Policy Brief:

Digital Sovereignty Requires Verifiable Interoperability

Why open standards alone are not enough.

Version 1.1

June 1st, 2026

Werner Illsinger
Executive Director
4future.institute
werneri@4future.group

This policy paper is part of a series by the 4future.institute on digital sovereignty in Europe. It builds on and deepens the policy brief "Digital Sovereignty in Europe" (4future.institute, V1 November 2025 / V2 June 2026).

Imprint

4future.institute
Graben 17/10 1010
Vienna Austria
+43 1 31440-0

4future.institute is part of the 4future.group and a brand of 4future.business GmbH.

Company Register Number: FN 459359 d
Company Court: Vienna Commercial Court
VAT ID: ATU71656745
Majority Shareholder: 4future.foundation

Executive Summary

The 4future.institute was founded to ask uncomfortable questions. What is actually going on here? What are the structural conditions? And above all: does this make sense — not just economically, but for us as a society?

Digital sovereignty is one of the three strategic questions the 4future.institute works on. This paper is not commissioned work. It is the result of a growing conviction.

Digital sovereignty is one of Europe's central strategic challenges. European digital policy has responded with infrastructure investment, cloud initiatives, and regulatory measures such as the Digital Markets Act. These initiatives are necessary. But they leave one critical dimension of digital dependency largely unaddressed:

the practical interoperability of digital systems.

Open standards have long been considered the foundation of digital sovereignty. This paper argues that formal openness is not enough. What matters is not merely the existence of a standard — but its verifiable, interoperable implementation in practice.

The reality of digital markets reveals a widening gap between formal standardisation and actual switchability. Document formats, APIs, collaboration platforms and communication protocols are frequently supported on paper but implemented asymmetrically in practice. Dominant platform ecosystems typically offer the most complete and lowest-risk user experience. Alternative vendors — even when they support the same standards — carry structural interoperability disadvantages.

The consequences are predictable: switching costs rise, lock-in deepens, and market concentration increases.

The transition to AI-powered knowledge and collaboration systems is making this worse. The next phase of digital dependency is taking shape at the level of semantic knowledge models, platform APIs, AI agents, and organisational context systems. The lock-in of tomorrow will not be about file formats. It will be about who owns the context in which decisions are made.

This paper proposes a European interoperability strategy. Its core elements are: a European interoperability certification scheme, standardised compliance tests, open reference implementations, and binding interoperability requirements in public procurement.

The goal is not to constrain technological innovation. It is to make innovation possible — by ensuring that digital markets remain open and genuinely competitive.

The central argument of this paper is simple:

Open standards alone are not enough. Digital sovereignty requires verifiable interoperability.

Table of Contents

1 Introduction: The Blind Spot of Digital Sovereignty 9
1.1 Digital Resilience and Geopolitical Capability 9
1.2 Digital Sovereignty as a European Challenge 10
1.3 Infrastructure Is Not Enough 11
1.4 Standards as Invisible Power Structures 12
1.5 Purpose of This Paper 13
2 Standards as the Foundation of Digital Power 14
2.1 What Standards Make Possible 14
2.2 Network Effects and Platform Economics 14
2.3 Open vs. Proprietary Standards 15
2.4 Open Source Does Not Automatically Mean Switchability 15
2.5 Formal Openness vs. Practical Interoperability 15
2.6 Standardisation Without Verifiable Conformance 16
2.7 The Difference Between Standardisation and Switchability 17
3 The Battle Over Document Standards 18
3.1 The Historical Dominance of Proprietary Office Formats 18
3.2 The Emergence of the OpenDocument Format (ODF) 18
3.3 Office Open XML (OOXML), ISO Standardisation, and the Strict/Transitional Problem 19
3.4 Why Document Standards Determine Digital Sovereignty 21
3.5 Long-Term Archiving and State Dependency 21
4 Asymmetric Interoperability in Practice 22
4.1 When Standards Are Only "Partially Open" 22
4.2 E-Mail: IMAP as Second-Class Citizen 22
4.3 Calendar and Contacts: CalDAV and CardDAV in Proprietary Ecosystems 23
4.4 Proprietary Extensions, APIs, and Migration-Induced Platform Dependency 24
4.5 "S3-Compatible" and Other Illusions of Switchability 26

5 Collaboration Platforms as the New Dependency 27
5.1 From Document to Platform 27
5.2 Teams, SharePoint, and Integrated Work Ecosystems 28
5.3 Workflow Lock-in 29
5.4 Identity, Communication, and Proprietary Integration 29
5.5 Why Switching Costs Rise Disproportionately 30
6 The Blind Spot of the Digital Markets Act (DMA) 32
6.1 Objectives and Mechanisms of the DMA 32
6.2 Gatekeeper Regulation and Its Limits 32
6.3 Why Work Standards Are Barely Addressed 33
6.4 Platform Power in the Office, Not the App Store 33
6.5 The DMA-Gatekeeper-Question: Microsoft 365 34
6.6 Missing Regulatory Interoperability Mechanisms 35
6.7 The European Interoperability Framework 35
6.8 The Data Act: Important Progress — But Not a Sufficient Answer to Modern Platform Dependency 36
7 The Next Lock-in Wave: AI and Semantic Platforms 38
7.1 From Documents to Knowledge Models 39
7.2 Proprietary AI Ecosystems 39
7.3 Agents and Semantic Dependencies 40
7.4 APIs as the New Standards 40
7.5 Risks for European Digital Sovereignty 41
8 Why Open Standards Alone Are Not Enough 42
8.1 **The Problem of Purely Formal Standardisation** 42
8.2 **Absent Compliance Verification** 42
8.3 **Absent Reference Implementations** 42
8.4 **Absent Migration Capability** 43
8.5 **Open Washing and Pseudo-Compatibility** 43
9 Proposal: European Interoperability Certification 44

9.1 Core Idea and Objectives 44
9.2 An Independent European Certification Body 44
9.3 Technical Compliance Tests 45
9.4 Reference Implementations and Test Suites 45
9.5 Certification Levels, Enforcement, and Financing 46
9.6 Interoperability as Market Transparency 47
9.7 Proportionality, Openness, and Low Entry Barriers 48
10 Public Procurement as a Strategic Lever 49
10.1 The Public Sector as Market Shaper 49
10.2 Certification as a Procurement Prerequisite 49
10.3 Promoting Competition and Innovation 50
10.4 Opportunities for European Vendors 50
10.5 Long-Term Archiving and Sustainability 51
11 Policy Recommendations 52
11.1 To the European Commission 53
11.2 To the Government of the EU Member States 53
11.3 To Standards and Standardisation Organisations 54
11.4 To Civil Society and Academia 54
12 Conclusion 55
I. Annex: About the Author 57
II. Annex: Glossary 58
III. Annex: References 62

1 Introduction: The Blind Spot of Digital Sovereignty

1.1 Digital Resilience and Geopolitical Capability

The growing concentration of critical digital infrastructure in the hands of a few global platform providers creates risks that go well beyond competition policy. They are geopolitical.

European businesses, public authorities, and institutions depend on non-European cloud, communication, and collaboration platforms for functions that are central to how they operate. This dependency is no longer limited to infrastructure. It increasingly extends to organisational workflows, knowledge systems, and AI-powered platform ecosystems.

The result is structural vulnerability. Geopolitical tensions, sanctions, extraterritorial legal claims, or regulatory conflicts can directly impair the operational capacity of European organisations — not in theory, but in practice, and at short notice.

Digital sovereignty cannot therefore be discussed solely through the lens of data protection or competition law. It is increasingly a question of strategic resilience — of Europe's ability to keep functioning when external conditions change.

This is already reflected in European regulation. The NIS2 Directive explicitly treats digital infrastructure as a component of strategic resilience. The conversation about digital sovereignty has moved beyond privacy and market structure. It is now about whether European institutions and businesses can sustain operations under pressure.

Digital sovereignty, under these conditions, does not mean technological self-sufficiency. It means the capacity to remain capable of action — even when geopolitical conditions turn against you.

1.2 Digital Sovereignty as a European Challenge

European digital policy has responded with regulation, infrastructure investment, data spaces, cloud initiatives, and the Digital Markets Act. These initiatives are necessary. They are also insufficient.

One critical structural dimension of digital dependency remains largely unaddressed:

the practical interoperability and switchability of digital systems.

The legal framework of digital dependency — extraterritorial legal claims, the CLOUD Act, FISA 702, the structural limits of the EU-US Data Privacy Framework — is analysed in depth in the policy brief *"Digital Sovereignty in Europe"* (4future.institute, 2025/2026). This paper goes one level deeper. It examines the technical and regulatory dimension: whether digital systems are practically interoperable — and therefore genuinely switchable.

1.3 Infrastructure Is Not Enough

Digital dependency does not begin at the infrastructure layer. It is created every day — in every document that will not open reliably, in every calendar that fails to synchronise, in every API that requires proprietary extensions to function.

Storing data in European data centres does not resolve this. Structural dependency persists when documents cannot be exchanged reliably between different systems, when proprietary extensions define the dominant market standard, when switching platforms carries significant operational risk, or when digital workflows cannot be migrated without substantial loss.

This is most visible in document and collaboration systems. Even within a single platform ecosystem, there are inconsistencies between desktop, web, and mobile implementations of standardised document formats. Open standards such as IMAP, CalDAV, and CardDAV are implemented across different platform ecosystems with varying functionality and integration quality.

The market consequences are direct. Businesses and public institutions gravitate towards dominant platform ecosystems because even minor compatibility deviations can create operational and reputational risk. The decision is rarely about preference. It is about risk avoidance.

Dominant platforms do not consolidate their position through product quality alone. They consolidate it through rising switching costs and the interoperability risks that alternatives carry — risks for which the alternative vendor, not the dominant incumbent, is held responsible.

1.4 Standards as Invisible Power Structures

Standards are the invisible infrastructure of digital markets. They determine how systems communicate, how documents are interpreted, how data is stored — and how easy or difficult it is to switch from one platform to another.

In traditional industries, standardised interfaces, certification schemes, and verifiable interoperability have been prerequisites for functioning markets for decades. USB-C, Ethernet, GSM — mandatory interoperability demonstrably drives competition, innovation, and market transparency. The principle is not controversial. It is simply not yet applied to digital work platforms.

The European Union has already recognised this logic in other domains. It has introduced regulatory requirements to standardise charging connectors and to promote interoperable communication platforms. In the area of digital document and collaboration ecosystems, comparable requirements remain largely absent.

The structural consequence is clear. Formal openness does not automatically produce practical interoperability. Dominant platform implementations define actual market behaviour — regardless of what formal specifications or standards bodies say. A standard that is nominally open but practically implemented only by one vendor is not a standard. It is a facade.

The lock-in effects that follow are not incidental. They shape competition, determine who can enter markets, constrain innovation, and erode long-term digital independence. Standards, in other words, are not technical instruments. They are instruments of power — and treating them as anything less is a political choice with economic consequences.

1.5 Purpose of This Paper

This paper builds on the policy brief *"Digital Sovereignty in Europe"* (4future.institute, 2025/2026) and deepens its chapter on interoperability — specifically Chapter 3.2.2, which defines interoperability as a binding foundation of digital sovereignty and identifies CalDAV, CardDAV, IMAP, and open document standards as minimum requirements. Where that brief stated the demand, this paper provides the empirical basis for why it is necessary: documenting, in concrete terms, why the mere existence of a formal standard is not enough.

The central argument is that open standards alone are not a sufficient foundation for digital sovereignty — not in their legal dimension, not in their technological dimension, and not in their economic dimension as defined in the first policy brief. What is decisive is their verifiable and interoperable implementation in practice.

On that basis, this paper develops a concrete proposal comprising a European interoperability certification scheme, standardised compliance tests, open reference implementations, and binding interoperability requirements in public procurement.

The goal is not to restrict innovation or competition. It is to make both possible. Verifiable interoperability creates digital markets that are open, competitive, and resilient.

Every standard is a good one — if only it were actually a standard.

2 Standards as the Foundation of Digital Power

2.1 What Standards Make Possible

Standards are the invisible infrastructure of modern digital societies. The internet itself would be unthinkable without open, standardised protocols — TCP/IP, HTTP, SMTP, DNS. In traditional industries, standardised interfaces have been a prerequisite for functioning markets for decades: they create interchangeability, reduce switching costs, and enable competition between different vendors.

In the digital domain, standards serve not only a technical function but a strategic one. They determine how easily digital platforms can be switched and how open or closed digital ecosystems remain. Standards define not just technical compatibility — they define economic power.

Whoever controls standards frequently controls access to the market.

2.2 Network Effects and Platform Economics

Digital markets are structurally different from traditional industries. Network effects mean that dominant systems become increasingly attractive as they spread — often regardless of their actual technical merit.

The more widely a particular document format, collaboration platform, or API ecosystem is adopted, the greater the pressure on other market participants to use the same systems. Standards play a central role here, because they determine how compatible alternative systems can remain with the dominant platforms.

The result is markets that increasingly stabilise themselves around existing platform ecosystems. Market concentration in these conditions does not arise solely from innovation or product quality. It arises from rising switching costs and asymmetric interoperability.

Over time, the competitive dynamics of digital markets weaken. New entrants can rarely translate technological innovation into market share when incumbent platform ecosystems are structurally protected by high switching costs. This is particularly visible in knowledge work. Documents, communication systems, and digital workflows must remain compatible with dominant platform ecosystems to avoid economic risk. Even minor compatibility deviations create operational uncertainty — and that uncertainty feeds directly back into market decisions.

2.3 Open vs. Proprietary Standards

Formally, digital standards can be divided into open and proprietary. Open standards are publicly documented and can in principle be implemented by any market participant. Proprietary standards are controlled by individual companies and frequently only partially disclosed.

In practice, this distinction is far less clear than it appears. Formally open standards can contain proprietary extensions, be interpreted differently, or be implemented asymmetrically. A standard can appear formally open while remaining practically dependent on a single dominant implementation.

This is one of the central problems of digital markets. Formal openness does not mean real switchability. The practical significance of a standard is determined less by its specification than by the dominant market implementation.

This is visible today in document formats, communication protocols, and calendar and contact synchronisation.

2.4 Open Source Does Not Automatically Mean Switchability

Open-source platform models do not automatically guarantee long-term interoperability or genuine switchability.

In many digital markets, hybrid models are increasingly common — open base components combined with proprietary extensions, platform-bound cloud services, or commercially controlled integrations. Formally open ecosystems can generate structural dependencies, particularly when core functions, APIs, or organisational workflows remain only partially interoperable or migratable.

Digital sovereignty cannot therefore be defined by licence model or geographic location alone. What matters is the practical ability to operate systems interoperably and to switch vendors for real.

2.5 Formal Openness vs. Practical Interoperability

The existence of an open standard does not guarantee practical interoperability. What matters is not whether a specification is publicly available — but whether different implementations actually work consistently and interchangeably in practice.

In complex document and collaboration systems, differences in rendering, layout, commenting, synchronisation, and workflow behaviour are common. Even

within a single platform ecosystem, inconsistencies between desktop, web, and mobile implementations occur.

The economic significance of these differences is routinely underestimated. Minor compatibility deviations can create operational and reputational risk. Organisations orient themselves towards dominant platform ecosystems precisely to avoid that risk.

For alternative vendors, this creates a structural problem. They bear the economic risk of compatibility deviations even when the cause lies outside their own implementation. Interoperability is not merely a technical challenge. It is a central competitive factor — and one that is systematically stacked against the challenger.

The lock-in effects that follow reinforce existing platform dominance further.

2.6 Standardisation Without Verifiable Conformance

Standards only produce their economic and social effects when implementation is consistent and interoperable behaviour is practically verifiable. Without conformance mechanisms, a paradox emerges: standards exist on paper — but their competitive effect remains limited.

The example of document formats makes this concrete. Office Open XML (OOXML) has been an ISO standard since 2008. Significant differences in rendering, layout, commenting, and collaboration behaviour between different implementations persist nonetheless.

The standardisation of OOXML took place in a politically and commercially contested environment. Critics pointed to the complexity of the specification, the parallel existence of the already established OpenDocument Format (ODF), and the practical difficulty of achieving interoperable implementations across different office systems.

The result is a situation in which multiple standardised document formats coexist, while complete practical interchangeability remains out of reach.

The existence of a standard is not sufficient to ensure open markets. Standards require verifiable conformance, interoperable reference implementations, and practical compliance mechanisms. Without these, standardisation remains formal — and its intended market effect is never fully realised.

2.7 The Difference Between Standardisation and Switchability

Standardisation alone does not mean real switchability between digital platforms. A market remains open and competitive only when documents, data, processes, and digital workflows can be practically migrated between different systems.

The decisive question is therefore not whether a standard exists. It is whether that standard enables real switchability between different platforms.

In many digital markets today, a significant gap exists between formal standardisation and practical switchability. Network effects, platform economics, and asymmetric interoperability widen that gap further.

Ensuring practical switchability is not a technical detail. It is a precondition for digital sovereignty, for functioning digital markets, and for long-term innovation capacity.

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

3 The Battle Over Document Standards

3.1 The Historical Dominance of Proprietary Office Formats

Few areas of digital infrastructure shape daily knowledge work as fundamentally as document formats. Text documents, spreadsheets, and presentations have been the operational foundation of businesses, public authorities, and educational institutions for decades. Documents do not merely contain information — they contain business processes, contracts, decisions, and institutional knowledge.

With the global spread of Microsoft Office from the 1990s onwards, a de facto global document standard emerged. Formats such as DOC, XLS, and PPT became the dominant basis of digital office communication for many years — long before open document standards became politically or regulatorily relevant.

This dominance did not arise from technical superiority alone. Network effects played a central role. The more organisations adopted the same formats, the harder it became for alternative systems to remain compatible. Documents had to work reliably within dominant Office environments to avoid operational risk. That pressure was self-reinforcing.

The result was structural lock-in. Control over document formats increasingly meant control over digital work processes themselves.

3.2 The Emergence of the OpenDocument Format (ODF)

As digital documents became more central to how organisations functioned, political and economic pressure for open, long-term document standards grew in the early 2000s. Public institutions in particular recognised the risk: that core state information could become permanently dependent on a single proprietary platform.

Against this backdrop, the OpenDocument Format (ODF) was developed and standardised in 2006 as ISO/IEC 26300. The goal was a fully open, documented, and vendor-neutral document format — one that could be implemented by different office systems without dependence on any single provider.

ODF was not merely a technical project. It was a political and economic signal: documents should remain readable, exchangeable, and archivable in the long term, independently of any individual vendor.

The debate around open document standards increasingly became a debate about digital sovereignty, competition, long-term archiving, and the role of open standards in public institutions. That debate has not been resolved. It has simply moved to a new arena.

3.3 Office Open XML (OOXML), ISO Standardisation, and the Strict/Transitional Problem

The political and commercial context of OOXML's standardisation is well documented. After the US state of Massachusetts mandated ODF as the required format for government agencies in 2005[1] and similar discussions were underway in European institutions, Microsoft brought its own XML-based document format into the standardisation process. ECMA International established technical committee TC45 for this purpose in December 2005 — chaired by two Microsoft employees.[2]

The subsequent ISO standardisation process was internationally contested. Multiple national standards bodies documented irregularities in the composition of technical committees in the period immediately before votes were held. Formal complaints were filed by Norway[3], South Africa, Brazil, and other countries. In Norway, thirteen members of the technical committee resigned in protest following the ISO ratification. The European Commission opened formal investigations in 2008, in part to examine whether Microsoft had influenced the ISO ballot process. Several national standards bodies — including Sweden — subsequently declared their own votes invalid.

OOXML was nonetheless standardised as ISO/IEC 29500 in 2008.

The standard defines two variants: "Strict" as the fully conformant implementation, and "Transitional" as a backwards-compatibility variant for older Microsoft Office formats. The ISO community had explicitly rejected the Transitional variant in the first ballot attempt in 2007. In practice, Transitional

[1] Commonwealth of Massachusetts, Information Technology Division: Policy for Implementing the OpenDocument Standard, 2007.
Rajiv Shah et al.: *Lessons for Open Standard Policies: A Case Study of the Massachusetts Experience*, University of Illinois, 2007.
[2] https://ecma-international.org/publications-and-standards/standards/ecma-376/
[3] https://arstechnica.com/uncategorized/2008/10/norwegian-standards-body-implodes-over-ooxml-controversy/

remained the dominant implementation for many years — not only among third-party vendors, but within Microsoft itself.

Dr. Alex Brown, chair of the ISO Ballot Resolution Meeting, stated publicly in 2010:

> "Microsoft appears to be on course to fail. In its pre-release form, Office 2010 does not support the approved Strict variant of OOXML — but exactly the format the global community rejected in 2007: the Transitional variant."[4]

The structural consequence is unambiguous. A standard whose primary implementation follows the rejected Transitional variant does not require alternative vendors to implement the formal specification. It requires them to reverse-engineer the behaviour of a proprietary implementation. The actual reference standard is not ISO/IEC 29500 Strict. It is whatever Microsoft Office does.

The coexistence of ODF and OOXML as ISO standards has not produced the interoperability that was promised. It has increased complexity — and deepened structural dependency on the dominant implementation.

[4] *Alex Brown, "On the state of OOXML interoperability", personal Blog, March, 31. 2010*

3.4 Why Document Standards Determine Digital Sovereignty

Document standards are not a technical footnote. They determine how knowledge is stored, exchanged, and remains usable over time.

When documents cannot be exchanged reliably between different systems, when migration is only partially possible, or when formats structurally favour particular platforms, deep dependencies follow. This is not an edge case. It is the normal condition of digital knowledge work today.

The stakes are highest in public institutions and organisations with long-term archiving and documentation obligations. Their documents must remain readable for decades, must be migratable between systems, and must remain accessible independently of any individual vendor. Practical interoperability is not a feature for these organisations. It is a legal and institutional requirement.

Where it is absent, the consequences are predictable: switching costs rise, platform dependencies deepen, and market openness narrows. Document standards are therefore a central infrastructural question of digital sovereignty — not a procurement detail.

3.5 Long-Term Archiving and State Dependency

The importance of open and interoperable document standards is nowhere more visible than in the long-term archiving of state and institutional information.

Government documents, contracts, administrative records, and scientific work must frequently remain readable for decades — sometimes centuries. Proprietary or only partially interoperable formats create substantial risks: future software dependencies, limited migration capacity, loss of formatting or metadata, and long-term loss of control over public information.

Digital sovereignty therefore means more than control over infrastructure and data locations. It means the long-term capacity to read, migrate, and archive your own information independently of any single platform ecosystem.

Public institutions carry a particular responsibility here. Their procurement decisions do not only affect short-term productivity. They shape market structures, competitive dynamics, and the long-term digital resilience of state information systems. Procurement is policy. It always has been.

4 Asymmetric Interoperability in Practice

4.1 When Standards Are Only "Partially Open"

The existence of open standards creates an impression of technical neutrality and switchability. In practice, interoperability rarely works completely. Systems are neither fully open nor fully closed. Instead, hybrid platform ecosystems emerge in which standards are formally supported but implemented with significant variation in depth and quality.

In digital platform markets, even partial asymmetry in interoperability is sufficient to generate strong lock-in effects. Systems broadly work together — but not equivalently. Certain functions remain limited, integrations incomplete, user experiences inconsistent.

The structural market asymmetry this produces is predictable. The dominant platform offers the most complete and lowest-risk user experience within its own ecosystem. Alternative vendors, despite supporting the same standards, are frequently perceived as "not fully compatible." Interoperability is formally guaranteed. Practically, it is progressively constrained.

4.2 E-Mail: IMAP as Second-Class Citizen

IMAP — the Internet Message Access Protocol — has been an open standard for email access for decades, specified in RFC 3501 and maintained by the Internet Engineering Task Force. It remains a central foundation of interoperable email communication.

In modern platform ecosystems, formal standard support does not mean equivalent functionality.

The new Microsoft Outlook, rolled out progressively from 2023, treats IMAP accounts structurally differently from Exchange or Microsoft 365 accounts. Features such as calendar integration, invitation synchronisation, and cross-platform collaboration differ from what Microsoft's own platform services provide.

Microsoft documents this itself: the new Outlook client no longer supports POP and IMAP accounts "in the traditional way." Users with classic POP/IMAP workflows

are explicitly directed to the legacy "Classic Outlook" client or alternative email applications. [5]

Calendar invitations received via IMAP accounts are in some cases processed in local calendar structures that do not automatically synchronise with other Outlook platforms. For users, the result is an asymmetric experience: the open standard remains usable, but does not reach the same integration depth as the proprietary platform ecosystem.

The pattern this illustrates is fundamental to modern platform markets. Standards are formally supported but integrated into the platform ecosystem at varying depths. Interoperability persists — but it is not equal.

4.3 Calendar and Contacts: CalDAV and CardDAV in Proprietary Ecosystems

CalDAV and CardDAV are open standards for calendar and contact synchronisation, specified in RFC 4791 and RFC 6352 by the IETF. They are natively supported by Apple Calendar, Google Calendar, Thunderbird, and the large majority of modern email and calendar clients.

Microsoft Outlook does not support CalDAV or CardDAV natively. A Microsoft employee confirmed this in 2024 on the official Microsoft support platform learn.microsoft.com:

"New Outlook does not currently support CalDAV."

The structural consequences for digital work ecosystems are substantial.

Outlook is the central email and calendar client in many businesses and public institutions. It reaches its deepest integration within the Microsoft 365 ecosystem. Systems based on open standards such as CalDAV and CardDAV cannot achieve the same integration quality within Outlook.

For older Outlook versions, third-party solutions such as "Outlook CalDav Synchronizer" — an open-source project with academic origins — provided workaround synchronisation capabilities. For the new Outlook client, no such integration is currently available.

[5] https://learn.microsoft.com/en-us/answers/questions/5643164/new-outlook-killed-pop-imap-microsoft-left-us-stra

Microsoft does not communicate the absence of CalDAV and CardDAV support as a deliberate rejection. The effect is the same regardless. Proprietary integration mechanisms are continuously developed and deepened. Open standard protocols receive no equivalent support within the dominant platform ecosystem. User requests for native CalDAV and CardDAV support have appeared on official Microsoft support and community platforms for many years, without any native implementation being announced.

Exchange ActiveSync (EAS) — Microsoft's proprietary protocol for mobile email and calendar synchronisation — illustrates a complementary pattern. EAS is a Microsoft-controlled and licensed protocol that much of the industry implemented to maintain compatibility with Exchange and Microsoft 365 environments. Outlook Mobile itself no longer uses EAS as its primary synchronisation architecture.

The structural asymmetry this creates is notable. Open standards are supported across the industry but not natively integrated within the dominant Outlook ecosystem. Microsoft's own proprietary protocols were adopted across large parts of the industry — and are now themselves being deprecated within modern Microsoft platform architecture.

The actual platform lock-in does not arise primarily from absent standardisation. It arises from the differential quality and depth of integration. Organisations face a practical incentive to use the fully integrated platform ecosystem to avoid operational friction and compatibility risk.

Interoperability formally exists. In practice, it has lost its equivalence.

4.4 Proprietary Extensions, APIs, and Migration-Induced Platform Dependency

A central pattern of asymmetric interoperability is not the outright rejection of open standards, but their selective implementation combined with proprietary extensions that create structural advantages within the dominant platform ecosystem. This pattern appears in document formats, communication protocols, calendar standards — and increasingly in the programmatic interfaces (APIs) that define access to platform data and services.

The documented example: EWS and Microsoft Graph

Exchange Web Services (EWS) was, from 2007 onwards, the central interface for programmatic access to Exchange mailboxes. Numerous third-party products — backup solutions, CRM systems, calendar clients, collaboration platforms — were built on this interface over many years.

In 2018, Microsoft ceased functional development of EWS. In 2023, the company announced that EWS would be fully deactivated in Exchange Online from October 2026. Its designated successor is the Microsoft Graph API.

Microsoft Graph is not a development of an open standard. It is a proprietary REST-based platform API under Microsoft's control — with its own authentication model, its own permission system, and platform-specific access concepts.

Microsoft documents that Graph, at the time of the announcement, did not have full functional parity with EWS. Certain functions will no longer be programmatically available in the same way after EWS is deactivated.

The structural consequence is both technical and economic. Third-party vendors who built their products over many years on a documented interface are required to migrate to a proprietary platform API within a fixed timeframe — with documented functional gaps and no standardised interoperable alternative.

The general pattern

EWS is not an isolated case. It is an expression of a general platform dynamic. Documented or open interfaces are progressively replaced by proprietary platform architectures. The migrations that result generate technical transition costs, organisational dependencies, and rising integration complexity.

Proprietary extensions now extend well beyond document formats and communication protocols. They encompass workflow logic, metadata, collaboration mechanisms, authentication models, and platform-specific integrations. The more complex digital work environments become, the harder it is for alternative vendors to replicate these integrations. The competitive disadvantage does not arise primarily at the level of standard implementation. It arises in the proprietary layer that surrounds the standard.

Interoperability formally persists. The structural asymmetry is built one layer above it.

4.5 "S3-Compatible" and Other Illusions of Switchability

The problem of asymmetric interoperability is particularly visible in so-called "compatible" platform services. A well-known example is the term "S3-compatible."

Amazon S3 — Simple Storage Service — has become the de facto standard for object-based cloud storage. Numerous European and international providers market their storage solutions as "S3-compatible" to signal interchangeability with existing cloud applications.

In practice, this compatibility frequently means only basic API functionality — not necessarily equivalence in permission models, metadata handling, performance, replication, security features, or workflow integration. In complex enterprise environments, even small differences can have significant operational consequences.

The result is a structurally distorted market. Alternative vendors appear formally compatible. The dominant platform is nonetheless perceived as the lower-risk reference implementation. Formal interoperability exists. Real switchability remains constrained.

Asymmetric interoperability is not a side effect of platform economics. It is one of its central operating mechanisms.

5 Collaboration Platforms as the New Dependency

5.1 From Document to Platform

Digital dependency in modern work environments no longer arises primarily at the level of individual document formats. Earlier lock-in effects were concentrated on files and proprietary formats. Platform power has since migrated to something more encompassing: integrated digital work ecosystems.

Documents are now just one component of complex collaboration platforms. Communication, calendars, identity, file storage, video conferencing, task management, permissions, and workflow systems are increasingly consolidated within unified platform environments.

The structure of digital dependency has shifted accordingly. What is at stake is no longer individual files. It is complete digital work processes.

Switching platform ecosystems therefore means migrating not just documents, but communication histories, collaboration structures, identity management, process logic, and organisational workflows. The switching costs this generates are not linear. They are cumulative — and they compound with every additional function the platform absorbs.

Figure 1: Evolution of digital Platforms

5.2 Teams, SharePoint, and Integrated Work Ecosystems

Modern collaboration platforms derive their strength primarily from deep integration. Systems such as Microsoft Teams, SharePoint, and comparable platform solutions bring together communication, file storage, rights management, meetings, collaboration, and workflow logic into a unified digital workspace.

Within such platforms, the user experience is consistent and highly integrated. Interoperability with external or alternative systems becomes correspondingly complex.

Documents are only one part of a much larger platform context. Permissions, comments, version histories, sharing configurations, meetings, automations, and AI functions are directly coupled to the platform ecosystem. The document cannot be cleanly separated from the environment in which it lives.

This creates a new form of digital dependency. The binding mechanism is no longer primarily the document format. It is the integrated work environment itself.

5.3 Workflow Lock-in

As digital work processes become more deeply integrated, the nature of lock-in shifts. Earlier dependencies were concentrated in proprietary file formats. Modern switching barriers arise increasingly at the level of workflows, integrations, automations, and collaboration logic.

The more deeply an organisation adapts its work processes to a particular platform ecosystem, the harder a subsequent switch becomes. This is especially true for automated processes, AI-powered workflows, integrated rights management, communication histories, and platform-specific extensions.

The core challenge is not migrating individual datasets. It is reconstructing functional organisational processes within a new system — processes that have been shaped, over time, by the affordances and constraints of a specific platform.

Lock-in is therefore increasingly semantic and organisational, not merely technical. The dependency is not in the file. It is in the way people have learned to work.

5.4 Identity, Communication, and Proprietary Integration

A critical component of modern platform ecosystems is the central integration of identity and communication. User accounts, access rights, group structures, calendars, chats, meetings, and collaboration functions are tightly interconnected.

The result is a highly integrated digital work environment whose value lies not in any individual application, but in the totality of its integrations. Individual

components can be replicated. The integrated whole cannot — at least not easily, and not without significant transition cost.

For alternative vendors, this creates a structural challenge that goes beyond feature parity. Even when individual functions are available through open standards or interoperable interfaces, full integration typically remains platform-specific. Alternative systems can provide basic functionality. They cannot replicate the integration depth and consistency of the dominant platform ecosystem.

Long-term dependencies arise precisely from this gap. They extend far beyond individual software products — into the organisational fabric of how institutions operate.

5.5 Why Switching Costs Rise Disproportionately

The economic value of modern platform ecosystems lies above all in their capacity to raise switching costs continuously.

Economic research shows that switching costs in platform markets rise disproportionately with integration depth.[6] With every additional integration, technical dependencies grow, organisational processes adapt, training requirements increase, data migrations become more complex, and procedural commitments deepen. Each integration, taken individually, appears manageable. Accumulated over years, they produce a platform ecosystem whose full migration becomes economically and organisationally unrealistic.

The compounding effect is the point. Organisations do not experience lock-in as a single decision. They experience it as a gradual narrowing of options — until the cost of switching exceeds any conceivable benefit.

At the same time, the complexity of interoperable alternatives rises. Even where individual components could technically be replaced, reconstructing comparable organisational processes in a new environment carries substantial risk. It is not the technology that is hardest to migrate. It is the institutional knowledge, the workflows, and the accumulated integration logic that has formed around the platform over time.

[6] Farrell, J. / Klemperer, P. (2007): Coordination and Lock-In: Competition with Switching Costs and Network Effects

Digital market power shifts accordingly — not through any single strategic move, but through the slow accumulation of integrations that each seemed reasonable at the time.

Under these conditions, interoperability is not merely a technical property of individual products. It is a precondition for digital markets that function at all.

6 The Blind Spot of the Digital Markets Act (DMA)

6.1 Objectives and Mechanisms of the DMA

With the Digital Markets Act, the European Union made its first serious attempt to address the structural market power of large digital platforms through regulation. The DMA aims to create fair competitive conditions in digital markets and to limit dependency on so-called "gatekeepers."

The regulation targets platform companies that, by virtue of their size, reach, and market position, occupy a central intermediary role between businesses and end users. Its purpose is to prevent dominant platforms from using that position to systematically constrain competition or structurally disadvantage alternative providers.

The DMA's central mechanisms include interoperability requirements, data portability obligations, restrictions on self-preferencing, and requirements to open certain interfaces to third parties.

The DMA represents an important regulatory shift in principle. Digital markets are no longer treated solely as spaces for innovation. They are increasingly recognised as infrastructural power structures — and regulated accordingly.

6.2 Gatekeeper Regulation and Its Limits

Despite its significance, the DMA has substantial structural limitations. The regulation is concentrated primarily on search engines, app stores, social networks, online advertising, and mobile platform ecosystems.

Digital work and collaboration platforms — precisely where long-term lock-in effects and high switching costs are generated — are far less comprehensively addressed.

The economic significance of modern office and collaboration ecosystems extends well beyond conventional software products. They have become the operational foundation of public administration, corporate knowledge work, internal communication, and organisational processes. Yet regulatory requirements regarding interoperable document formats, equivalent communication standards, workflow migration, or practical switchability between platform ecosystems remain limited.

The DMA addresses platform power in the consumer domain. The structural importance of digital work ecosystems has so far received only partial attention.

6.3 Why Work Standards Are Barely Addressed

A significant reason lies in the historical development of European platform regulation. Digital market power was long defined primarily through search engines, social networks, e-commerce, and mobile platforms. Document formats, collaboration platforms, and digital work processes were typically treated as conventional software markets — not as infrastructural power structures.

In practice, modern collaboration platforms have long since become central digital infrastructure. They govern communication, knowledge organisation, identity management, document flows, and organisational collaboration. The network effects this generates are particularly strong. Organisations do not orient themselves around individual applications. They orient themselves around complete work ecosystems.

The question of interoperable work standards has therefore become a central challenge for economic and competition policy — one that the current regulatory framework has not yet caught up with.

6.4 Platform Power in the Office, Not the App Store

The most significant digital dependency faced by European organisations today frequently does not arise in social media or mobile app stores. It arises within digital work environments.

Documents, meetings, chats, calendars, identity, permissions, and workflows are increasingly consolidated within integrated platform ecosystems. Platform power shifts accordingly — from individual applications to complete organisational work environments.

The switching costs of such systems are fundamentally different from those in conventional software markets. Organisations switching platforms are not replacing individual programmes. They are potentially replacing communication structures, document logic, process landscapes, identity models, and organisational knowledge systems — simultaneously.

This generates new forms of structural platform dependency that conventional competition metrics are poorly equipped to capture. Market share, pricing, and consumer choice tell only part of the story. The deeper question is how much it would actually cost — in time, risk, and operational disruption — to leave.

6.5 The DMA-Gatekeeper Question: Microsoft 365

The Digital Markets Act defines gatekeepers using quantitative thresholds — revenue, market capitalisation, and user numbers.

Microsoft services such as Teams and Outlook reach substantial levels of penetration within European businesses and public institutions. Microsoft Teams recorded over 320 million monthly active users globally in 2024,[7], with EMEA accounting for approximately 30 percent of that global user base.[8]

At the same time, the European Commission determined, within the DMA framework, that certain Microsoft services — despite meeting quantitative thresholds — do not automatically qualify as an "important gateway" within the meaning of the Act.[9]

The regulatory consequence is significant. Core components of modern work ecosystems are currently subject only to limited specific interoperability obligations under the DMA — precisely where structural switching costs and platform dependencies are most pronounced.

The actual market power of modern platforms is increasingly generated through integration depth, workflow dependency, identity management, API control, and asymmetric interoperability. This is the domain where long-term organisational lock-in is produced. It is also the domain that the DMA, in its current form, only partially reaches.

The regulation identifies the right problem. Its instruments were designed for a different map.

[7] *Microsoft Earnings Call Q3 FY2024*
[8] *Microsoft Annual Report FY2024*
[9] European Commission, Implementing Decision pursuant to Art. 3(4) DMA, Sept. 2023. https://digital-markets-act.ec.europa.eu/commission-designates-six-gatekeepers-under-digital-markets-act_en

6.6 Missing Regulatory Interoperability Mechanisms

The DMA contains individual interoperability requirements. It does not yet address the question of verifiable practical interoperability in complex work and collaboration systems.

What is currently absent is telling: standardised compliance tests, interoperable reference implementations, regulatory conformance checks, and binding criteria for practical switchability. The result is a regulatory gap. Standards can formally exist without anyone verifying whether their interoperable implementation actually works.

In highly concentrated platform markets, formal openness is not sufficient. Without verifiable conformance, structural lock-in effects, high switching costs, and long-term market asymmetries persist regardless. The central challenge of digital sovereignty is therefore not only the existence of open standards. It is their practical enforceability.

The DMA has begun to address digital platform power. The question of verifiable interoperability in digital work ecosystems remains largely unresolved.

6.7 The European Interoperability Framework

The European Union already possesses an important strategic foundation in the European Interoperability Framework (EIF). EIF defines fundamental principles of organisational, semantic, technical, and legal interoperability within European administrative structures. It addresses open standards, reusability, cross-border collaboration, and long-term digital sustainability.

The EU has therefore already recognised the strategic importance of interoperable digital systems in principle. The EIF matters. Its limitations, however, are equally clear.

The Framework is primarily advisory and conceptual in character. Binding technical conformance checks, interoperable reference implementations, and standardised compliance mechanisms for complex platform ecosystems are not yet its focus.

Modern collaboration and knowledge platforms generate structural dependencies that go well beyond classical administrative interoperability. Practical switchability in integrated work environments depends increasingly on

organisational workflows, platform APIs, semantic models, and AI-powered context systems. EIF provides an important strategic starting point. The question of verifiable practical interoperability in complex platform ecosystems remains only partially addressed.

6.8 The Data Act: Important Progress — But Not a Sufficient Answer to Modern Platform Dependency

With the Data Act, the European Union has taken a meaningful regulatory step towards reducing structural dependencies in digital markets. The Act addresses data portability, cloud switching, and technical barriers to switching between digital services. Providers are required not to artificially impede switching, to avoid excessive exit costs, and to provide standardised interfaces for data migration.

In the area of cloud infrastructure and platform services, this represents genuine progress. The measures are economically sound and necessary. They address primarily infrastructural and data-related dependencies. The actual switchability of modern digital work ecosystems extends considerably further.

Structural platform dependency in modern collaboration and knowledge systems arises not only from data holdings, but from integrated workflows, organisational process logic, permission models, automation mechanisms, platform-specific APIs, and semantic connections between different services. The transition to AI-powered work environments is accelerating this further.

Exporting files or data does not guarantee real organisational switchability.

This is most visible in modern workplace and collaboration platforms. Organisations increasingly integrate document management, communication, meetings, task management, identity management, and workflow automation within shared platform ecosystems. The productivity and integration benefits are real. So are the organisational switching costs.

The actual challenge is rarely the migration of individual datasets. It is the reconstruction of functional organisational processes within an alternative system. Documents can be exported. Automation processes, approval workflows, integrations, permission logic, and organisational context knowledge cannot automatically migrate with them — and frequently cannot be reconstructed without substantial loss.

The next phase of digital platform dependency is therefore increasingly semantic and organisational — not primarily a question of data or infrastructure.

The Data Act addresses this only partially. Data portability is a necessary precondition for digital sovereignty. It is not a sufficient condition for real switchability in complex work and knowledge platforms.

This is precisely why verifiable practical interoperability is becoming more important, not less. Digital sovereignty in the future will mean not only the ability to export data — but the ability to keep organisational work processes, semantic knowledge structures, and digital collaboration interoperable and migratable across platforms.

7 The Next Lock-in Wave: AI and Semantic Platforms

The observations in this chapter describe emerging developments based on current market trends. They do not claim to be exhaustive. Their purpose is to identify structural risks that are already visible today.

The current debate about digital sovereignty remains heavily focused on infrastructure: data centres, cloud platforms, networks, and data location. This perspective is increasingly insufficient.

Digital dependency is shifting — progressively and structurally — from infrastructure towards integrated knowledge, context, and AI systems.

Three levels of technological sovereignty capture this development. The first is digital infrastructure. The second is interaction with the physical world. The third, and strategically most significant, is data and knowledge.

The first phase of digital sovereignty was primarily about infrastructure. The strategically relevant dependencies of the future are forming one level higher — at the level of semantic knowledge and AI systems. Infrastructure can be replicated. Knowledge architecture, organisational context, and the models trained on years of institutional data are considerably harder to move.

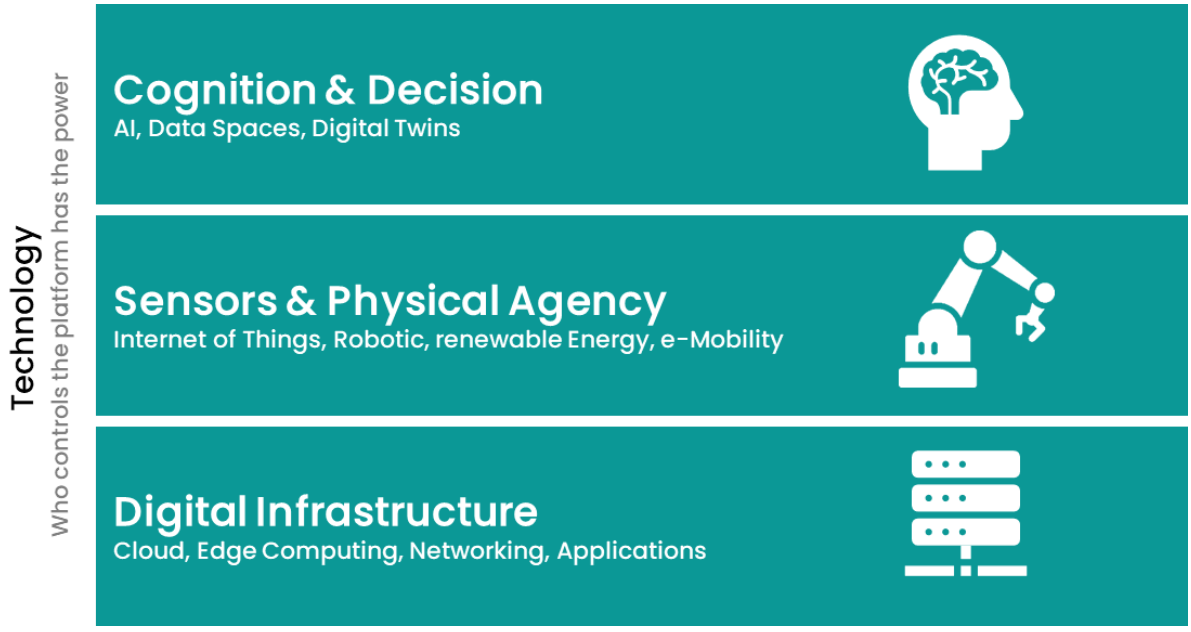

Figure 2: Levels of Digital Sovereignty and Technological Dependency

The importance of interoperable standards grows substantially as a result. Documents, communication systems, platforms, and APIs are no longer merely

technical work tools. They are increasingly the semantic foundation on which AI-powered systems are built.

7.1 From Documents to Knowledge Models

The next phase of digital platform dependency is no longer forming primarily at the level of individual documents or applications. It is forming at the level of semantic knowledge models and AI-powered work processes.

Earlier lock-in effects arose primarily from proprietary file formats and platform integrations. Digital dependency is now shifting towards knowledge structures, context models, semantic connections, AI-powered automation, and platform-bound data spaces.

Modern document formats are already far more than file formats. They have become the infrastructural foundation of digital knowledge work — and are developing into semantic carriers of organisational knowledge. Documents today contain not only content, but comments, metadata, version histories, approvals, collaboration information, and organisational context structures.

AI systems access precisely these structures. Content is no longer merely stored or exchanged. It is interpreted, prioritised, connected, and automatically processed by AI systems acting on the full depth of the platform's context.

A new form of digital dependency follows from this. What determines switchability is no longer simply access to data. It is control over the semantic interpretation of that data.

7.2 Proprietary AI Ecosystems

Modern AI systems derive their power increasingly from deep integration into existing platform ecosystems. AI assistants draw on documents, communication, calendars, meetings, permissions, knowledge bases, and organisational processes — connecting this information into contextual work models.[10]

The actual value of such systems arises less from individual AI models than from exclusive access to integrated data and workflow ecosystems. The model is the entry point. The platform context is the moat.

[10] Cortiñas-Lorenzo, Karina et al., "Through the Looking-Glass: Transparency Implications and Challenges in Enterprise AI Knowledge Systems", arXiv:2401.09410, January 2024.

The deeper AI functions become embedded in proprietary platforms, the harder it becomes to migrate organisational knowledge to alternative systems. Digital dependency is increasingly generated not through data formats, but through contextual knowledge, semantic connections, and platform-bound knowledge models.

Control over AI ecosystems is becoming a new form of infrastructural market power.

7.3 Agents and Semantic Dependencies

The development of autonomous AI agents intensifies this problem further. AI agents no longer interact only with individual documents. They interact with workflows, communication systems, organisational knowledge, and business processes — continuously and at scale.

New forms of semantic lock-in follow directly from this. Work logic, prioritisation schemes, context models, and organisational knowledge structures are progressively encoded within proprietary AI systems. With each cycle of interaction, the system learns more about how a specific organisation thinks and operates. That accumulated context has no standard export format.

Migration becomes considerably more complex than classical data migration. Even when data remains exportable, this does not mean that contextual knowledge, automations, semantic relationships, or organisational work logic can be migrated equivalently. What transfers is the content. What stays behind is the intelligence built around it.

Platform dependency is therefore increasingly located at the level of semantic models, organisational knowledge structures, and AI-powered decision logic — not at the level of files or databases. This is the dependency that current regulatory frameworks do not yet address. And it is the one that will matter most.

7.4 APIs as the New Standards

In the AI era, APIs — application programming interfaces — are becoming the actual standards of digital platform ecosystems. They define how AI systems

access data, how applications are integrated, how automations function, and which platform services can interact with one another.[11]:

Formally open APIs are increasingly insufficient to ensure real switchability. Proprietary extensions, platform-specific SDKs, semantic models, and non-standardised integrations generate new dependencies that extend well beyond classical file formats. This is particularly acute for AI agents, workflow automation, knowledge graphs, semantic search systems, and platform-integrated AI assistants.

Whoever controls the APIs increasingly controls the semantic infrastructure of digital work.

7.5 Risks for European Digital Sovereignty

The next phase of digital sovereignty will not be decided by cloud infrastructure, data centres, or data location alone. The decisive question is whether knowledge models, AI-powered work processes, semantic integrations, and organisational context systems remain interoperable and migratable over time.

The challenges already visible today in document formats, APIs, and collaboration platforms risk becoming significantly more severe in the domain of AI and semantic platforms. The patterns are the same. The stakes are higher.

Missing interoperability in AI systems generates rising organisational dependencies, long-term platform binding, constrained switchability, and new concentration effects in digital markets. The window for establishing standards before these dependencies calcify is open — but it will not remain open indefinitely.

Digital sovereignty under these conditions means not only control over data. It means control over semantic structures, organisational knowledge, and AI-powered work processes. Europe has learned — slowly and at considerable cost — what dependency on proprietary document formats and cloud infrastructure looks like. The AI layer is being built now. The decisions made today will determine whether that layer is open or closed.

[11] Sharma, Rishi et al., „Collaborative Agentic AI Needs Interoperability Across Ecosystems", arXiv:2505.21550, May 2025"

8 Why Open Standards Alone Are Not Enough

The preceding chapters have demonstrated through concrete examples that formal standardisation is not a sufficient condition for practical interoperability. This chapter draws together the structural patterns.

8.1 The Problem of Purely Formal Standardisation

OOXML has been an ISO standard since 2008. Microsoft nonetheless implemented not the approved Strict variant, but the rejected Transitional variant (see Chapter 3.3). CalDAV and CardDAV have been IETF standards for over twenty years. Outlook does not support them natively to this day (see Chapter 4.3). IMAP has been RFC-standardised since 1988. In the new Outlook, it is functionally degraded (see Chapter 4.2).

The pattern is consistent. Formal standardisation does not guarantee real switchability. Standards only produce their market effects when implementation is consistent and interoperable behaviour is verifiable. Without that, a standard is a specification — not a guarantee.

8.2 Absent Compliance Verification

Exchange Web Services (EWS) was a documented interface. Third-party vendors built on it for years. In 2026 it will be deactivated — its successor, Microsoft Graph, is a proprietary API with no standardised alternative (see Chapter 4.4). No one has verified whether this transition meets the interoperability requirements of the DMA — because Microsoft 365 is not subject to DMA interoperability obligations (see Chapter 6.4).

Compliance verification is absent not only technically. It is absent regulatorily.

8.3 Absent Reference Implementations

OOXML Strict exists as a specification. A binding reference implementation demonstrating how Strict should correctly be implemented does not exist. The result: dominant market implementations define the standard in practice (see Chapter 3.3). The same applies to S3-compatible storage services — "compatible" without a reference benchmark is meaningless (see Chapter 4.5).

A standard without a reference implementation is an aspiration. The market fills the gap — and the market leader fills it first.

8.4 Absent Migration Capability

Interoperability is frequently reduced to data export. Actual switchability encompasses workflows, permissions, metadata, communication histories, and organisational context information (see Chapters 5.3, 5.4, 5.5). In AI-powered systems, the next generation of dependencies is forming at the semantic level — not the file level (see Chapter 7). Exporting data is the beginning of migration. It is not migration.

8.5 Open Washing and Pseudo-Compatibility

The documented examples reveal a consistent pattern. Platforms market themselves as open — OOXML as an "open standard," EWS as a "documented interface," S3 as a "compatible protocol" — without this producing equivalent usability or real switchability.

This is not necessarily the product of bad intent. It is the structural outcome of a market without verifiable conformance mechanisms. When openness cannot be tested, it cannot be trusted. And when it cannot be trusted, it functions as marketing — not as infrastructure.

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

9 Proposal: European Interoperability Certification

9.1 Core Idea and Objectives

The preceding chapters identify a structural problem in digital markets: open standards alone are not sufficient to ensure real switchability and functioning competition. What matters is not only the existence of a standard, but its verifiable, interoperable implementation in practice.

This is precisely where a European interoperability certification scheme would intervene.

The goal of such a system would not be to regulate technological innovation, disadvantage particular platforms, or achieve technological self-sufficiency. The goal would be verifiable market transparency: which systems actually implement standards interoperably, which platforms enable genuine switchability, and which solutions generate long-term structural dependencies.

A European interoperability certification would fulfil a function analogous to technical certification in traditional industries. It would not prevent innovation. It would create trust, switchability, and market transparency.

9.2 An Independent European Certification Body

A credible interoperability certification system requires an independent European governance and assessment framework — not to favour particular technologies or vendors, but to ensure objective verification of practical interoperability based on transparent technical criteria.

An appropriate model would be a decentralised network of nationally accredited testing bodies operating under a shared European framework — comparable to existing conformity and certification systems in other industrial sectors.

Europe already possesses the institutional infrastructure to make this possible. National standards and certification organisations — Austrian Standards, DIN in Germany, AFNOR in France — could serve as organisational foundations. European standardisation bodies CEN and CENELEC, specialised agencies such as ENISA in cybersecurity certification, and existing national IT certification bodies such as Germany's BSI are all relevant starting points.

No entirely new institutional system would need to be created. A European interoperability certification framework could be built on existing standardisation, testing, and accreditation structures.

What would be decisive is institutional independence. Certification must be transparent, traceable, reproducible, and vendor-neutral. Only under these conditions can the necessary trust be established — among businesses, public institutions, and alternative vendors alike.

9.3 Technical Compliance Tests

The core of an interoperability certification would be standardised technical compliance tests. The question is not merely whether a standard has formally been implemented, but whether different systems actually work interoperably in practice.

Such tests could verify consistent document rendering, lossless migration, interoperable calendar and contact synchronisation, API compatibility, workflow behaviour, permission models, and cross-platform collaboration functions.

The practical user perspective is particularly important here. Interoperability must hold not only in theory, but in real-world deployment. In complex platform ecosystems, specification conformance alone is frequently insufficient to ensure real switchability.

9.4 Reference Implementations and Test Suites

Technical standards require verifiable reference models. A European interoperability certification should therefore be complemented by open reference implementations, standardised test suites, and publicly documented conformance criteria.

The objective is to reduce interpretive discretion and asymmetric implementations. In the areas of document formats, APIs, collaboration platforms, and AI-powered workflow systems, such reference models could make a substantial contribution to practical interoperability.

One clarification is important. The reference implementation would not itself become a mandatory market standard. It would serve as an objective technical benchmark — a measuring stick, not a mandate. This would help avoid the

situation that currently prevails, in which dominant market implementations effectively become the reference standard by default.

9.5 Certification Levels, Enforcement, and Financing

Not all forms of interoperability have the same maturity. A tiered certification model is therefore appropriate.

Level 1 — Standard Support The platform formally supports an open standard and documents its implementation transparently. This does not yet guarantee full practical switchability, but creates market transparency as the basis for informed procurement and architecture decisions.

Level 2 — Full Interoperability The platform demonstrates that core functions work interoperably and consistently with other certified systems — including document rendering, synchronisation, metadata, collaboration functions, and cross-platform behaviour.

Level 3 — Lossless Migration The highest certification level confirms that data, documents, metadata, workflows, and organisational context information can be practically migrated without material loss of function or information. This capability is becoming increasingly relevant in integrated collaboration platforms, AI-powered work environments, and semantic knowledge systems.

Enforcement and Economic Relevance

Certification levels only produce effects when they become economically and regulatorily relevant. Three mechanisms are particularly suitable.

Public procurement: contracting procedures for public institutions could progressively define minimum interoperability requirements — Level 1 for general workplace systems, Level 2 for systems with long-term archiving obligations or critical infrastructure status. This follows the established principle of technical conformance verification in other industrial sectors: not the vendor is regulated, but the interoperable property of the product is transparently demonstrated.

Integration with existing DMA mechanisms: for platforms with significant market power, interoperability certification could be progressively linked with existing regulatory instruments under the Digital Markets Act — particularly where platform ecosystems generate substantial switching costs, organisational

dependencies, or structural market advantages through asymmetric interoperability.

Transparency obligation: providers of digital workplace, collaboration, and platform solutions could be required to disclose their interoperability status publicly. Absence of certification would not be a prohibition on sale — but would create market transparency regarding migration capability, standard conformance, and practical switchability.

Financing

The certification system should be financed primarily through certification fees — consistent with existing conformity and testing procedures in other industrial sectors. It is important that interoperability certification does not itself become a market entry barrier. Reduced fee models should therefore be available for open-source projects, small and medium-sized providers, and public-interest digital infrastructure projects. The development of open test suites, reference implementations, and interoperable testing tools could be co-financed through European research and innovation programmes.

Timeline

The concrete implementation timeline is a matter for political agreement between the European Commission, member states, and standards organisations. As an indicative framework, the following phasing appears realistic: Phase 1 (years 1–2): establishment of the certification framework, development of open test suites, and pilot operation with voluntary certification. Phase 2 (years 3–4): binding Level 1 procurement requirement for public authorities. Phase 3 (from year 5): binding Level 2 requirement for security-critical and archiving-obligated systems, and linkage with DMA mechanisms for dominant platform providers.

9.6 Interoperability as Market Transparency

A European interoperability certification would not only make technical quality visible. Above all, it would create structural market transparency. Businesses and public institutions would be better placed to assess which platforms enable real switchability, which systems generate long-term dependencies, and which solutions remain interoperable and migratable.

Interoperability would shift from an unverifiable technical detail to a visible competitive attribute. That is the core economic policy significance of such a system — not regulation for its own sake, but the creation of transparent preconditions for digital markets that actually function.

9.7 Proportionality, Openness, and Low Entry Barriers

A European interoperability certification can only fulfil its economic policy purpose if it does not itself create new market entry barriers.

Certification procedures must therefore be transparent, reproducible, modular, and — as far as possible — automatable. A highly complex or cost-intensive certification system would be particularly problematic for small and medium-sized European vendors. Interoperability regulation must not inadvertently further concentrate markets that are already concentrated.

Dominant platform providers possess substantial organisational and financial resources to manage complex compliance and certification processes. Small vendors, open-source projects, and European specialist providers frequently do not. A functioning certification model must therefore deliberately keep entry barriers low.

This means open and publicly documented test suites, standardised reference tests, reproducible assessment procedures, modular certification components, and largely automatable conformance checks. Certifications should not rely exclusively on resource-intensive individual assessments, but should be built as far as possible on open technical tests, standardised validation procedures, and transparent conformance criteria.

A tiered approach is appropriate here too. Simple standard implementations should be certifiable with minimal effort. Complex platform ecosystems should be required to provide correspondingly comprehensive interoperability evidence.

The critical point bears repeating. The actual reference must not be defined by dominant market implementations. It must be defined by open, traceable, and reproducible technical criteria.

Interoperability certification must not itself become a lock-in. Its purpose is to lower switching barriers — not to create new regulatory dependencies.

10 Public Procurement as a Strategic Lever

10.1 The Public Sector as Market Shaper

The public sector is among the largest purchasers of digital technology in Europe. Public administrations, educational institutions, health systems, and state-adjacent organisations invest billions annually in software, cloud services, collaboration platforms, and digital infrastructure.

Procurement is therefore not merely an operational administrative function. It is a central instrument of economic policy. Public tenders influence technological standards, market structures, innovation dynamics, and long-term platform dependencies.

In the digital domain, the structural effects are substantial. When public institutions procure platform ecosystems with limited interoperability or migration capability, they reinforce existing lock-in structures — at public expense, and with consequences that extend across decades.

Digital sovereignty is therefore not only a question of technological development. It is a question of strategic procurement policy.

10.2 Certification as a Procurement Prerequisite

Interoperability only produces its effects when it becomes economically relevant. This is precisely where public procurement can play a decisive role.

A European interoperability certification could be progressively established as an objective evaluation criterion in public tenders. The goal would not be to exclude particular vendors, but to create transparent requirements for switchability, data migration, standard conformance, and practical interoperability.

For the first time, interoperability would become a measurable competitive factor.

This is particularly relevant in areas with long-term dependencies: document management, collaboration platforms, cloud services, communication systems, and AI-powered work environments. Procurement decisions would no longer evaluate only short-term functionality — they would also assess long-term digital resilience and migration capability.

10.3 Promoting Competition and Innovation

Interoperability strengthens competition. When switching costs fall and platforms remain practically exchangeable, market entry barriers are lower, innovation space expands, and competition between different vendors increases.

European vendors stand to benefit significantly. Today, many digital markets impose structural disadvantages through dominant platform ecosystems, proprietary integrations, and asymmetric interoperability. Small and medium-sized providers must frequently not only implement open standards, but additionally reverse-engineer the behaviour of dominant platforms to remain competitive.

Binding interoperable standards and verifiable conformance mechanisms could reduce these structural disadvantages. Interoperability would not become an obstacle to innovation. It would become a precondition for innovation markets that actually function.

10.4 Opportunities for European Vendors

Europe has a substantial base of capable vendors in cloud infrastructure, open-source software, collaboration platforms, security solutions, and digital administration systems. Many of these providers do not fail because of insufficient technical quality. They fail because of the high switching costs of incumbent platform ecosystems, asymmetric interoperability, and the absence of practical exchangeability.

An interoperability-oriented procurement framework could create new market opportunities. Public institutions would not primarily favour particular technologies — they would favour systems that implement open standards with practical interoperability, enable real switchability, and reduce long-term platform dependencies.

European vendors could compete more on quality, security, innovation, and service — rather than primarily against the structural entrenchment of incumbent lock-in.

10.5 Long-Term Archiving and Sustainability

Public procurement does not only concern current product decisions. It concerns digital infrastructures with lifespans measured in decades.

Documents, administrative data, scientific information, and organisational knowledge must remain readable, migratable, and usable independently of individual platform ecosystems over the long term. Missing interoperability creates substantial risks: rising migration costs, long-term vendor dependencies, loss of semantic information, and constrained archiving capability.

In the public sector, this creates a structural tension between short-term functionality and long-term digital resilience. Under these conditions, interoperability becomes a question of sustainable state infrastructure policy.

The public sector therefore has not only the opportunity, but the responsibility, to actively promote interoperable and migratable digital systems. Public procurement can become a central instrument for structurally strengthening competition, digital sovereignty, and long-term technological resilience.

Procurement is policy. Nowhere is this more consequential than in the digital infrastructure of democratic institutions.

11 Policy Recommendations

The preceding chapters have shown that digital sovereignty cannot be achieved through European infrastructure or formal standardisation alone. What is decisive is whether digital systems remain interoperable, migratable, and practically switchable over the long term.

The concrete proposals are set out in Chapters 9 and 10. This chapter directs the central recommendations explicitly at the relevant audiences.

A note on terminology

Microsoft Office is the most widely used office software suite in European businesses and public institutions — comprising Word, Excel, PowerPoint, and Outlook. It is sold both as a perpetual licence (Microsoft Office 2024) and as a cloud subscription under the designation Microsoft 365, with or without the AI extension Copilot. The market power of Microsoft Office exists independently of the licensing model and independently of product rebranding. In the context of this paper, "Microsoft Office" refers to the product in all its distribution forms.

Microsoft Office dominates the market for office software in European businesses and public institutions, with an estimated market share of approximately 80–85 percent.[12] Google Workspace follows at a substantial distance. All remaining providers — including LibreOffice, OnlyOffice, and other European solutions — share what remains.

Market shares of 80 percent or more are not automatically problematic. They become economically relevant where high switching costs, network effects, and asymmetric interoperability structurally constrain competition.

Functioning markets require real switchability. When platform ecosystems become practically non-exchangeable through proprietary integrations, workflow dependencies, and semantic lock-in, competition loses its disciplining effect.

[12] Nielsen Company, Office Report 2020: Microsoft Office market share in German companies (50–50,000 employees): 85%. Source: Statista, https://de.statista.com/statistik/daten/studie/77226/ — Confirmed by Intra2net SME Study, September 2024 (>80% among German SMEs). Global: >75% (24 Market Reports, 2024). Austria and Germany have structurally comparable enterprise IT markets; a current Austria-specific primary survey is not available.

11.1 To the European Commission

Extend the Digital Markets Act to include binding interoperability requirements for digital work and collaboration platforms — in particular for document formats, calendar and contact protocols, programmatic interfaces, and interoperability between services; for cloud infrastructure standards and APIs, particularly where proprietary interfaces have become de facto market standards without a regulatory basis; and for AI platform ecosystems and semantic knowledge systems, particularly where proprietary AI agents and knowledge models are generating new forms of migration-induced platform dependency.

Assess whether Microsoft Office — distributed both as a perpetual licence and as a cloud subscription under the designation Microsoft 365 — should be designated as a gatekeeper under the DMA. Microsoft Office meets the quantitative thresholds of Article 3(2) DMA. The structural lock-in effects through asymmetric interoperability — documented in Chapter 4 of this paper — correspond to the regulatory purpose the DMA was designed to serve.

Assess the gatekeeper designation for further platforms that meet quantitative DMA thresholds but have not yet been designated — particularly where de facto standards have emerged without a regulatory basis, or where migration-induced platform dependency structurally prevents switchability.

Commission ENISA and CEN/CENELEC to develop a European interoperability certification framework, building on existing standardisation and accreditation structures.

Introduce a binding transparency obligation for providers of digital workplace and collaboration solutions regarding their interoperability status — as the basis for informed procurement decisions by public and private institutions.

11.2 To the Government of the EU Member States

Introduce interoperability certification as a procurement prerequisite for public tenders of digital workplace and collaboration systems — beginning incrementally with Level 1 certification.

Commission national standardization organisations like Austrian Standards International or Deutsches Institut für Normung (DIN) to develop a national pilot programme for interoperability certification — as the foundation for a scalable European certification framework.

Fund open reference implementations and test suites within national digital programmes — in particular for IMAP, CalDAV, CardDAV, ODF, and OOXML Strict.

Actively advance the topic of verifiable interoperability within European digital policy — including through the Interoperable Europe Act and European procurement reform.

11.3 To Standards and Standardisation Organisations

Develop standardised compliance tests for open protocols — IMAP, CalDAV, CardDAV, ODF, OOXML Strict — as publicly accessible test suites.

Establish a European network of accredited interoperability testing bodies under a shared framework — consistent with existing conformity assessment systems.

Actively participate in the further development of the Interoperable Europe Act and in European standardisation processes for digital workplace and collaboration systems.

Develop a tiered certification model with low entry barriers — in particular for open-source projects and small providers.

11.4 To Civil Society and Academia

Systematically document and publish interoperability deficiencies in real work environments — as the evidential basis for evidence-based regulation.

Build open test suites and reference implementations as digital commons — funded through European research and innovation programmes such as Horizon Europe.

Provide independent academic oversight of the certification process — to ensure technical neutrality and vendor independence.

12 Conclusion

Europe's debate about digital sovereignty has in recent years concentrated on infrastructure, cloud platforms, data protection, and geopolitical dependencies. This perspective remains important. It is no longer sufficient.

Digital dependency today increasingly arises not at the level of data centres or data locations, but within digital work and knowledge ecosystems — in document formats, APIs, collaboration platforms, workflow systems, and semantic AI structures. It is precisely there that the question is decided: whether digital systems remain interoperable, migratable, and practically switchable over the long term.

The central finding of this paper is therefore this:

Open standards alone are not enough.

Standards only produce their economic and social effects when their implementation remains interoperable, their conformance is verifiable, and real switchability between platforms remains possible. Where practical interoperability is absent, high switching costs, structural lock-in effects, and long-term market concentration emerge regardless of formal openness. The result is a gradual shift of digital power — away from open markets, towards integrated platform ecosystems.

This development becomes especially critical in the age of AI-powered knowledge systems. The next generation of digital dependency is forming not over documents or data formats, but increasingly over semantic models, organisational knowledge, APIs, AI agents, and platform-bound context systems. The lock-in of tomorrow is being built today — in the layer that regulators have not yet reached.

Digital sovereignty under these conditions means not only control over infrastructure or data location. It means, increasingly, the practical ability to switch digital systems. Interoperability is therefore a central precondition for functioning digital markets, technological resilience, long-term innovation capacity, and European strategic autonomy.

Europe has the opportunity to develop an independent regulatory and technological path in this area. The Digital Markets Act has begun to address

structural platform power. The question of verifiable interoperability in digital work and knowledge ecosystems remains largely unresolved.

This paper therefore proposes to verify interoperable standards more rigorously in practice, to establish European certification models, to fund open reference implementations, and to integrate interoperability systematically into public procurement.

The goal is not to constrain technological innovation. On the contrary: open and verifiably interoperable systems create the foundation for competition, innovation, market diversity, and long-term digital resilience.

Interoperability is not a technical footnote. It is becoming one of the central industrial, economic, and social policy challenges of digital societies.

The decisive question going forward is no longer simply:

"Are standards open?"

It is:

"Do they enable real digital freedom?"

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

I. Annex: About the Author

Werner Illsinger, is founder and Executive Director of the 4future.institute.

His career spans the full arc of modern IT — from 1987 to 2020, across three institutions that represent three distinct phases of the industry's development.

At debis — the IT services arm of Daimler-Benz — he worked on personal computers and networks in the early years of enterprise computing, and on mainframe development when large-scale infrastructure still meant something built and owned on-premise. At Microsoft, he progressed from Systems Engineer to Global Business Manager — moving from technical implementation to the strategic centre of the company that shaped how the world works with software. He was present for the OOXML standardisation process of 2008: not as an observer, but as an insider.

At Raiffeisen, one of Austria's largest banking groups, he led IT consulting at board level. There he sat on the other side of the table — managing the structural dependencies between a major European institution and its dominant technology suppliers: Microsoft, IBM, Oracle. The leverage those vendors carried, the switching costs they generated, and the decisions that were shaped by the practical impossibility of leaving: these are not abstractions in this paper. They are things Werner Illsinger had to navigate.

This paper is not commissioned work. It is the result of a growing conviction — formed across three decades and three sides of the same industry — that Europe must shape the structural conditions of its digital future now, while the window is still open.

II. Annex: Glossary

API (Application Programming Interface) An API is a standardised interface through which different software systems can communicate. APIs define how applications exchange data or use functions from other systems. In the context of digital platform economics, APIs are increasingly becoming strategic control points within digital ecosystems.

Asymmetric Interoperability Asymmetric interoperability describes a situation in which systems broadly work together, but not equivalently. The dominant platform typically offers the greatest functional scope, the deepest integration, the most consistent user experience, and the lowest risk. Alternative vendors remain formally compatible but frequently carry higher interoperability and reputational risks.

Switchability Switchability denotes the practical ability to change digital systems or platforms without disproportionate technical, economic, or organisational barriers. Switchability encompasses more than data export capability. What matters is whether documents, workflows, metadata, organisational processes, and semantic structures remain practically migratable.

CalDAV CalDAV is an open standard for synchronising calendar data between different systems. It enables shared calendars, scheduling, invitations, and cross-platform synchronisation.

CardDAV CardDAV is an open standard for synchronising contact and address book data. It enables the interoperable exchange of contact information between different platforms and applications.

Compliance Test A compliance test verifies whether a technical standard has actually been implemented correctly and interoperably. In contrast to formal standard support, a compliance test evaluates the practical behaviour of a system.

Data Portability Data portability denotes the ability to export data from one system and transfer it to another. Data portability alone does not guarantee complete switchability or interoperability.

De Facto Standard A de facto standard is a standard that has become established in practice through market adoption, regardless of whether it has

been formally standardised. Dominant platform implementations frequently develop into de facto standards.

Digital Markets Act (DMA) The Digital Markets Act is a European regulation designed to limit the structural market power of large digital platform providers ("gatekeepers"). The DMA includes requirements relating to interoperability, data portability, platform openness, and competitive conduct.

Digital Sovereignty Digital sovereignty denotes the ability of states, organisations, and individuals to use digital technologies independently, controllably, and with sustained capacity for action. This encompasses control over infrastructure, data governance, switchability of digital systems, interoperability, and technological resilience.

Gatekeeper Gatekeepers are particularly large digital platform providers with structural market power. The term is used specifically in the Digital Markets Act. Gatekeepers frequently control central digital access points or platform ecosystems.

IMAP (Internet Message Access Protocol) IMAP is an open standard for accessing email mailboxes. It enables synchronisation of emails between different devices and mail servers.

Interoperability Interoperability denotes the ability of different systems, applications, or platforms to work together consistently and interchangeably. Practical interoperability means not merely basic functional compatibility, but equivalent behaviour in real-world deployment.

ISO Standard An ISO standard is an internationally standardised technical norm of the International Organization for Standardization. ISO standards define common technical specifications and are intended to promote interoperability and switchability.

AI Agent An AI agent is a software-based system capable of executing tasks, preparing decisions, or managing work processes autonomously or semi-autonomously. AI agents frequently access documents, APIs, communication systems, calendars, and knowledge models.

Collaboration Platform A collaboration platform is an integrated digital work environment for communication, document editing, meetings, workflow

management, task management, and teamwork. Examples include Microsoft Teams, SharePoint, and comparable work ecosystems.

Lock-in Effect A lock-in effect describes a situation in which switching systems or platform vendors involves high technical, organisational, or economic costs. Lock-in typically arises through proprietary extensions, absent interoperability, workflow dependencies, or network effects.

Metadata Metadata is structured supplementary information about data or documents — including author information, version histories, approvals, timestamps, and permissions.

Network Effect A network effect arises when the value of a system increases with the number of its users. Digital platform markets frequently exhibit strong network effects.

ODF (OpenDocument Format) ODF is an open and ISO-standardised document format for text documents, spreadsheets, and presentations. ODF was developed to enable long-term vendor independence and interoperable document formats.

OOXML (Office Open XML) OOXML is an XML-based document standard for office documents, developed by Microsoft and standardised as ISO/IEC 29500 in 2008. The standard exists in two variants: "Strict" and "Transitional."

Platform Economics Platform economics describes digital markets in which platform providers act as central intermediaries between different market participants. Platforms typically benefit from network effects, integration advantages, data aggregation, and lock-in effects.

Proprietary Extension A proprietary extension supplements an open standard with additional functions that are only fully supported within a particular platform ecosystem. This allows formal openness to persist while practical switchability is constrained.

Reference Implementation A reference implementation is a technical realisation of a standard that serves as an objective benchmark. Reference implementations help reduce interpretive discretion, enable interoperability testing, and make conformance verifiable.

S3 (Simple Storage Service) S3 is a cloud storage service for object-based data developed by Amazon. The S3 API has become the de facto standard for object-based cloud storage solutions. Many providers therefore market their services as "S3-compatible."

Semantic Platform A semantic platform processes not only data, but interprets its meaning, context, and relationships. Such platforms play a central role in AI-powered knowledge systems.

Standard A standard defines common technical rules or specifications to enable interoperability, switchability, and compatibility between different systems.

Standardisation Standardisation denotes the process of defining and harmonising technical rules or formats. Standardisation alone does not guarantee practical interoperability.

Workflow Lock-in Workflow lock-in describes a form of digital dependency in which organisational processes, automations, and process logic are tightly bound to a particular platform ecosystem. The actual switching barrier arises less from data formats than from integrated work processes.

III. Annex: References

Primary Sources, Regulation, and Standards

Digital Markets Act (DMA) — Regulation (EU) 2022/1925 Data Act — Regulation (EU) 2023/2854 NIS2 Directive — Directive (EU) 2022/2555 European Interoperability Framework (EIF) Interoperable Europe Act EU Artificial Intelligence Act European Data Strategy ISO/IEC 26300 — OpenDocument Format (ODF) ISO/IEC 29500 — Office Open XML (OOXML)

RFC 3501 — Internet Message Access Protocol (IMAP) RFC 4791 — Calendaring Extensions to WebDAV (CalDAV) RFC 6352 — CardDAV: vCard Extensions to WebDAV

W3C — Standards Overview NIST Cloud Computing Standards Roadmap

Academic Literature and Platform Economics

Shapiro, Carl / Varian, Hal R. (1999): *Information Rules: A Strategic Guide to the Network Economy.* Harvard Business School Press. Parker, Geoffrey / Van Alstyne, Marshall / Choudary, Sangeet Paul (2016): *Platform Revolution.* W. W. Norton & Company. Wu, Tim (2010): *The Master Switch: The Rise and Fall of Information Empires.* Knopf. Zuboff, Shoshana (2019): *The Age of Surveillance Capitalism.* PublicAffairs. Brynjolfsson, Erik / McAfee, Andrew (2017): *Machine, Platform, Crowd.* W. W. Norton & Company. Lessig, Lawrence (2006): *Code: Version 2.0.* Basic Books. Benkler, Yochai (2006): *The Wealth of Networks.* Yale University Press. Farrell, Joseph / Klemperer, Paul (2007): "Coordination and Lock-In: Competition with Switching Costs and Network Effects." In: *Handbook of Industrial Organization.* Arthur, W. Brian (1989): "Competing Technologies, Increasing Returns, and Lock-In by Historical Events." *Economic Journal.* Rochet, Jean-Charles / Tirole, Jean (2003): "Platform Competition in Two-Sided Markets." *Journal of the European Economic Association.*

Document Standards and Interoperability

Weir, Rob — Technical articles and analyses on ODF, OOXML, and interoperability. Updegrove, Andrew — Analyses of open standards, ISO processes, and interoperability. Brown, Alex — Analyses and documentation of the OOXML standardisation process. OpenForum Europe — Open Standards Position Papers. Document Foundation — Interoperability and Open Standards. Open Source

Observatory (OSOR). Microsoft Graph Documentation. Exchange Web Services (EWS) Deprecation Documentation.

Platforms and Semantic Systems

Human-AI Collaboration in Knowledge Ecosystems: A Multidisciplinary Review, Integrative Framework and Future Directions. Sharma, Rishi et al. (2025): "Collaborative Agentic AI Needs Interoperability Across Ecosystems." arXiv:2505.21550. Cortiñas-Lorenzo, Karina et al. (2024): "Through the Looking-Glass: Transparency Implications and Challenges in Enterprise AI Knowledge Systems." arXiv:2401.09410. Towards an Interoperable Ecosystem of AI and Language Technology Platforms. OECD AI Principles. European AI Act.

Digital Sovereignty, Resilience, and Geopolitical Dependencies

Bria, Francesca — Publications and lectures on digital sovereignty and platform economics. Gaia-X Initiative. European Digital Sovereignty — Bertelsmann Stiftung. Fraunhofer ISI — Studies on digital sovereignty and European technology policy. The European Correspondent — "Trump's Power Switch." Euronews — Analyses of geopolitical risks of digital infrastructure dependency. Illsinger, Werner (2025): *Digital Sovereignty in Europe.* 4future.institute. https://4future.institute/2025/11/18/digitale-souveraenitaet-in-europa/

Public Procurement and Open Source Governance

European Commission — Public Procurement Strategy. European Commission — Open Source Software Strategy 2020–2023. Open Source Procurement Toolkit — OSOR. Interoperable Europe Portal.

Society. Economy. Technology. Sustainability.

The future emerges from balance and deliberate design.

The 4future.institute is a clearly defined and independent unit within 4future.business GmbH. The majority shareholder is the 4future.foundation.

Independence is the prerequisite for our work — not its outcome.

4future.institute | Graben 17/10 | 1010 Vienna | +43 1 31440-0 | hello@4future.institute