually shut down in Exchange Online since October 2026 and will be shut down permanently from April 2027. Its successor is the proprietary Microsoft Graph API.

→ Formal openness does not automatically lead to practical interoperability.

Two Cases, Two Answers

If an implementation violates the standard, the implementation must be corrected. If the standard permits incompatible implementations, the standard must be made more precise or supplemented by a binding interoperability profile. As with a standardised screw: it must fit the standardised nut within the specified tolerances.

> The paper does not presuppose intent. **It is directed at the demonstrable mechanism: without verifiable conformance, alternative providers and customers who want to switch bear the costs of deviation.**

The Challenge for Users

If a presentation or a contract is rendered incorrectly at the recipient's end, the risk is borne not by the platform provider but by whoever has switched. With every integration – collaboration, identity, automation and, increasingly, AI assistants and agents – switching costs grow further. There is as yet no established open exchange format for the overall context of an AI-supported workplace.

The Regulatory Gap

Since Version 1.1, the framework has moved. The gap remains:

Digital Markets Act: Microsoft is designated as a gatekeeper for Windows and LinkedIn; Teams and the Office applications are not designated core platform services. The proceedings on AWS and Azure concern infrastructure, not office software.

Teams commitments (September 2025): The Commission recognises asymmetric interoperability as a competition problem. The solution, however, is a case-specific arrangement whose effectiveness third parties cannot verify by means of open tests.

Data Act: It requires functional equivalence on switching only for infrastructure services. For office and collaboration services, the export of data suffices until common specifications are available.

CADA and Interoperable Europe Act: The Cloud and AI Development Act (COM(2026) 502) does not test practical interoperability; the Interoperable Europe Act targets cross-border public services, not the interchangeability of office platforms.

→ Europe mandates common chargers and interoperable messengers – but not the verifiable interchangeability of the office software on which administrations and the economy run.

The Proposal: Verifiable Interoperability

A European interoperability certification based on a public test corpus: each test case documents the full editing cycle and classifies every deviation – as a breach of the standard, a gap in the specification, a vendor extension or an implementation error. Three levels:

Level I – Verified Baseline Profile: The service meets the open standards required for its type. Deviations must be disclosed, but disclosure does not replace compliance.

Level II – Verified Interoperability: Defined functions are processed consistently with independent implementations within specified tolerances.

Level III – Verified Switchability: Migration to an independent implementation has been demonstrated in a reference scenario – including effort, costs, parallel operation and remaining dependencies.

Test criteria and results are public, product changes trigger a new test, and deficiencies must be remedied within a deadline. Reduced fees for open-source projects and SMEs prevent certification from itself becoming a barrier to entry.

→ It is not the provider that is regulated. The interoperable property of the product is demonstrated.

What Needs to Be Done Now

1. Use procurement as a lever

Anchor verifiable interoperability and tested switchability as a selection or award criterion in the proposed procurement regulation (COM(2026) 590); gradually require at least Level I for workplace systems and Level II for critical systems and systems subject to archiving obligations.

2. Link the CADA

Tie services at CADA assurance levels 2 to 4 to at least Level II, and services at level 4 additionally to Level III. The highest assurance level should not be attainable without tested replaceability.

3. Issue a standardisation request

A request under Regulation (EU) No 1025/2012 to CEN, CENELEC and ETSI for a European certification framework; at national level, a pilot programme, for example with Austrian Standards International.

4. Examine the DMA

Examine whether Microsoft Office – including in its form as Microsoft 365 – can be covered as a core platform service. The ongoing investigation into cloud services should include office and collaboration services offered as software as a service.

5. Create transparency

Providers disclose their interoperability status. The results of the trustee's monitoring of the Teams commitments are published in a form that allows third parties to verify the promised interoperability.

Key message

Standards without verifiable conformance are not standards. They are promises.

Digital sovereignty means being able to switch systems in practice. Europe has the opportunity to make the difference between formal openness and genuine freedom of choice verifiable.

Full version with all evidence: Policy Brief No. 2026-002 (EN), Version 2 (November 2026), 4future.institute Policy Brief Series, ISSN 3061-1881 (Online), DOI 10.5281/zenodo.24052138. German version prevails: https://doi.org/10.5281/zenodo.24052138

Contact:

Werner Illsinger (Executive Director) | werneri@4future.institute | +43 664 7996221

4future.institute | Graben 17/10 | 1010 Vienna | Austria | Europe

Part of the 4future.group · independent unit within 4future business GmbH ·

Majority shareholder: 4future.foundation · Disclosure: the author is also CTO of 4future.digital (European cloud and collaboration services), which uses the open standards discussed and would be affected by such a certification; 4future.digital is neither named nor assessed in the analytical part of the paper.