



D1.2 BRIEF ON DIGITAL COMMONS PRIORITIES: THE BUILDING BLOCKS

A DIGITAL COMMONS-BASED APPROACH FOR
PROVISIONING EUROPE'S DIGITAL INFRASTRUCTURE

Revision: v.1.0.

Work package	WP1
Task	Task 1.2
Due date	31/07/2025
Submission date	30/07/2025
Deliverable lead	OpenForum Europe (OFE)
Version	1.0
Authors	Nicholas Gates
Reviewers	Adrienn Lawson, Paula Grzegorzewska, and Mirko Boehm [LF], Aditya Singh and Zuzanna Warso [OF]

Abstract	This document presents potential Digital Commons-based Building Blocks in a concise way, representing the priority areas that need the most support and attention to work towards EU's digital sovereignty. It takes into account global nomenclature and frameworks, such as DPGs and SDGs, to develop its own framework for identifying potential Building Blocks and incorporating them into the planned Open Internet Stack. The deliverable led by T1.2, with input from T1.1 and contributing to D1.4.
Keywords	Digital Commons, Building Blocks, Open Internet Stack, Digital Sovereignty, Sovereign Digital Infrastructure

commons.ngi.eu



Grant Agreement No.: 101135279
Type of action: HORIZON Coordination and Support Actions

Topic: HORIZON-CL4-2023-HUMAN-01-14
Call: HORIZON-CL4-2023-HUMAN-01-CNECT

DISCLAIMER



Funded by
the European Union

Project funded by



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI

NGI Commons (*Open Source and Internet Commons for Europe's Digital Sovereignty*) project is funded by the European Union's **Horizon Europe research and innovation programme** under Grant Agreement number 101120640. This work has received funding from the **Swiss State Secretariat for Education, Research, and Innovation (SERI)**.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

COPYRIGHT NOTICE

© 2024 - 2026 NGI Commons Consortium

Project funded by the EC in the Horizon Europe Programme		
Nature of the deliverable:	R*	
Dissemination Level		
PU	Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page)	✓
SEN	Sensitive, limited under the conditions of the Grant Agreement	
Classified R-UE/ EU-R	EU RESTRICTED under the Commission Decision No2015/ 444	
Classified C-UE/ EU-C	EU CONFIDENTIAL under the Commission Decision No2015/ 444	
Classified S-UE/ EU-S	EU SECRET under the Commission Decision No2015/ 444	

* R: Document, report (excluding the periodic and final reports)

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

DATA: Data sets, microdata, etc.

DMP: Data management plan

ETHICS: Deliverables related to ethics issues.

SECURITY: Deliverables related to security issues

OTHER: Software, technical diagram, algorithms, models, etc.



Funded by
the European Union

EXECUTIVE SUMMARY

As the European Union (EU) enters a new institutional cycle, digital sovereignty has become a defining principle guiding both European Commission (EC) and European Parliament (EP) digital policymaking. Motivated by mounting strategic dependencies, platform consolidation, and geopolitical uncertainty, EU institutions are accelerating efforts to build sovereign – independent, autonomous, and resilient – digital infrastructure. Central to this vision is a shift from rhetorical commitments to sovereignty toward a tangible, systems-oriented approach: one that centres not only on technology, but also on open communities, governance models, and shared capabilities built as Digital Commons.

PURPOSE OF THE BRIEF

This brief argues that a ‘Building Blocks’ approach offers a concrete approach for operationalising European digital sovereignty through the Open Internet Stack (OIS), a new initiative from DG CNECT intended as a successor to the Next Generation Internet (NGI) programme. Building Blocks, in this context, are understood as modular digital capabilities – both technical (e.g., open source software, protocols, hardware) and non-technical (e.g., governance models, procurement tools, community assemblies) – that are reusable, scalable, and aligned with EU policy objectives.

Developed through nearly 18 months of community engagement, consultation, and mapping by the NGI Commons consortium, this report presents a comprehensive taxonomy of Building Blocks and recommends key actions to embed Digital Commons principles within the architecture, governance, and implementation of the OIS. This methodology ensured the resulting taxonomy reflects both bottom-up insights from practitioners and alignment with top-down EU policy ambitions.

The development of the brief included the following activities:

- Interviews and workshops with Digital Commons projects, policy experts, academics, and public sector stakeholders.
- Targeted engagement with the Digital Commons Task Force (DCTF) and Digital Commons Policy Council (DCPC).
- A structured mapping exercise of 12 capability categories aligned with European digital policy and infrastructure priorities.
- Iterative validation through expert reviews, cross-sector dialogue, and public consultation.

THE ROLE OF DIGITAL COMMONS IN EUROPEAN SOVEREIGNTY

Digital Commons – encompassing open source software, standards, hardware, and governance – are essential for delivering infrastructure that reflects European values: openness, interoperability, participation, and public accountability. They provide viable, trustworthy alternatives to foreign-controlled proprietary systems and enable public and private actors in Europe to deploy infrastructure on their own terms.

The transition from NGI to OIS marks a strategic pivot: from funding experimental innovation toward provisioning open infrastructure at societal scale. This demands not only the identification of critical technical capabilities, but also recognition and investment in the community, legal, and governance layers that make those capabilities sustainable over time. It also requires a renewed commitment to Digital Commons, including both the technical artefacts themselves and the communities and governance models that surround them.

A TAXONOMY OF BUILDING BLOCKS FOR THE OPEN INTERNET STACK

We understand Building Blocks as fundamental digital capabilities (either technical or non-technical) that support the provisioning of digital infrastructure and which have broad societal functions, particularly when used to deploy technological solutions at scale. Positioning Building Blocks within a commons-based approach enables the EU to:

- Avoid vendor lock-in by promoting open, interoperable, standards-based infrastructure.
- Leverage community expertise, reducing duplication and enhancing resilience.
- Embed democratic governance and public interest principles into digital infrastructure.
- Accelerate innovation through transparent and collaborative development ecosystems.

The brief presents a layered taxonomy of Building Blocks organised into five domains:

- **Foundational Layer** – Core infrastructure including open hardware, cloud storage, network management, and protocols. These are essential for autonomy and resilience at the deepest layers of the stack.
- **Intermediation Layer** – Capabilities that enable trust, transactions, and interoperability, such as digital wallets, registries, payments, and vulnerability management.
- **Access and Interaction Layer** – Citizen- and user-facing services like decentralised communication tools, content delivery networks, and sovereign office suites that ensure end-user alignment with European values.
- **Non-Technical Layer** – Community, governance, legal, funding, and skills-based capabilities that provide the human and institutional infrastructure underpinning digital systems. These include civic assembly frameworks, public-commons partnership charters, and procurement consortia.
- **Functional Layer** – Cross-cutting EU policy objectives such as trust, interoperability, decentralisation, and governance. These guide prioritisation and alignment of Building Blocks with broader EU strategies, including the Digital Decade targets.

The taxonomy serves as a discovery and prioritisation tool to guide implementation of the OIS and future digital sovereignty initiatives.

FROM MAPPING TO ACTION KEY PRIORITIES FOR THE EUROPEAN COMMISSION

To operationalise a commons-based OIS and avoid reproducing extractive or proprietary models, the EC must go beyond technological components and build institutional capacity for sustainable, collaborative digital infrastructure. This includes:

1. **Enabling Collaborative Governance** – The EC should actively support the creation and maintenance of governance mechanisms that embed Digital Commons communities in the design, development, and oversight of Building Blocks.
2. **Clarifying the Role of Telecom Providers** – The relationship between traditional telecom infrastructure and open OIS components must be clearly defined to protect openness, modularity, and non-extractive infrastructure design.
3. **Adopting a Readiness Assessment Framework** – A formal evaluation framework is needed to assess candidate Building Blocks not just on openness, but on governance models, community health, and alignment with strategic EU goals.

4. **Refining the Building Blocks Taxonomy** – The current taxonomy should be co-developed further with Member States, civil society, and technical communities to ensure that future OIS investments support real-world, production-ready commons.
5. **Investing in Institutional Capacity and Dialogue** – Sustained dialogue between EU institutions, Member States, and commons communities will be essential to steward the OIS and ensure that commons-based practices are embedded at every level.

PRIORITY BUILDING BLOCKS FOR IMMEDIATE CONSIDERATION

Based on strategic alignment, operational maturity, and high relevance to sovereignty, the following seven Building Blocks are identified as immediate candidates for EC consideration:

1. **Cloud Storage:** Foundational to sovereign data management and independence from hyperscalers.
2. **Digital Wallets:** Critical for identity and trust systems under eIDAS 2.0.
3. **Vulnerability Management:** Ensures secure, transparent handling of infrastructure risk.
4. **Decentralised Communication Protocols:** Reduce reliance on foreign platforms and embed EU values.
5. **Digital Registries:** Enable cross-border services and enforce EU data policies.
6. **Civic Assembly Frameworks:** Ensure democratic legitimacy in infrastructure governance.
7. **Public–Commons Partnership Charters:** Institutionalise collaborative, co-managed infrastructure development.

These Building Blocks reflect both technical and non-technical capabilities that can immediately support Europe’s digital sovereignty ambitions, and each aligns with values of openness, participation, and collective stewardship.

CONCLUSION

The transition to a sovereign digital infrastructure model represents both a political imperative and a generational opportunity for Europe. The Building Blocks taxonomy presented in this report offers the European Commission a concrete, actionable approach to implementing the Open Internet Stack – one grounded in the successful practices of the Digital Commons ecosystem.

Europe’s future will be shaped not just by the infrastructure it builds, but by how it builds it: transparently, collaboratively, and in the public interest. By embracing a Building Blocks model that combines technical artefacts with participatory governance, sustainable funding, and community empowerment, the EU can demonstrate global leadership in provisioning digital infrastructure as a public good. The recommendations herein serve as a foundation for that vision – one that is modular, interoperable, democratically governed, and, above all, sovereign.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
TABLE OF CONTENTS.....	6
LIST OF TABLES	8
ABBREVIATIONS.....	9
1 INTRODUCTION	10
1.1 A BRIEF NOTE ON THE METHODOLOGY AND APPROACH.....	11
2 BACKGROUND: THE EUROPEAN UNION’S EFFORTS TO BUILD SOVEREIGN DIGITAL INFRASTRUCTURE	13
2.1 EFFORTS FROM THE EUROPEAN COMMISSION AND EUROPEAN PARLIAMENT	13
2.2 A TACTICAL APPROACH TO DIGITAL COMMONS	14
2.3 GETTING IT RIGHT	15
3 BUILDING BLOCKS: A DIGITAL COMMONS-BASED APPROACH FOR PROVISIONING EUROPE’S DIGITAL INFRASTRUCTURE	17
3.1 WHAT ARE BUILDING BLOCKS?	17
3.2 KEY CHARACTERISTICS	18
4 OVERVIEW – TECHNICAL BUILDING BLOCKS	21
4.1 FOUNDATIONAL LAYER.....	22
4.1.1 Hardware Capabilities.....	22
4.1.2 Compute and Storage Infrastructure Capabilities.....	23
4.1.3 Network and Internet Infrastructure Capabilities.....	24
4.1.4 Protocols and Standards Capabilities.....	25
4.2 INTERMEDIATION LAYER.....	25
4.2.1 Trust and Identity Capabilities	26
4.2.2 Data and Registries Capabilities.....	27
4.2.3 Payments and Transaction Capabilities	28
4.2.4 Security Capabilities	29
4.2.5 Management and Monitoring Capabilities	30
4.2.6 Operational Capabilities.....	30
4.3 ACCESS AND INTERACTION LAYER.....	31
4.3.1 Communications and Collaboration Capabilities	32
4.3.2 Web Technologies Capabilities	33
4.3.3 Domain-Specific Applications and Services Capabilities.....	34
4.4 NON-TECHNICAL LAYER	35
4.4.1 Community Capabilities	35
4.4.2 Legal Capabilities	36
4.4.3 Funding Capabilities	37
4.4.4 Governance Capabilities.....	38
4.4.5 Skills and Capacity-Building Capabilities.....	39
4.5 FUNCTIONAL LAYER.....	40
5 FROM MAPPING TO IMPLEMENTATION	41
5.1 PRIORITIES FOR IMPLEMENTATION OF A DIGITAL COMMONS-BASED APPROACH TO BUILDING BLOCKS	41

5.1.1	Priority #1: Establish Collaborative Governance Mechanisms for Digital Commons Communities	41
5.1.2	Priority #2: Define Strategic Roles and Responsibilities for Telecommunication Providers	41
5.1.3	Priority #3: Adopt a Digital Commons Readiness Assessment Framework for the Open Internet Stack	42
5.1.4	Priority #4: Update and Refine a Typology of Digital Commons-Based Building Blocks	42
5.1.5	Priority #5: Engage in Dialogue	42
5.2	PRIORITISING BUILDING BLOCKS FOR EUROPEAN SOVEREIGN DIGITAL INFRASTRUCTURE	42
5.2.1	Priority Building Block #1: Cloud Storage	42
5.2.2	Priority Building Block #2: Digital Wallets	43
5.2.3	Priority Building Block #3: Vulnerability Management	43
5.2.4	Priority Building Block #4: Decentralised Communication Protocols	43
5.2.5	Priority Building Block #5: Digital Registries	43
5.2.6	Priority Building Block #6: Civic Assembly Frameworks	43
5.2.7	Priority Building Block #7: Public–Commons Partnership Charters	43
6	CONCLUSION	44

LIST OF TABLES

TABLE 1: OVERVIEW OF TAXONOMY OF POTENTIAL LAYERS, CAPABILITIES, AND BUILDING BLOCKS..... 21

ABBREVIATIONS

DCTF	Digital Commons Task Force
SAP	Strategic Advisory Panel
DCPC	Digital Commons Community Platform
NGI	Next Generation Internet
OFE	OpenForum Europe
EC	European Commission
OIS	Open Internet Stack
WP(s)	Work Package(s)
LFE	Linux Foundation Europe
OSS	Open Source Software
DPGs	Digital Public Goods
DCPC	Digital Commons Policy Council
EDIC	European Digital Infrastructure Consortium
DCCP	Digital Commons Community Platform
CSA	Coordination and Support Action
CNRS	Centre national de la recherche scientifique
EP	European Parliament

1 INTRODUCTION

As the European Union (EU) enters a new institutional cycle, digital sovereignty has emerged as a defining imperative for both the European Commission (EC) and the European Parliament (EP)'s digital policy. In the face of growing geopolitical uncertainty, strategic dependencies on non-European infrastructure, and mounting concerns over the consolidation of digital power in foreign platforms, EU institutions are accelerating efforts to build *sovereign* – independent, autonomous, and resilient – digital infrastructure.

Sovereignty is increasingly not just an abstract goal; instead, it is rapidly becoming a structuring principle of EU digital policy. The political momentum behind this change is clearly evident: from the EC's proposal of a new Digital Networks Act (DNA) and its explicit commitment to boosting digital autonomy, to the Parliament's calls for a comprehensive "Cloud and AI Development Act". These developments are complemented by a more strategic role for open source technologies and Digital Commons, exemplified by new funding priorities in Horizon Europe and the institutionalisation of sovereignty-focused roles such as the new Executive Vice President for Tech Sovereignty, Security and Democracy, now held by Henna Virkkunen. At the heart of this shift lies a broader recognition that Europe's future digital infrastructure must be based on technologies and communities that reflect European values such as openness, interoperability, democratic governance, and human/digital rights.

This brief argues that a Building Blocks approach to provisioning digital infrastructure offers a tangible path forward in delivering on European digital sovereignty goals. We understand Building Blocks as fundamental digital capabilities (either technical or non-technical) that support the provisioning of digital infrastructure and which have broad societal functions, particularly when used to deploy technological solutions at scale. This understanding will be expanded on later in Section III.) The relevance of a Building Blocks approach is particularly true for the EC's Directorate-General for Communications, Content and Technology (DG-CNECT)'s new proposed flagship project, the Open Internet Stack (OIS), as well as related efforts like the proposed European Digital Infrastructure Consortium (EDIC) for Digital Commons. In doing so, we make the case that the EU must go beyond rhetorical commitments to digital sovereignty, and instead focus on both the open technical artefacts themselves, and the communities and governance models that enable access, participation, and usage of them as shared digital resources.

In this sense, an approach wherein Building Blocks are built on Digital Commons facilitates genuine competition by lowering barriers to entry and preventing vendor lock-in scenarios that have historically constrained European digitalisation efforts, both in EU institutions and across the EU's Member States. When infrastructure components are built on open standards and freely accessible codebases, smaller European technology companies, research institutions, and public sector organisations can participate as equals in the digital ecosystem, contributing innovations and competing on merit rather than being excluded by proprietary gatekeeping mechanisms. This creates a more resilient and diverse technological landscape where European values around privacy, transparency, and democratic governance can be embedded directly into the technical architecture of digital systems, rather than being retrofitted onto foreign-designed platforms that may operate according to different regulatory and cultural frameworks.

We therefore propose that delivering on the OIS demands a more intentional approach to identifying Building Blocks that can serve as the foundations of the proposed stack,¹ and in consideration of the contributions Digital Commons can make. In line with the philosophy of

¹ Note: While the use of the term Building Blocks might seem abstract, it is linked to the language used directly by the EC as part of publicly available information about the OIS. The term will be problematised, interrogated, and explained more in-depth in subsequent sections of the brief.

Digital Commons, this approach should emphasise both the *tangible* technological artefacts themselves and the *intangible* communities and governance models which enable their success. For example, the approach would likely be unsuccessful without funding to go directly towards maintaining projects. An approach overly focused on the technology without consideration of the conditions for enabling that technology would not deliver on the stated goals of ‘deploying trusted digital tools that don’t just match proprietary offerings but surpass them[,] facilitating regulatory compliance and guaranteeing sovereign EU solutions’.²

The theory of change here is clear: Digital Commons can serve as the foundational layer upon which genuine digital sovereignty can be built, moving beyond mere policy declarations toward concrete technological independence. These commons-based approaches provide European stakeholders with meaningful alternatives to proprietary systems dominated by non-European actors, offering choice not just in terms of vendors or service providers, but in fundamental architectural decisions about how digital infrastructure operates and is then later supported and governed. The choice to extrapolate infrastructure from Digital Commons solutions, communities, and ideals into concrete policy Building Blocks thereby translates into higher degrees of control over critical systems, allowing European institutions and organisations to understand, modify, and govern the technologies they depend upon, rather than remaining subject to the strategic decisions of foreign corporate entities.

The rest of this brief outlines possible Building Blocks for the OIS and provides examples that are well-suited to be provisioned by Digital Commons. Based on in-depth consultation and community engagement, it presents a comprehensive analysis of key capabilities which will be necessary for provisioning Europe’s sovereign digital infrastructure, building out a taxonomy that will help with the discovery and prioritisation of Building Blocks. These Building Blocks can be both *technical* (e.g. open source software (OSS), open protocols and standards, open hardware, etc) as well as *non-technical* (e.g. communities, governance models,³ procurement logics, etc). Both types of Building Blocks will be important ways of conceptualising and enabling governments, industry, and citizens to collectively build, deploy, and maintain sovereign digital infrastructure⁴ together as Digital Commons. We also advance understanding of the *functional* Building Blocks necessary for translating these prospective Building Blocks into concrete policy decisions that the EC can operationalise through the OIS. The brief concludes by providing policymakers and technical communities with actionable priorities to help guide the development of sovereign digital infrastructure in Europe while leveraging and contributing to Digital Commons.

1.1 A BRIEF NOTE ON THE METHODOLOGY AND APPROACH

This brief is authored by members of the consortium for the NGI Commons CSA, a Horizon Europe-funded EU project supporting policymaking and investment into the Digital Commons ecosystem.⁵ It builds upon extensive community engagement from nearly one and a half years

² <https://ngi.eu/download/ngi-forum-2025-from-ngi-to-open-internet-stack-powering-europes-digital-sovereignty-2-pager/?wpdmdl=66927>

³ While we refer here to ‘governance models’, it is important to note that, as highlighted in Deliverable 1.1, our aim is not to prescribe fixed or universal governance models. There is no ‘one-size-fits-all’ approach to governance in the context of Digital Commons; rather, the intention is to map and understand existing practices and approaches that can inform the development and stewardship of Building Blocks.

⁴ Sovereign digital infrastructure refers to the foundational technologies, systems, and institutions that enable a society to exercise autonomy, resilience, and control over its digital environment. It encompasses both the technical and institutional capacity to design, govern, and maintain critical digital services in alignment with democratic values, legal mandates, and strategic interests—without undue dependence on external actors.

⁵ <https://commons.ngi.eu/>

of the project's existence, including conversations, interviews, and workshops with representatives of Digital Commons projects, as well as policymakers, academics, and practitioners involved in Digital Commons and/or OSS specifically. The consortium members also did focused consultation with NGI Commons' Digital Commons Task Force (DCTF)⁶ and structured feedback sessions at the Digital Commons Policy Council (DCPC)⁷ meeting in Liverpool in May 2025.⁸

The effort also included a structured mapping exercise in late 2024 and early 2025 that surveyed online repositories to identify common taxonomies of solutions. This mapping inductively identified twelve initial core categories of Building Blocks, ranging from Digital Identity and Authentication to Communications and Collaboration, Network Infrastructure, Data Management, and emerging technologies. Each category contributes differently to the functional layers of the prospective OIS – Trust, Transactions, Connectivity, Decentralisation, Interoperability, and Governance – while advancing various Digital Decade targets. These categories were refined and adapted over time with inputs from experts and communities. This was then elaborated on through the addition of non-technical Building Blocks, which drew extensively from various community engagement activities and in particular from the DCPC Workshop in Liverpool in May 2025.

The taxonomy of Layers, Capabilities, and Building Blocks in Section IV aims to bridge policy objectives with technical implementation, creating a taxonomy for discovery and prioritisation that serves both policymakers and technical communities. In our view, the integration of Building Blocks into a cohesive taxonomy represents more than a technical exercise – it embodies a strategic vision for Europe's shared digital future, which is why Digital Commons artefacts and principles are more important than ever. This approach recognises that digital sovereignty requires not just technological solutions but also governance frameworks and sustainable communities. By prioritising capabilities – projects and communities – that advance multiple policy objectives simultaneously, we aim to create synergies between commons communities and European strategic goals, particularly around digital sovereignty.

Ultimately, there are always going to be limitations in such a taxonomy, and it will inevitably fail to cover or capture fully the nuances of digital infrastructure. Different individuals and stakeholder groups have different conceptions of digital infrastructure, and they express and categorise the constituent parts of that infrastructure, meaning what we present can at best offer something resembling an average of available experiences and perspectives, and an incomplete one at that. Instead, what we aim to offer is a first step for thinking about the discovery and prioritisation of Building Blocks, as well as a contextualisation of what it means for them to be based on Digital Commons and how they can be meaningfully operationalised. Moreover, what is suggested in the rest of this brief should not be taken as a prescription of what the EC will do or what the OIS will consist of – which is still being scoped and refined. Instead, it should be considered a substantive and evidence-based suggestion for how the OIS – the successor to the Next Generation Internet (NGI)⁹ – can be rooted in the ideals and policy objectives of the Digital Commons ecosystem the NGI programme has previously supported, as well as the ideals at the heart of the NGI Common CSA.

⁶ <https://commons.ngi.eu/dctf/>

⁷ <https://dcpc.info/>

⁸ <https://dcpc.info/policy-labs/lab2025/>

⁹ <https://commons.ngi.eu/>

2 BACKGROUND: THE EUROPEAN UNION'S EFFORTS TO BUILD SOVEREIGN DIGITAL INFRASTRUCTURE

The EU's digital sovereignty has emerged as one of the single most dominant political objectives of the EC's 2024-2029 term.¹⁰ In light of complex geopolitical tensions related to uncertainty in the American political system and evolving multilateral relationships, the current geopolitical landscape in Europe is more precarious than ever before. The challenges brought by these complex political and economic circumstances have also spilled over into the digital realm.

The digital ecosystem that underpin Europe's economy faces unprecedented challenges and opportunities. Dominant platforms continue to consolidate market power (which the EU is attempting to counteract via the Digital Markets Act),¹¹ critical digital infrastructure increasingly falls under non-European control,¹² and strategic dependencies in manufacturing and digital value chains threaten Europe's strategic autonomy in the digital world.¹³ It is now clearer than ever Europe's digital future relies on building its own infrastructure. It must not be infrastructure which is now owned by a single actor (usually a large corporation) but infrastructure which is open, independent, autonomous, and resilient – as well as interoperable and portable in the event of routine failure or acute crisis.

2.1 EFFORTS FROM THE EUROPEAN COMMISSION AND EUROPEAN PARLIAMENT

In 2025, many of the EU's digital policy efforts are framed under the banner of 'digital sovereignty',¹⁴ sometimes called 'tech sovereignty'.¹⁵ These efforts have accelerated¹⁶ in recent months, with the new EC's announcement of the new Executive Vice President for Tech Sovereignty, Security, and Democracy Henna Virkkunen – who has a mandate explicitly focused on digital/tech sovereignty – as well as the efforts¹⁷ of the EP's Committee on Industry, Research and Energy (ITRE) to write dual draft reports on technological sovereignty.¹⁸ They are also made manifest in the efforts of the independent EuroStack initiative, which focus on rallying public and industrial policy to support European digital independence.¹⁹

On the executive side, the pivot towards a more sovereignty-oriented posture on digital policy has been forthcoming in the work of the EC, and in particular DG-CNECT since at least last year. The EC's proposed 2025 Work Programme – titled 'Moving forward together: A Bolder, Simpler, Faster Union'²⁰ – reflects a light shift in emphasis on independence, autonomy, and

¹⁰ <https://ec.europa.eu/stories/2024-2029-commission/>

¹¹ <https://www.theguardian.com/business/live/2025/mar/19/trump-tariffs-trade-war-high-uncertainty-bank-of-japan-warns-musk-x-44bn-stock-markets-business-live>

¹² This view is affirmed in the recent State of the Digital Decade 2025 report: <https://digital-strategy.ec.europa.eu/en/library/state-digital-decade-2025-report>

¹³ <https://cepr.org/voxeu/columns/eus-strategic-dependencies-unveiled>

¹⁴ [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)

¹⁵ <https://cepa.org/article/europes-digital-leaders-call-for-tech-sovereignty/>

¹⁶ <https://www.euractiv.com/section/defence/news/tech-sovereignty-gets-its-own-executive-vice-president-in-the-new-commission/>

¹⁷ <https://www.euractiv.com/section/tech/news/rival-report-to-knafos-on-eu-tech-sovereignty-more-content-more-cautious/>

¹⁸ [https://oeil.secure.europarl.europa.eu/oeil/en/procedure-file?reference=2025/2007\(INI\)](https://oeil.secure.europarl.europa.eu/oeil/en/procedure-file?reference=2025/2007(INI))

¹⁹ <https://eurostack.eu/>

²⁰ https://commission.europa.eu/publications/2025-commission-work-programme-and-annexes_en

resiliency in EU digital policy, constituting an embrace of a more sovereignty-oriented position. Moreover, the ‘Horizon Europe Work Programme 2025’²¹ – specifically Part 7 on Digital, Industry, and Space²² – complements this approach, dedicating funding to open source projects such as the aforementioned OIS, a new public-industrial collaboration driven by the EC and aimed at developing open cloud, edge, and telecom infrastructure grounded in European control.²³

On the legislative side, the Parliament’s recent report tied to the 2025 Work Programme calls for comprehensive legislation – including a proposed ‘Cloud and AI Development Act’ – to ensure EU data and infrastructure fall under EU jurisdiction and are secure from high-risk foreign control, all in service of safeguarding Europe’s strategic autonomy.²⁴ As recently as the end of June 2025, such efforts have been likened by Henna Virkkunen as emphasising the need for support of Digital Commons like OSS and open standards communities – and potentially even in supporting investment in open source developers.²⁵ Additionally, there are the compromise-forcing efforts to produce the INI report on tech sovereignty,²⁶ which have led to a variety of proposals for funds related to tech sovereignty. Additionally, four major political groups – including the European People’s Party (EPP), Socialists and Democrats (S&D), Renew Europe, and the Greens/EFA²⁷ – put their collective efforts into rewriting the original text with their own version.²⁸ Some of these proposals build on but are distinct from the proposals being made as part EuroStack. Like on the EC side, such investments have a strong industrial focus and have made some overtures towards enabling the participation of open source communities and initiatives.

2.2 A TACTICAL APPROACH TO DIGITAL COMMONS

Expectedly, such efforts are being framed as essential in delivering on Europe’s varied but diffuse digital sovereignty ambitions. Taken together, they illustrate that digital sovereignty is not merely rhetoric; it is now embedded across legislative, funding, and regulatory levers of the 2025 agenda. Said Thibaut Kleiner, the Director for Future Networks at the EC’s DG-CNECT, at the recent NGI Forum 2025:²⁹ “The threat of losing to solutions on the other side of the Atlantic is real. Digital Sovereignty is about Europe developing, governing, and deploying its own infrastructure, on the one hand, but also its own solutions.”

This distinction made by Kleiner represents a pivot from the smaller, innovation-focused work being done by the EC through the NGI programme towards funding open source-based public and industrial infrastructures, which will help to meet the scale of digital sovereignty challenges the EU needs to address. While at first it will undoubtedly be disruptive for some of for those small innovators who have come to rely on that funding,³⁰ the transition from NGI to OIS is

²¹ https://hadea.ec.europa.eu/news/horizon-europe-2025-work-programme-available-now-2025-05-14_en

²² https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2025/wp-7-digital-industry-and-space_horizon-2025_en.pdf

²³ https://cordis.europa.eu/programme/id/HORIZON_HORIZON-CL4-2025-03-DATA-11

²⁴ https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html

²⁵ A few summaries of the remarks have been made online, but a recording of the event where EVP Virkkunen made these remarks can be viewed on the CEPS website. To access the video, see: <https://www.ceps.eu/ceps-events/eurostack-a-concrete-pathway-to-european-digital-sovereignty-and-strategic-autonomy/>

²⁶ [https://oeil.secure.europarl.europa.eu/oeil/en/procedure-file?reference=2025/2007\(INI\)#section2](https://oeil.secure.europarl.europa.eu/oeil/en/procedure-file?reference=2025/2007(INI)#section2)

²⁷ <https://openfuture.eu/blog/europe-talks-digital-sovereignty/>

²⁸ https://www.europarl.europa.eu/meetdocs/2024_2029/plmrep/COMMITTEES/ITRE/DV/2025/06-03/ITEM5_AlternativeCA1_EPP_SD_Renew_Greens_Europeantechnologicalsovereignty_INI_EN.pdf

²⁹ <https://ngi.eu/ngi-forum25/>

³⁰ <https://sciencebusiness.net/news/r-d-funding/backlash-against-planned-horizon-europe-cuts-open-source-software-projects>

nevertheless – as proposed – a scale-up in terms of the level of ambition for Digital Commons like OSS and open standards in the EU's public and industrial strategy for the digital world.³¹ It remains to be seen how it will be implemented, but from the outside it represents a substantial embrace of OSS in particular as part of EC policy.

The key question, then, is identifying the right Building Blocks for this approach, making sure the EC can draw on the large pool of Digital Commons – many of which it has invested in in recent years through the NGI – towards aligned public and industrial policymaking which is more forward-looking. As these projects begin to be described more simply as 'software' – perhaps to clarify their purpose – it is essential to ensure that the Digital Commons focus on community and governance is not lost. Digital Commons can play a vital role in helping European public institutions to promote an inclusive, participatory, and non-extractive development process for the scale of open solutions as sovereign digital infrastructure in the EU.³²

So, how will the role of Digital Commons in EC policy change from here, especially in light of the dominant focus on digital sovereignty? As it regards the OIS, which aligns itself with the EC's goals of digital sovereignty, the Digital Commons ecosystem has a unique opportunity through NGI Commons and related community fora to emphasise how non-extractive, rights-respecting, and intentionally-designed OSS can be scaled as Digital Commons. In doing so, the community can work with NGI Commons and the European Commission to identify a vision for coordinated public-industrial collaboration and development which aligns with their current digital sovereignty needs and extends what worked under the NGI. Such alignment would support the ability for the EC to transition its grassroots innovation funding towards funding with (possibly) greater scale and reach than before.

As a result, when shaping public and industrial policy for a more open and public interest form of digital sovereignty, we argue that Digital Commons are as vital as they have ever been. As the EC continues articulating the concept of the OIS, this brief highlights two often-overlooked but essential dimensions. First, we examine how technological (both technical and non-technical) Building Blocks can be part of the OIS, enabling the use of a Digital Commons-based approach for provisioning Europe's digital infrastructure (Sections III and IV). Second, we argue that sustained investment in not just the scale-up but the maintenance and evolution of the Digital Commons ecosystems underpinning the stack – and the digital infrastructure it supports³³ – is crucial (Section V).

2.3 GETTING IT RIGHT

Getting the NGI to OIS transition right and operationalising digital sovereignty goals through tangible policy decisions is critical, and it will invariably influence the security, innovation, and competitiveness of Europe in the years to come. But it is also important to consider how initiatives – such as the proposed OIS – might be used by Europe to position itself and engage in norm-setting through global digital collaboration, including international partnerships and dialogues.

The European Commission and the High Representative for Foreign Affairs and Security Policy³⁴ recently adopted its "The International Digital Strategy for the European Union".

³¹ [https://cdn.netzpolitik.org/wp-upload/2025/06/From NGI to Open Internet Stack Activating the European open digital industry.pdf](https://cdn.netzpolitik.org/wp-upload/2025/06/From%20NGI%20to%20Open%20Internet%20Stack%20Activating%20the%20European%20open%20digital%20industry.pdf)

³² <https://commons.ngi.eu/>

³³ https://openfuture.eu/wp-content/uploads/2024/11/241113_Digital-Commons-as-Providers-of-Public-Digital-Infrastructures.pdf

³⁴ <https://www.consilium.europa.eu/en/council-eu/high-representative-foreign-affairs-security-policy/>

Broadly, the strategy tries to link up European digital policy with its international strategy for engaging with the rest of the world – something which was long overdue.³⁵ The EC's report does some work to link up EU values as it regards its internal tech policy with a more coherent approach to international partnerships and global governance. The report does many notable things, such as articulating a Global Tech Business Offer, doubling down on its role in convening and norm-setting, and extending new global positioning around topics like AI, online platforms and digital public infrastructure.³⁶

As the EU continues to codify this position globally, showing what it is doing internally will allow the rest of the world to learn from what is happening in Europe, especially as it regards openness in digital infrastructure. If done right, the proposed OIS and other sovereign digital infrastructure projects could offer a strong and coherent approach to developing open and sovereign digital infrastructure would be a vital part of both internal policy *and* this external positioning. Many countries across the globe will be looking towards Europe to see how the EU and its Member States are seeking to attain digital sovereignty through digital infrastructure efforts, especially as they work on their own under various names such as GovTech,³⁷ Digital Public Infrastructure,³⁸ and Government-as-a-Platform³⁹ (amongst many others).

But, the impulse to act swiftly in building out sovereign digital infrastructure could create risk if the EU does not create the stability and continuity of purpose the Digital Commons and open source community ecosystems need to respond to participate in this change. Failing to work with the open source and Digital Commons communities towards this vision could create challenges in long-term cooperation, disadvantaging the movement towards a Digital Commons-based approach for provisioning Europe's digital infrastructure, and creating fragmentation in the EU's global digital cooperation.

³⁵ <https://digital-strategy.ec.europa.eu/en/library/joint-communication-international-digital-strategy-eu>

³⁶ Ibid.

³⁷ <https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/govtech>

³⁸ <https://www.undp.org/digital/digital-public-infrastructure>

³⁹ https://ash.harvard.edu/wp-content/uploads/2024/02/293091_hvd_ash_gvmnt_as_platform_v2.pdf

3 BUILDING BLOCKS: A DIGITAL COMMONS-BASED APPROACH FOR PROVISIONING EUROPE'S DIGITAL INFRASTRUCTURE

We argue that Building Blocks – which are publicly expressed⁴⁰ as commitments of the OIS – represent a unique expression of digital capabilities which are ideally suited to be provisioned by Digital Commons and which can help Europe in provisioning the society-scale infrastructure it needs to drive its digital sovereignty efforts. But what should we even understand a Building Block as?

3.1 WHAT ARE BUILDING BLOCKS?

The understanding of what a Building Block is remains up for debate, with some defining it broadly in terms of societal functions and others defining it more narrowly in terms of software modules (and yet more somewhere in-between). For example, as defined by the EC itself, Building Blocks provide “... secure, interoperable digital solutions that streamline cross-border activities, helping public administrations and businesses connect across Europe and paving the way for a unified single digital market.”⁴¹ Another definition of Building Blocks from the GovStack Initiative⁴² is as follows: “Building blocks (BBs) are software modules that can be deployed and combined in a standardised manner. Each building block is capable of working independently.”⁴³

For our purpose, we broadly understand Building Blocks as fundamental digital capabilities (either technical or non-technical) that support the provisioning of digital infrastructure and which have broad societal functions, particularly when used to deploy technological solutions at scale. In a European context, Building Blocks are those digital capabilities which enable sustainable development and sovereignty at scale when used at society-scale (as laid out in the “Digital Commons as Providers of Public Digital Infrastructures” paper).⁴⁴ We adopt a comprehensive view of Building Blocks that encompasses the full spectrum of Digital Commons, including OSS, open standards, open data, open content, open hardware, etc. This inclusive approach recognises that achieving Europe's digital sovereignty ambitions and various related policy objectives can be provisioned in many different ways, and channeled towards the delivery of key capabilities across multiple domains and across various layers of the Internet Stack.

Our vision for Building Blocks extends this vision by proposing a modular and (in theory) interoperable typology of core digital capabilities that can be based on Digital Commons, and which can be reused across systems to support sovereign digital infrastructure. Within each category of capabilities, there are many different types of Building Blocks. Moreover, we not only broaden the traditional software-centric understanding of these Building Blocks to encompass data, standards, content, and hardware – aligning with the expansive scope of Digital Commons – but also include non-technical Building Blocks necessary for building enabling capacity for their development, deployment, and maintenance. This novel framing, we argue, serves both policymakers and technical communities, offering a shared language

⁴⁰ <https://ngi.eu/download/ngi-forum-2025-from-ngi-to-open-internet-stack-powering-europes-digital-sovereignty-2-pager/?wpdmdl=66927>

⁴¹ <https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/Digital+Building+Blocks+for+Europe>

⁴² <https://www.govstack.global/>

⁴³ <https://govstack.gitbook.io/sandbox/explore-stack/building-blocks>

⁴⁴ https://openfuture.eu/wp-content/uploads/2024/11/241113_Digital-Commons-as-Providers-of-Public-Digital-Infrastructures.pdf

for identifying which capabilities can deliver the most strategic value to society-scale digital transformation in Europe, as well as best leverage the value and participation of Digital Commons projects, communities and governance models.

The identification and prioritisation of these Building Blocks might seem abstract – and it is, to a certain extent. But at its core, it extends broad concepts of infrastructure provisioning into concrete priorities that can guide policy development and resource allocation leveraging commons, in particular OSS. Building Blocks can be both developed from the bottom-up and exogenously defined from the top down. It would be inaccurate to claim that one approach is necessarily more possible or likely than the other to arrive at any definition of Building Blocks, as there are always elements of both approaches at play.

Our approach was both bottom-up and top-down. It sought to engage Digital Commons communities and identify priorities which were natural expressions of how people working in these communities were already understanding and conceptualising broad categories of these capabilities – and then help link them up with the expressed priorities of the EC. For example, proposed by the EC itself at the NGI Forum 2025 on 19-20 June 2025, the Open Internet Stack (OSI) will specifically deliver: “... a curated set of interoperable, open-source digital building blocks designed explicitly for ease of use and rapid deployment. These building blocks will cover critical areas like secure digital identities, cybersecurity, decentralised platforms, and interoperability.”⁴⁵ Such a taxonomy of Building Blocks must, of course, take these areas and considerations into account.

3.2 KEY CHARACTERISTICS

The conceptualisation of Building Blocks as fundamental components of sovereign digital infrastructure draws from well-established principles in systems architecture and platform theory. The literature suggests designing and developing the infrastructure of data management platforms through a layered-modular architectural approach, which entails dividing the platform into a content layer, service layer, network layer, and device layer.⁴⁶ This modular approach enables what digital platform ecosystems achieve by utilising an ecosystem of autonomous agents to co-create value, moving beyond traditional organisational boundaries to create society-scale infrastructure capabilities.⁴⁷

In this sense, the theoretical foundation for Building Blocks rests on the understanding that digital technology is enmeshed in and tightly coupled with physical systems in a layered architecture, but also human systems which support its deployment, support, and governance in the real-world. This coupling is particularly relevant for European digital sovereignty ambitions, where the infrastructure must be both technically robust and politically independent. Extrapolating from the literature, we can reason that digital platforms confer competitive advantage through superior architectural configurations,⁴⁸ suggesting that the systematic design of Building Blocks can provide strategic advantages at the societal level, not merely at the organisational level.

The modular architecture paradigm is especially pertinent when considering the scale and complexity of pan-European digital transformation. This principle becomes critical when

⁴⁵ <https://ngi.eu/download/ngi-forum-2025-from-ngi-to-open-internet-stack-powering-europes-digital-sovereignty-2-pager/?wpdmli=66927>

⁴⁶

https://www.researchgate.net/publication/220079642_The_New_Organizing_Logic_of_Digital_Innovation_An_Agenda_for_Information_Systems_Research

⁴⁷ https://www.researchgate.net/publication/220079897_Research_Commentary_-_Platform_Evolution_Coevolution_of_Platform_Architecture_Governance_and_Environmental_Dynamics

⁴⁸ <https://onlinelibrary.wiley.com/doi/abs/10.1111/jpim.12105>

designing infrastructure that must serve diverse national contexts, regulatory environments, and technological ecosystems across Europe while maintaining coherence and interoperability. The Building Blocks approach allows for what can be understood as ‘infrastructural sovereignty’,⁴⁹ or the ability to maintain control and adaptability over core digital capabilities while enabling innovation and collaboration across boundaries.

The infrastructure perspective on Building Blocks acknowledges that digital capabilities are not merely software components but constitute the foundational layer upon which societal functions depend. This aligns with broader infrastructure theory that recognises infrastructure as both technical systems and social institutions that enable collective action.⁵⁰ In the European context, Building Blocks represent a strategic approach to creating what might be termed ‘infrastructural commons’ – shared digital capabilities that serve public purposes while remaining open to innovation and adaptation by diverse stakeholders. As such, Building Blocks should not be viewed solely as technical artefacts but as institutionalised commons arrangements that require active governance, maintenance, and community involvement. Recognising them as infrastructural commons underscores their role as enduring socio-technical systems that embed public values and enable long-term collective provisioning of essential digital functions part of Europe’s public digital infrastructure.⁵¹

In helping to ensure that selected Building Blocks fulfil such ambitions, the characteristics that follow are therefore not simply technical specifications, but design principles that reflect the complex requirements of building digital infrastructure that is simultaneously open, sovereign, scalable, and sustainable. These characteristics emerge from the recognition that Europe’s digital future depends on a modular, interoperable foundation of digital capabilities that can evolve with changing needs while maintaining democratic control and public orientation. We therefore propose the following key characteristics for an EU taxonomy of Building Blocks:

- **Open:** Building Blocks are highly open, being based on artefacts with OSS licenses and leveraging the participation of communities and open governance models.
- **Independence:** Building Blocks can function autonomously while offering well-defined interfaces for integration with other components.
- **Interoperability:** Building Blocks adhere to open standards and protocols that enable seamless interaction across systems and borders.
- **Modularity:** Building Blocks are designed with clear boundaries and responsibilities, allowing them to be updated or replaced without disrupting the entire ecosystem.
- **Standardisation:** Building Blocks follow consistent patterns and specifications that facilitate integration and reduce implementation complexity.
- **Strategic Alignment:** Building Blocks support European digital sovereignty goals and other digital policy ambitions.

In principle, all proposed categories of Building Blocks layers collectively can advance the European Digital Decade objectives as well. For example:

- **Digital Skills** development is supported by accessible developer tools, web technologies, and applications.
- **Digital Infrastructure** benefits from network components, hardware, and cybersecurity.

⁴⁹ <https://www.ictworks.org/digital-sovereignty-digital-development/#:~:text=Infrastructural%20Sovereignty:%20Nations%20claim%20control,often%20mask%20complex%20international%20dependencies>

⁵⁰ <https://mitpress.mit.edu/9780262525374/media-technologies/>

⁵¹ https://openfuture.eu/wp-content/uploads/2024/11/241113_Digital-Commons-as-Providers-of-Public-Digital-Infrastructures.pdf

- **Digital Business** transformation is enabled by financial services, data management, and emerging technologies.
- **Digital Public Services** are enhanced through identity systems, collaboration tools, and applications.

By embracing openness, independence, interoperability, modularity, standardisation, and strategic alignment as core design principles, these Building Blocks create the foundation for 'infrastructural sovereignty' – the ability to maintain democratic control over essential digital capabilities while fostering innovation and collaboration across borders. This comprehensive understanding extends beyond traditional software-centric definitions to encompass the full spectrum of digital commons, including data, standards, content, and hardware, as well as the non-technical capacities necessary for their sustainable governance and maintenance.

Through this modular, layered approach, Building Blocks not only serve as technical components but as 'infrastructural commons' that embed public values and enable Europe to achieve its Digital Decade objectives while preserving its commitment to democratic governance, technological independence, and societal benefit. The resulting infrastructure becomes more than the sum of its parts – a resilient, adaptable, and genuinely European digital ecosystem of capabilities that can evolve with changing needs while maintaining Europe's foundational commitment to openness, sovereignty, and the public good as part of its public digital infrastructure.

4 OVERVIEW – TECHNICAL BUILDING BLOCKS

The following section offers a taxonomy that is intended to be useful for identifying potential technical Building Blocks for sovereign digital infrastructure. It contains categories of Building Blocks for consideration to the EC – referred to as “Capabilities”. These broad Capabilities are in turn subsets of “Layers”, which represent even broader parts of the stack. All groupings are illustrative but are intended to help identify Digital Commons worth investing in.

A summary of the taxonomy can be found below in Table 1.

TABLE 1: OVERVIEW OF TAXONOMY OF POTENTIAL LAYERS, CAPABILITIES, AND BUILDING BLOCKS

Layer	Capability Category
Foundational Layer	Hardware Capabilities
	Compute and Storage Infrastructure
	Network and Internet Infrastructure
	Protocols and Standards
Intermediation Layer	Trust and Identity
	Data Capabilities
	Payments and Transactions
	Security Capabilities
	Management and Monitoring
	Operational Capabilities
Access and Interaction Layer	Communications and Collaboration
	Web Technologies
	Domain-Specific Applications
Non-Technical Layer	Community Capabilities
	Legal Capabilities
	Funding Capabilities
	Governance Capabilities
	Skills and Capacity-Building
Functional Layer	Cross-Cutting Policy Priorities

The taxonomy is derived directly from a structured mapping of digital infrastructure domains, categories, and solutions, which have been preliminarily mapped against EU policy frameworks. They have been drawn from numerous sources including independent mappings and understandings of ideas like Digital Public Infrastructure (DPI)⁵² and GovStack.⁵³ Feedback on the taxonomy was given at numerous stages through one-to-one discussions and workshops with community members of NGI Commons.

⁵² <https://www.undp.org/digital/digital-public-infrastructure>

⁵³ <https://www.govstack.global/>

Note that while a list of example Building Blocks and more detailed spotlight of individual Building Blocks have been provided under each category of Capabilities, these examples are intended to be illustrative rather than exhaustive. The spotlighted Building Blocks have been selected based on their strategic relevance, the maturity of potential solutions, and strong potential application of existing Digital Commons. The goal of presenting these examples in this format is to showcase the possibilities for what a Building Block might be, supporting the EC in illustrating high-priority starting points that ensure strong alignment with Digital Commons technologies, communities, and governance models.

Further analysis and stakeholder input will be necessary to refine, validate, and eventually operationalise a shortlist of candidate Building Blocks for consideration, in consideration of the Functional Layer and possibly using the grouping of Layers and Capabilities as a starting point. An early attempt at doing this will be presented in Section 6.1. This will be later followed by surveys which will draw in community engagement to help identify more concrete priorities based on the ideas expressed in this brief.

4.1 FOUNDATIONAL LAYER

The Foundational Layer of sovereign digital infrastructure encompasses the essential foundation – both physical and virtual – infrastructure on which all other digital services depend. This includes capabilities such as open source hardware, compute and storage infrastructure, network and internet infrastructure, and protocols and standards.

By ensuring autonomy and resilience at the deepest layers of the digital stack, these foundational layers might not be the ‘flashy’ capabilities that interest people the most, but they are critical prerequisites for public interest innovation as you move higher up the stack. Having control of these foundational layers is arguably the most important for digital sovereignty, as control over capabilities such as cloud and networks in particular help the EU to gain control of its supply chains, reduce dependencies on proprietary vendors, supporting modularity and scalability, and promoting alignment with Europe’s digital policy ambitions.

4.1.1 Hardware Capabilities

The Digital Commons perspective on hardware reframes hardware in a novel way. It shows that need not only be treated as a commercial product – to be procured and implemented using waterfall approaches and huge upfront capital expenditure. Instead, it views hardware as potentially open and shared critical infrastructure, dependent on the participation of communities and able to be shaped by models for open governance and open collaboration.

4.1.1.1 Example Building Blocks

1. Open Hardware
2. Open Semiconductors
3. Radio (Mesh/LoRa)
4. Internet Exchange Points
5. Routers

4.1.1.2 Spotlight Building Block: Open Hardware

Open Hardware projects – like RISC-V⁵⁴-based systems, Libre Computer,⁵⁵ etc – will be central to European digital sovereignty. Open Hardware aligns with Europe's goals of reducing reliance on foreign vendors, increasing trust in public infrastructure, and enabling home-grown manufacturing ecosystems. For example, in the case of RISC-V, its benefits lie in its open and programmable architecture, which offers flexibility across many potential sectors and industries,⁵⁶ reducing reliance on vendors to support implementations.

In practice, investing in and supporting Open Hardware as Digital Commons would require a strong enabling policy framework to help develop and implement Open Hardware initiatives. For example, this might include updating public procurement mandates in favour of more verifiable, repairable, and modular systems, funding cooperative manufacturing hubs/shared design platforms, or building out reference implementations (e.g., RISC-V clusters running OpenStack)⁵⁷ to demonstrate viability in public cloud, edge, and HPC environments.⁵⁸ That said, these capabilities would be foundational for sovereignty digital infrastructure, particularly if those provisioning it were to work closely with the private sector in provisioning the infrastructure the public sector can then build on top of.

4.1.2 Compute and Storage Infrastructure Capabilities

Digital Commons projects and communities cast a new light on how we understand compute and storage infrastructure. Treating these foundational capabilities as Digital Commons invite a new set of priorities; rather than viewing technologies like virtualisation, orchestration, and backend compute through the lens of large-scale commercial platforms or fixed vendor relationships, this way of thinking positions compute them as shared, flexible, federated, and governed in the public interest.

4.1.2.1 Example Building Blocks

1. Cloud Storage
2. Compute Virtualisation
3. Edge Computing
4. Internet of Things

4.1.2.2 Spotlight Building Block: Cloud Storage

Cloud Storage plays a pivotal role in the EC's digital sovereignty agenda. The ability to host data on a cloud has unlocked trillions of dollars of market capitalisation in recent years across the globe, and open source technology has already been critical in enabling the growth of the largest offerings from organisations like Microsoft and Amazon. By instead offering EU-hosted, standards-based alternatives to U.S. hyperscalers, the EU knows that it can help reduce on foreign-controlled infrastructure that may be subject to extraterritorial surveillance, such as the U.S. CLOUD Act.⁵⁹

⁵⁴ <https://riscv.org/>

⁵⁵ <https://libre.computer/>

⁵⁶ <https://www.riser-project.eu/the-intersection-of-open-hardware-and-european-data-sovereignty-2/>

⁵⁷ <https://arxiv.org/abs/2407.12008>

⁵⁸ <https://arxiv.org/abs/2505.02650>

⁵⁹ <https://nextcloud.com/blog/trumps-second-term-a-critical-turning-point-for-open-source-and-digital-sovereignty/>

In practice, open source platforms like MinIO⁶⁰ enable sovereign AI and cloud environments, supporting hybrid and private deployments that avoid vendor lock-in while offering cost-efficiency and performance benefits.⁶¹ Meanwhile, solutions like Nextcloud are already widely adopted by public institutions as a secure collaborative storage solution fully manageable under EU jurisdiction, and they have huge participation from the open source community. In Denmark, there is a huge effort underway to move away from Microsoft Office and Windows with the goal of digital sovereignty.⁶² Such efforts may yet better remain federated and decentralised, but warrant further investigation.

4.1.3 Network and Internet Infrastructure Capabilities

Digital Commons are part of the very foundations of Network and Internet Infrastructure. Historically, Digital Commons principles have not merely been the background plumbing of the Internet, but helped form the Internet itself. In this framing, networks are not just engineered systems managed by telecommunications operators or private vendors, but dynamic and interconnected public goods that underpin the functioning of digital societies.

4.1.3.1 Example Building Blocks

1. Network Management
2. Network Testing
3. Network Monitoring
4. Software Defined Networking Platforms

4.1.3.2 Spotlight Building Block: Network Management

Network management systems allow public institutions to monitor, secure, and optimise the digital infrastructure. These systems create foundational infrastructure for network visibility, performance assurance, and incident response, ensuring that connectivity is maintained in a resilient, efficient, and sovereign manner.⁶³ These capabilities may include individual tools and protocols (e.g. routing and traffic monitoring) or integrated platforms supporting end-to-end service reliability, quality of service (QoS), and anomaly detection.⁶⁴

In Europe, robust network management is particularly important to ensure interoperability across Member State infrastructures, especially in federated systems involving domains such as digital identity, healthcare, or customs.⁶⁵ Coordinated approaches to network management could allow Member States to more easily diagnose cross-border outages, monitor the security of intergovernmental platforms, or enforce data sovereignty and localisation obligations. Reusable open source network management components could help ensure that public digital services are not only functional and performant, but also independently verifiable and resilient against disruptions or dependency risks.

⁶⁰ <https://min.io/>

⁶¹ https://www.linkedin.com/posts/timothyjcoats_mitigating-geopolitical-concerns-with-a-sovereign-activity-7328825846108999680-zsXR

⁶² <https://www.zdnet.com/article/why-denmark-is-dumping-microsoft-office-and-windows-for-libreoffice-and-linux/>

⁶³ <https://www.enisa.europa.eu/publications/recommendations-for-eu-cybersecurity-investments>

⁶⁴ <https://www.ripe.net/publications/docs/ripe-767/>

⁶⁵ <https://digital-strategy.ec.europa.eu/en/policies/interoperability-public-services>

4.1.4 Protocols and Standards Capabilities

A Digital Commons perspective might understand protocols and standards as more than technical specifications or bureaucratic requirements. These are foundational tools that enable digital systems through community participation and open governance. Open standards, when co-designed by diverse stakeholders, can create a more federated, rights-respecting internet, especially when collectively governed and updated over time.

4.1.4.1 Example Building Blocks

1. Decentralised Communication Protocols
2. Open Authentication and Authorisation Protocols
3. Secure, Privacy-Preserving DNS
4. Real-Time Peer-to-Peer Communication Protocols
5. Federated Social Networking Protocols
6. Decentralised Identifiers (DIDs)

4.1.4.2 Spotlight Building Block: Decentralised Communication Protocols

Decentralised Communication protocols can play a critical role in the open Internet by enabling secure messaging across a range of bodies, including the public sector. Open protocols like ActivityPub⁶⁶ and the Matrix protocol,⁶⁷ as well platforms such as Mastodon,⁶⁸ are supporting the growth of a federated "Fediverse" model that reduces reliance on centralised platforms and aligns infrastructure with European values like privacy. Open standards initiatives like the W3C's decentralised identifiers⁶⁹ are also leading the charge and exemplify how standards can be co-designed by diverse actors to serve more federated and rights-respecting communication on the Internet.

In practice, Decentralised Communication Capabilities allow European institutions to maintain control over their communication infrastructure rather than relying on American or Chinese platforms like WhatsApp, Telegram, or Slack. A substantial portion of governmental digital infrastructure continues to depend on service providers outside the EU.⁷⁰ This dependency creates vulnerabilities in Europe's digital autonomy. For example, in France the Interministerial Directorate for Digital Affairs (DINUM) has made explicit the goals of security and digital sovereignty, both of which were deemed to be impossible through proprietary systems. It has since deployed Matrix-based systems for government communications, which have many advantages from a digital sovereignty perspective.⁷¹

4.2 INTERMEDIATION LAYER

The Intermediation Layer of sovereign digital infrastructure serves as the connective tissue, enabling trusted data exchange, identity verification, secure access control, and financial transactions between foundational systems and user-facing services. This includes capabilities

⁶⁶ <https://activitypub.rocks/>

⁶⁷ [https://en.wikipedia.org/wiki/Matrix_\(protocol\)](https://en.wikipedia.org/wiki/Matrix_(protocol))

⁶⁸ <https://mastodon.social/explore>

⁶⁹ <https://www.w3.org/TR/did-1.0/>

⁷⁰ <https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package>

⁷¹ <https://www.heise.de/en/background/Interview-Element-CEO-on-the-matrix-protocol-and-digital-sovereignty-10333426.html>

such as trust and identity, data and registries, payments and transactions, security, management and monitoring, and operations.

By serving as a bridge between foundational layers and more public-facing applications and services, these intermediation layers encompass a range of spotlighted Building Blocks which might be important for public service delivery, in line with the principles behind Digital Public Infrastructure, or DPI. Strong investment in Building Blocks across such layers could help support implementation and enforcement of key European legislation and regulation – such as the General Data Protection Regulation (GDPR), the European Data Strategy,⁷² and the Digital Identity Framework – positioning them as central pillars in enabling citizen-centric, rights-preserving sovereign digital infrastructure.

4.2.1 Trust and Identity Capabilities

A Digital Commons perspective on Trust and Identity Capabilities as Digital Commons might reframe identity and trust systems beyond simple technical solutions or compliance requirements. In this view, those systems could represent political infrastructure connected to real people; they determine how citizens, businesses, governments, and other actors authenticate one another, interact securely, and manage data consent. They also enable cross-border digital services and provide the technical foundations for implementing regulations governing the movement of people.

4.2.1.1 Example Building Blocks

1. Digital Wallets
2. Self-Sovereign Identity Protocols
3. Identity and Access Management
4. Consent-Management Platforms
5. Digital Identity Systems
6. E-Signature
7. Registration

4.2.1.2 Spotlight Building Block: Digital Wallets

In the EU, Digital Wallets will already allow individuals to store and present digital credentials (e.g. identity cards, professional licenses, authorisations) under their control.⁷³ These systems – which are being actively developed – create secure infrastructure for identity verification, data sharing, and electronic signatures that work across European borders. The EUDI Wallet⁷⁴ uses open standards like W3C Verifiable Credentials⁷⁵ and operates under eIDAS 2.0 regulations,⁷⁶ giving people direct control over their personal data, as well as the ability to decide what information to share, when, and with which organizations while maintaining GDPR compliance.

⁷² https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

⁷³ https://eur-lex.europa.eu/resource.html?uri=cellar:057ef8d0-c3d2-11eb-a925-01aa75ed71a1.0001.02/DOC_1&format=PDF

⁷⁴ https://www.idemia.com/pdf-export.php?post_id=11692&utm

⁷⁵ <https://www.w3.org/TR/vc-data-model-2.0/>

⁷⁶ <https://linuxfoundation.eu/blog/openwallet-foundation-and-eudi-wallets/>

These technologies enable streamlined access to services ranging from banking to university applications without revealing unnecessary personal details. In practice, such technologies are already being worked on but the EUDI wallet and related technologies could be elaborated on further as a shared Building Block. At the moment, the OpenWallet Foundation⁷⁷ essentially provides the open source technical foundation and industry coordination that supports the EUDI Wallet initiative, rather than being a direct implementer.⁷⁸ They create the underlying standards-based components that European wallet providers can build upon, ensuring interoperability while the EU handles the regulatory framework and implementation through eIDAS 2.0.

4.2.2 Data and Registries Capabilities

Digital Commons-based Data and Registries Capabilities can be seen as active public infrastructure, not just passive storage or resources to be extracted from. They include core registries covering civil status, land ownership, and business records, along with geospatial databases, analytics platforms, and digital archives – many of which form the backbone of essential public services and the functioning of the state.

4.2.2.1 Example Building Blocks

1. Digital Registries
2. Data Management Platform
3. Database Management
4. Data Integration
5. Business Intelligence
6. GIS
7. File Sharing
8. Data Analytics
9. File Management
10. Land Registries

4.2.2.2 Spotlight Building Block: Digital Registries

Digital registries can be understood as ‘centrally managed databases that uniquely identify persons, vendors, facilities, procedures, products and sites related to an organisation, industry or activity’.⁷⁹ These systems can create foundational infrastructure for trusted data exchange, enabling secure identification, record-keeping, and cross-border interoperability of critical information. In the EU, such registries are already used for tax (e.g. VIES), company (e.g. BRIS), and social security (e.g. EESSI) data, and are increasingly governed through open standards and shared data models, including those defined by the European Interoperability Framework and SEMIC.⁸⁰

Digital registries form the backbone of many necessary cross-border services – from e-prescriptions to business licensing – by ensuring that reference data is accurate, trusted, and

⁷⁷ <https://openwallet.foundation/>

⁷⁸ <https://openwallet.foundation/>

⁷⁹ <https://exchange.dial.global/building-blocks/digital-registries>

⁸⁰ <https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic>

aligned with legal requirements like GDPR and the Single Digital Gateway Regulation.⁸¹ Open source foundations like the Interoperability Test Bed provide blueprints that can support European coordination without mandating a single vendor or architecture, ensuring sovereignty, resilience, and interoperability across Member State systems.⁸² Moving forward, it will be important for the EU to expand and harmonise these capabilities by offering reusable components and governance models for public registries.

4.2.3 Payments and Transaction Capabilities

Thinking of Payments and Transactions Capabilities as Digital Commons reframes financialisation and value creation in a novel way. It shows that such capabilities need not only be treated as commercial services – to be procured from commercial platforms using extractive models and huge intermediary fees. In this view, it sees such capabilities as potentially open and shared critical infrastructure, which can be shaped, supported, and even governed by the people they also serve.

4.2.3.1 Example Building Blocks

1. Public Financial Management (PFM) Systems
2. Payments Systems
3. Business Application
4. Open Networks for Commerce
5. Customer Relationship Management (CRM)
6. E-Commerce Platforms
7. E-Marketplace
8. Marketing Automation

4.2.3.2 Spotlight Building Block: Public Financial Management Systems

Public financial management (PFM) systems allow governments to store, present, and share financial data (e.g. budget allocations, expenditure records, compliance certificates) under their sovereign control.⁸³ They can include both parts of the broader systems and more integrated solutions covering a range of solutions, such as the integrated financial management information systems (IFMIS).⁸⁴ In practice, such technologies are already being developed (at least in part) through various EU digital government initiatives,⁸⁵ but PFM systems in Europe could be significantly enhanced through coordinated implementation across Member States and common resources and tools to build on.

In the EU, open standards like GovStack,⁸⁶ digital public goods like OpenFisca,⁸⁷ and other open source solutions like TruBudget⁸⁸ offer potential solutions for enabling fiscal management and interoperability. Such technologies might enable streamlined access to EU-wide financial

⁸¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1724>

⁸² <https://joinup.ec.europa.eu/collection/interoperability-test-bed>

⁸³ <https://www.imf.org/en/Publications/WP/Issues/2016/12/31/Public-Financial-Management-and-Its-Emerging-Architecture-26850>

⁸⁴ <https://blog-pfm.imf.org/en/pfmblog/2021/12/digital-public-infrastructure-platforms-and-public-finance>

⁸⁵ <https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/digital-public-administration-factsheets>

⁸⁶ <https://www.govstack.global>

⁸⁷ <https://www.openfisca.org>

⁸⁸ <https://www.trubudget.net>

services and interoperability of financial services,⁸⁹ ranging from (for example) structural fund disbursements to VAT reconciliation without revealing unnecessary fiscal details. For example, an EU Member State could verify budget compliance for EU co-financing without exposing detailed line-item expenditures, or automatically share aggregated revenue data for fiscal surveillance while keeping granular transaction records confidential.⁹⁰

4.2.4 Security Capabilities

The Digital Commons perspective on cybersecurity reframes security in a novel way. It shows that security need not only be treated as a defensive product – to be procured from vendors using black-box approaches and proprietary obscurity. Instead, it views security as potentially open and shared critical infrastructure, dependent on the participation of communities and able to be shaped by principles of collective governance.

4.2.4.1 Example Building Blocks

1. Vulnerability Management
2. Security Information and Event Management
3. Network Security Monitoring
4. Endpoint Protection
5. Password Control
6. Data Loss Prevention (DLP)

4.2.4.2 Spotlight Building Block: Vulnerability Management

Vulnerability management systems provide critical infrastructure for identifying, disclosing, and remediating security flaws across sovereign digital infrastructure, supporting coordinated responses to cybersecurity threats through shared registries of known vulnerabilities, affected components, and mitigation measures. In the EU, such capabilities are supported by platforms like the European Vulnerability Coordination and Disclosure platform under ENISA⁹¹ – as well as the more recently announced EU Vulnerability Database (EUVD)⁹² – and increasingly draw on international standards such as CVE (Common Vulnerabilities and Exposures)⁹³ and OSV (Open Source Vulnerabilities).⁹⁴

By integrating open standards for vulnerability data exchange and disclosure protocols, Member States can enable secure and timely coordination across national Computer Emergency Response Teams (CERTs), software maintainers, and procurement authorities – particularly when dealing with open source components widely deployed across critical systems. Initiatives like OSV.dev and the OpenSSF Vulnerability Disclosure Working Group⁹⁵ could help in these efforts, supporting European implementations that build upon to support trusted and sovereign cybersecurity operations. In this sense, vulnerability management components and systems could help ensure that disclosure workflows, patch notifications, and software bill of materials (SBOMs) are interoperable across borders, reducing risk.

⁸⁹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0134>

⁹⁰ <https://www.oecd.org/digital/digital-economy-outlook-2021.htm>

⁹¹ <https://www.enisa.europa.eu/topics/vulnerability-disclosure>

⁹² <https://euvd.enisa.europa.eu/>

⁹³ <https://www.cve.org/>

⁹⁴ <https://osv.dev/>

⁹⁵ <https://openssf.org/technical-initiatives/vulnerability-disclosures/>

4.2.5 Management and Monitoring Capabilities

Management and Operational Capabilities are similarly easy to conceptualise as Digital Commons Rather than being tools that are consumed as a service, they can become dynamic projects that bring together different functionalities to enable larger-scale use cases.

4.2.5.1 Example Building Blocks

1. Document Management
2. Service Lifecycle Management
3. Monitoring
4. Remote Device Management
5. Operation Management
6. Workflow

4.2.5.2 Spotlight Building Block: Document Management

Document management systems enable public administrations to create, store, access, and share official documents. These systems enable information governance, records retention, digital archiving, and collaborative workflows, ensuring that official documents are traceable, versioned, and legally compliant throughout their lifecycle. Such capabilities are increasingly central to digital government initiatives, particularly as Member States modernise administrative processes and adopt paperless workflows in line with the Single Digital Gateway Regulation,⁹⁶ eIDAS⁹⁷ frameworks, and others.

Open standards such as PDF/A⁹⁸ for archiving and XML-based formats like UBL⁹⁹ are already widely used for document exchange, while open source tools like Alfresco,¹⁰⁰ ONLYOFFICE,¹⁰¹ and Nextcloud¹⁰² provide reusable and customisable platforms for secure document management in the public sector. The Interoperability Test Bed¹⁰³ and SEMIC¹⁰⁴ support cross-border document metadata harmonisation, ensuring that records can be correctly interpreted across Member States. Coordinated support for open source document management systems could support digital sovereignty by providing secure, standards-based tools for recordkeeping, collaboration, and compliance, without locking public administrations into proprietary formats or vendor-specific platforms.¹⁰⁵

4.2.6 Operational Capabilities

A Digital Commons approach to software development might think of contribution to and adoption of software development tools in a novel way. It shows they need not only be treated as engineering products – to be procured from vendors using siloed approaches and

⁹⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1724>

⁹⁷ <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>

⁹⁸ <https://en.wikipedia.org/wiki/PDF/A>

⁹⁹ <https://www.storecove.com/blog/en/what-is-ubl/>

¹⁰⁰ <https://www.alfresco.com>

¹⁰¹ <https://www.onlyoffice.com>

¹⁰² <https://nextcloud.com>

¹⁰³ <https://joinup.ec.europa.eu/collection/interoperability-test-bed>

¹⁰⁴ <https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic>

¹⁰⁵ <https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/dms-open-source-eu>

proprietary constraints. Instead, it views them as shared resources that can support skills development, capacity-building, and engineering across large sections of society.

4.2.6.1 Example Building Blocks

1. Container Management
2. API Gateway/Data Exchange Layers
3. Information Mediation DevOps
4. Software Development Tools/Suites
5. Project Management
6. Workflow Automation / Scheduler
7. Low-Code Platforms
8. No-Code Platforms
9. Server Control Panels
10. Developer Environment

4.2.6.2 Spotlight Building Block: Container Management

Container Management systems provide the operational backbone for deploying, scaling, and maintaining applications across diverse infrastructure environments.¹⁰⁶ These systems allow applications and their dependencies to be packaged and executed in isolated, reproducible environments, increasing reliability, portability, and security. In the EU, container technologies are already being used to support cloud-native architectures under initiatives like the European Alliance for Industrial Data, Edge and Cloud, and are key enablers for interoperability across Member State infrastructure service.¹⁰⁷

By standardising how public services are deployed and orchestrated using container platforms such as Kubernetes,¹⁰⁸ European governments can ensure that software components – from e-government portals to open source registries – are modular, maintainable, and compliant with cybersecurity and data residency requirements. Reusable container management capabilities could offer building blocks for secure deployment pipelines, policy enforcement, and service federation across jurisdictions. Additionally, emerging standards for software supply chain security – such as Supply-chain Level for Software Artifacts (SLSA)¹⁰⁹ and the Open Container Initiative (OCI)¹¹⁰ – help ensure containers are verifiable, auditable, secure, and free from tampering.

4.3 ACCESS AND INTERACTION LAYER

The Interaction and Access Layers of sovereign digital infrastructure represent the public-facing interfaces through which citizens, businesses, and institutions directly engage with digital services and participate in the digital economy. This includes capabilities such as communications and collaboration, web technologies, and domain-specific applications.

¹⁰⁶ <https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/containers-and-kubernetes>

¹⁰⁷ <https://digital-strategy.ec.europa.eu/en/policies/european-cloud-federation>

¹⁰⁸ <https://kubernetes.io/>

¹⁰⁹ <https://slsa.dev>

¹¹⁰ <https://opencontainers.org/>

These layers are where digital sovereignty becomes most tangible to everyday users, as they determine whether citizens interact with their digital environment through foreign-controlled platforms or through locally-governed, rights-respecting alternatives. By ensuring that these user-facing capabilities are built on Digital Commons principles, the EU can offer citizens meaningful choice and control over their digital experiences while reducing dependency on extractive platform models. These layers are essential for autonomy resilience, as they enable public discourse, civic participation, and cultural expression to occur within digital spaces that reflect European values of openness, interoperability, and user empowerment.

4.3.1 Communications and Collaboration Capabilities

Digital Commons thinking might consider communications and collaboration not as secondary IT functions or consumer-grade conveniences, but as foundational public capabilities essential to democratic governance, institutional coordination, and civic participation. In this light, messaging systems, videoconferencing platforms, decentralised social networks, and collaborative editing tools are not simply utilities, they are enablers of participatory models for contribution and governance.

4.3.1.1 Example Building Blocks

1. Decentralised Social Media
2. Messaging
3. Video Conferencing
4. Peer-to-Peer (P2P) Encryption
5. Email Server

4.3.1.2 Spotlight Building Block: Decentralised Social Media

Decentralised social media platforms and systems allow public discourse to occur through open, federated networks rather than centralised commercial platforms. These platforms, built on protocols like ActivityPub,¹¹¹ enable users and institutions to maintain control over their data and online interactions, ensuring alignment with European digital values such as privacy, interoperability, and autonomy.¹¹² Platforms like Mastodon and PeerTube represent leading examples of this shift, offering alternatives to dominant corporate platforms such as X (formerly Twitter), YouTube, and Instagram.¹¹³

In this way, decentralised social media directly supports the EU's goals of technological sovereignty, democratic resilience, and data protection, aligning with frameworks such as the Digital Services Act, the Digital Markets Act, and the Declaration on European Digital Rights and Principles.¹¹⁴ A bundled Fediverse offering would provide not just alternatives to platform capitalism, but a means of reclaiming public space online, where terms of engagement are defined transparently and openly. European institutions, public broadcasters, and civil society organizations increasingly experiment with federated platforms to host communication on their own infrastructure, reducing dependency on foreign platforms. For example, German public

¹¹¹ <https://www.w3.org/TR/activitypub/>

¹¹² <https://digital-strategy.ec.europa.eu/en/policies/digital-principles>

¹¹³ <https://www.france24.com/en/europe/20221109-fediverse-mastodon-peertube-europe-digital-sovereignty>

¹¹⁴ <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>

broadcasters maintain their own Mastodon instances,¹¹⁵ and European research networks like GÉANT¹¹⁶ support open federated platforms for academic use.

4.3.2 Web Technologies Capabilities

The Digital Commons perspective reframes web technologies not as mere delivery mechanisms for static content or marketing tools. When developed and maintained as commons, tools like content management systems, static site generators, web analytics platforms, and knowledge management platforms become critical digital infrastructure through which public institutions interact with citizens, deliver services, and build trusted information environments.

4.3.2.1 Example Building Blocks

1. Content Delivery Network (CDN)
2. Knowledge Management Platforms
3. Live Video Streaming
4. Web Analytics Platforms
5. Static Site Generator
6. Content Management System
7. Social Media Management
8. URL Shortening
9. Domain Registration

4.3.2.2 Spotlight Building Block: Content Delivery Networks

Content Delivery Networks (CDNs) are distributed systems that optimise the delivery of digital content – such as websites, software updates, and media – by caching data across a geographically dispersed network of servers.¹¹⁷ They are essential for ensuring that public digital services are fast, reliable, and accessible regardless of a user's location. In Europe, CDNs play a critical role in reducing latency and bandwidth strain for pan-European services such as e-government portals, education platforms, public health dashboards, and others. They also help improve resilience during periods of peak demand or network disruption by dynamically routing content through alternative nodes.¹¹⁸

As public sector services increasingly rely on dynamic web applications and open source infrastructure, European governments must consider how CDN capabilities are provisioned, particularly in relation to questions around sovereignty and data localisation. Reusable CDN components could be developed or federated to provide secure, standards-based content distribution under public governance. Open source initiatives such as Apache Traffic Server¹¹⁹ and the OpenCDN¹²⁰ specification offer technical starting points for Member States or trusted consortia to develop CDN infrastructure aligned with EU values and regulation.

¹¹⁵ <https://social.bund.de/@ARD>

¹¹⁶ <https://connect.geant.org>

¹¹⁷ <https://www.cloudflare.com/learning/cdn/what-is-a-cdn/>

¹¹⁸ <https://www.enisa.europa.eu/publications/content-delivery-networks-cdns>

¹¹⁹ <https://trafficserver.apache.org/>

¹²⁰ <https://opencdn.nic.br/en/>

4.3.3 Domain-Specific Applications and Services Capabilities

The Digital Commons perspective reframes domain-specific applications not as isolated vertical solutions or commercial off-the-shelf products, but as modular, interoperable building blocks of digital public infrastructure. These capabilities – ranging from e-government portals and digital health platforms to educational systems, participatory budgeting tools, and cooperative marketplace – represent essential interfaces between institutions and citizens.

4.3.3.1 Example Building Blocks

1. Office Suites
2. Public Health Systems
3. E-Government Portals
4. Education Platforms
5. Wiki Software
6. Open Educational Resources
7. Digital Archive Software
8. Platform Cooperatives
9. Crowdfunding
10. Health and Fitness

4.3.3.2 Spotlight Building Block: Office Suites

Open alternatives to Office Suites allow organisations to manage their own digital infrastructure and data by using locally hosted, open source tools for workspaces, rather than relying on the largest technology providers. Platforms like Nextcloud, Matrix, and OnlyOffice¹²¹ empower European institutions to govern communications, file storage, and collaborative workflows, ensuring compliance with EU data protection laws and preserving digital sovereignty. Leading options – including Nextcloud Hub¹²² and ONLYOFFICE Workspace¹²³ – offer robust alternatives to dominant services like Microsoft 365 and Google Workspace.

Governments are already stepping in too; efforts are already underway in European Member States like France and Germany and could be scaled. The efforts in the Digital Commons EDIC are revealing in this regard, promising a version of open source collaboration on specific projects as commons, like the Sovereign Digital Workplaces.¹²⁴ This is being piloted through the EDIC as an effort to formalise the collaboration already happening between Germany's *OpenDesk*¹²⁵ and France's *La Suite numérique*,¹²⁶ which just released a new open source document editor called *Docs* in a pilot phase.¹²⁷

¹²¹ <https://www.onlyoffice.com/>

¹²² <https://nextcloud.com/hub/>

¹²³ <https://www.onlyoffice.com/workspace.aspx>

¹²⁴ <https://www.digitalsme.eu/events/tech-solutions-made-in-europe-building-a-sovereign-digital-workplace/>

¹²⁵ <https://www.opendesk.eu/de>

¹²⁶ <https://lasuite.numerique.gouv.fr/en>

¹²⁷ <https://news.itsfoss.com/la-suite-numerique-docs/>

4.4 NON-TECHNICAL LAYER

A major outcome of the workshops that produced this brief was the recognition that just like with Digital Commons, technical Building Blocks must be complemented by supporting communities and open governance models. Therefore, a focus on technical Building Blocks alone would be insufficient. Instead, it is necessary to also prioritise non-technical Building Blocks, together which support the realisation of embedding Digital Commons principles into European policymaking. Technical Building Blocks alone would risk recreating some of the very issues – such as extractive value creation and lock-in on to a different set of stakeholders – that the movement towards Digital Commons in EU policymaking has highlighted as concerns.

In this sense, infrastructure is only as strong as its stewards – the human capacity and communities that enable those infrastructures. Building Blocks must be embedded within communities and governance logics that support maintenance, capacity-building, and contributor sustainability. Resources, tools, and solutions in these areas can be made to be reusable across domains, and many are built on OSS, open standards, open content, and so on. Such Building Blocks would help to ensure long-term operational capacity and support sustainable involvement of the people and practices that media interaction, participation, and use of them, which is vital at the scale of ambition one imagines when the EU talks about sovereign digital infrastructure.

4.4.1 Community Capabilities

Infrastructures are more than code, but also social systems underpinned by communities and specific governance models which reflect those communities. There must therefore be Building Blocks which bring the community in and help define how decisions are made, who has voice, and how conflicts are resolved. Building such frameworks, tools, and solutions into repeatable, open models would align public interest goals with the operational realities of Digital Commons-style principles of openness and collaboration. They should function as reusable patterns for establishing democratic control over digital public infrastructure, especially when managed through networks of municipalities, public administrations, or transnational alliances.

4.4.1.1 Example Building Blocks

1. Civic Assembly Frameworks
2. Community Governance Templates
3. Participatory Budgeting Tools
4. Federated Community Forums
5. Decision Logs
6. Community Moderation Guidelines
7. Conflict Resolution Toolkits
8. Public Sector–Commons Partnership Agreements
9. Cross-Jurisdictional Municipal Alliance Templates

4.4.1.2 Spotlight Building Block: Civic Assembly Frameworks

Citizen assembly frameworks offer structured approaches for embedding deliberative democracy and inclusive community participation into the governance of digital infrastructure. Rooted in traditions of participatory decision-making, these frameworks bring together diverse

stakeholders to co-create policies, prioritise public investments, and resolve conflicts.¹²⁸ When applied to digital systems, citizen assemblies help ensure that governance is not limited to technical experts or institutional actors, but instead reflects the plural interests and values of the communities those systems serve.¹²⁹ They help translate public interest goals into concrete decision-making structures and protocols, offering a democratic scaffolding for managing shared digital infrastructure across jurisdictions.¹³⁰

One such example of a citizen assembly frameworks, Metadecidim¹³¹ is the meta-community and governance layer of the Decidim project. It functions as an open and participatory space where contributors, users, institutions, and researchers collectively shape the evolution of the platform. Unlike Decidim's core digital infrastructure, Metadecidim functions as a democratic forum for deliberation, conflict resolution, roadmap co-design, and community accountability. As such, it serves as a compelling example of the principles of community assembly frameworks that embeds community participation directly into the governance of digital public infrastructure.¹³²

4.4.2 Legal Capabilities

To support legal clarity and cross-border interoperability, there must be reusable legal Building Blocks that enable reliable, standardised models for collaboration, governance, and compliance. Such legal tooling is critical not only for protecting digital commons from enclosure or misuse, but also for enabling the local adaptation of digital infrastructure without unnecessary legal complexity. By providing resources or solutions such as model clauses, template contracts, and standard terms as Building Blocks, it will be possible to help public administrations and other public interest organisations to adopt open source solutions with legal confidence. This would reduce transaction costs and ensuring alignment with EU legal frameworks such as the GDPR, the Digital Markets Act,¹³³ or the Data Governance Act.¹³⁴

4.4.2.1 Example Building Blocks

1. Public Procurement–Compatible Licensing Templates
2. Open Source Licensing Suites
3. Contributor License Agreements
4. Developer Certificates of Origin
5. Data Trust Governance Clauses
6. Ombuds or Complaint Handling Procedures
7. Model Contracts for Commons-Based Commissioning
8. Terms of Use

¹²⁸ <https://www.oecd.org/governance/innovative-citizen-participation-and-new-democratic-institutions-339306da-en.htm>

¹²⁹ <https://www.newamerica.org/digital-impact-governance-initiative/collections/infrastructure-for-the-digital-age/digital-participation-infrastructure/>

¹³⁰ <https://www.noemamag.com/a-movement-thats-quietly-reshaping-democracy-for-the-better/>

¹³¹ <https://metadecidim.org>

¹³² <https://www.oidp.net/docs/repo/doc1488.pdf>

¹³³ https://digital-markets-act.ec.europa.eu/index_en

¹³⁴ <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>

4.4.2.2 Spotlight Building Block: Public Procurement–Compatible Licensing Templates

Public procurement–compatible licensing templates offer a foundational legal Building Block for enabling the adoption of open source solutions within public administrations. Templates like these might provide public sector entities with standardised, vetted tools for releasing, modifying, or integrating OSS into digital infrastructure.¹³⁵ By aligning licensing terms with principles of openness, transparency, and reusability, they reduce legal ambiguity and lower the barriers to adopting Digital Commons infrastructure within formal institutional contexts. When embedded in broader digital strategies, these templates can serve as reusable legal infrastructure, ensuring that open source solutions meet both the legal and operational requirements of governments.

One such example is the European Union Public Licence (EURL), which was the first open source licence drafted and approved by an EU institution, specifically tailored to the needs of European public administrations.¹³⁶ Fully compatible with EU law and available in 23 official languages, the EURL was developed to be interoperable with other major open source licences, while ensuring enforceability in a European legal context.¹³⁷ It is expressly designed for use in public sector software distribution and reuse, and has been adopted by multiple EU institutions, national governments, and municipalities for open sourcing public sector digital tools. The EURL provides a clear and widely accepted model for licensing public code that can be reused, adapted, and shared across Member States, embodying the principles of open, commons-based infrastructure while enabling legal certainty for public entities.¹³⁸

4.4.3 Funding Capabilities

To support the long-term sustainability of Digital Commons, it is important for there to be reusable funding toolkits that enable stable, coordinated, and scalable support for open digital infrastructure. Financial tooling is essential for maintaining critical components beyond the lifespan of short-term grants. By providing resources like maintainer subsidies, pooled procurement consortia, or shared financing mechanisms, it would help shift public institutions away from short-term, project-based procurement when looking at the development of sovereign digital infrastructure. This would support lifecycle funding approaches and ensure alignment with the broader principle of treating digital infrastructure as a public good.

4.4.3.1 Example Building Blocks

1. Procurement Consortia
2. Maintenance Subsidy or Payment Schemes
3. Stewardship-as-a-Service Contracts
4. Crowdfunding Platforms
5. Open Source Endowments
6. Cooperative Funding Platforms
7. Incentive Models for Multi-Stakeholder Co-Funding
8. Lifecycle-Based Procurement Frameworks

¹³⁵ <https://joinup.ec.europa.eu/collection/open-source-observatory-osor/licensing>

¹³⁶ <https://joinup.ec.europa.eu/collection/eupl/eupl-text-eupl-12>

¹³⁷ <https://opensource.org/license/eupl/>

¹³⁸ <https://joinup.ec.europa.eu/collection/open-source-observatory-osor/eupl-use-cases>

4.4.3.2 Spotlight Building Block: Procurement Consortia

Procurement consortia offer a means of scaling the adoption and sustainability of open solutions, particularly OSS, across public administrations.¹³⁹ These consortia reduce duplication, improve negotiating power, and create incentives for modular, reusable solutions aligned with Digital Commons principles. This can help public administrations avoid vendor lock-in, ensure long-term maintainability of commons, and promote interoperability across jurisdictions.¹⁴⁰ Such consortia can serve as reusable governance and procurement frameworks, supporting public sector collaboration while aligning procurement practices with the goals and strategic objectives of the EC and its Member States.

One example is OS2,¹⁴¹ a Danish association of more than 80 municipalities that jointly procure, govern, and maintain open source digital solutions for the public sector. Rather than procuring tools independently, OS2 members co-develop shared software solutions through transparent governance structures and co-financing arrangements. This collaborative model has led to the sustained use and evolution of multiple open source tools for citizen services, case management, and administrative workflows.¹⁴² OS2 exemplifies how procurement consortia can enable public sector actors to move beyond project-based procurement toward commons-based infrastructure investment.

4.4.4 Governance Capabilities

Layered governance ensures accountability, participation, and adaptability over time. Governance capabilities provide meta-structures that guide how Building Blocks are maintained, updated, and governed over their lifecycle. They include mechanisms for multi-stakeholder input, transparency in decision-making, and institutional legitimacy in public-commons partnerships. Governance resources, solutions, and tooling should reflect modularity and subsidiarity – allowing different actors to assume roles appropriate to their scale and capacity. These structures also facilitate alignment with EU-wide digital policy goals while respecting the autonomy of local or sector-specific implementations, in line with Digital Commons ideals and principles

4.4.4.1 Example Building Blocks

1. Public-Commons Partnership Charters
2. Governance Charters
3. Role-Based Governance Models
4. Cross-Institutional Stewardship Bodies
5. Audit and Accountability Toolkits
6. Governance Lifecycle Frameworks
7. Adaptive Governance Protocols

4.4.4.2 Spotlight Building Block: Public–Commons Partnership Charters

Public-commons partnership charters represent a governance-oriented Building Block for structuring long-term collaboration between public institutions and digital commons

¹³⁹ <https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/municipal-consortia-and-open-source>

¹⁴⁰ https://ec.europa.eu/info/policies/public-procurement_en

¹⁴¹ <https://www.os2.eu/english>

¹⁴² <https://joinup.ec.europa.eu/news/denmark-os2-shares-code-and-know-how>

communities.¹⁴³ By embedding mutual accountability, transparency, and shared decision-making into formal agreements, they enable sustainable co-management of digital tools, data infrastructure, or platforms that serve a public interest function.¹⁴⁴ A public-commons partnership charter could be valuable for bridging legal and operational gaps between informal community-led initiatives and formal public sector processes.

One example is the Public-Commons Partnership Charter proposed by the Decidim community, which outlines how public administrations and civic actors can jointly govern digital platforms in line with democratic, participatory, and commons-based principles.¹⁴⁵ Developed collaboratively by the Decidim ecosystem, the charter includes commitments to transparency, co-decision, shared investment, and non-extractive licensing models. It serves as a working model for institutionalising collaborative governance at the interface of municipalities and digital commons communities.

4.4.5 Skills and Capacity-Building Capabilities

Deploying a sovereign digital infrastructure depends on robust capacity-building mechanisms that ensure those responsible for deploying, maintaining, and evolving its components have the skills, resources, and institutional support required over time. These mechanisms form a foundational layer of the stack, encompassing modular training pathways, peer learning infrastructures, and recognition systems that foster both technical proficiency and long-term engagement. Such capacity-building structures enable not just digital upskilling, but the development of resilient, self-sustaining ecosystems of practice around each Building Block.

4.4.5.1 Example Building Blocks

1. Open Learning Curricula
2. Learning Management Systems
3. Modular Training Curriculum
4. Federated Skills Registries
5. Contributor Databases
6. Institutional Liaisons
7. Public Sector–Commons Apprenticeship Tracks
8. Certification and Microcredential Systems
9. Career Pathway Frameworks

4.4.5.2 Spotlight Building Block: FOSS4GAcademy

Open learning curricula represent a potential capacity-building Building Block for equipping public institutions, communities, and contributors to support sovereign digital infrastructure. These curricula offer structured, accessible pathways for digital upskilling, policy literacy, and commons-based stewardship across different roles and technical levels.¹⁴⁶ By aligning with open standards and fostering collaboration between public administrations, academic

¹⁴³ <https://commonstransition.org/public-commons-partnerships-enabling-institutional-innovation-in-the-public-sector/>

¹⁴⁴ <https://www.decidim.org/blog/en/2022/02/22/the-commons-and-the-city/>

¹⁴⁵ https://metadecidim.s3.amazonaws.com/uploads/decidim/attachment/file/1001/Public-Commons_Partnership_-_Proposal.pdf

¹⁴⁶ <https://fsfe.org/activities/education/education.en.html>

institutions, and open source communities, open learning curricula enable distributed learning ecosystems tailored to the needs of public interest technology.¹⁴⁷

One example is the FOSS4G Academy,¹⁴⁸ a global initiative that provides openly licensed geospatial curricula developed in collaboration with OSGeo, universities, and public agencies (source). Delivered through modular courses, hands-on labs, and international collaborations, the FOSS4G Academy supports learners in acquiring practical and theoretical knowledge around Free and Open Source Software for Geospatial applications. Its materials are designed for integration into formal education systems as well as professional training environments, making it a flexible resource for both academic and governmental institutions.¹⁴⁹

4.5 FUNCTIONAL LAYER

The Functional Layer is cross-cutting and can help in identifying Building Blocks aligned with expressed EU values and policy priorities. This layer represents the EU policy context and is not a grouping of Building Blocks so much as it is values by which the EC can use to help prioritise Building Blocks which enable or help in the achievement of those attributes. In this regard, the Functional Layer is critical for understanding how the other layers contribute to a European vision for sovereign digital infrastructure, including that currently posed by the EC DG-CNECT as part of the OIS. In this sense, these layers do not operate in isolation but work together to create a cohesive framework.

The Functional Layer include capabilities such as:

1. **Trust** underpins all other layers, supporting authentication, security, and reliability across the stack.
2. **Transactions** provide the mechanisms for value exchange, contracts, and financial interactions.
3. **Connectivity** ensures physical and network infrastructure can support digital services.
4. **Decentralisation** distributes control and reduces dependencies on centralised systems.
5. **Interoperability** enables different systems and components to work together seamlessly
6. **Governance** provides the frameworks for maintenance, decision-making, and sustainability.

¹⁴⁷ <https://opensource.com/article/17/6/geospatial-foss4g-academy>

¹⁴⁸ <https://foss4gacademy.org>

¹⁴⁹ <https://www.osgeo.org/initiatives/geo-for-all/>

5 FROM MAPPING TO IMPLEMENTATION

As Europe enters a new phase of digital sovereignty policymaking, integrating Digital Commons should remain a priority for the EC and Member States alike. Digital Commons a strategic opportunity to ground Europe's sovereign digital infrastructure initiatives in open, interoperable, and collectively governed technologies. While this vision is still being elaborated, we hope the contents of this brief will provide a first step to the EC in thinking about how to identify Building Blocks in key areas of capabilities across different layers of the stack, as well as match them with communities, governance models, and other resources that enable them to succeed.

Moving forward, it is imperative that OSS – and other open technologies leveraged – remain grounded in ideas of Digital Commons. This means extending our understanding beyond technical artefacts like code or open source licensing to include community participation and open governance. There should be means in place to ensure that the development model remains non-extractive, leverages inclusive participation, supports the development of vibrant communities, and includes highly open governance models.

5.1 PRIORITIES FOR IMPLEMENTATION OF A DIGITAL COMMONS-BASED APPROACH TO BUILDING BLOCKS

As the EC seeks to operationalise such an approach for its OIS, the following considerations emerge as key priorities for ensuring the Digital Commons agenda remains centred. These priorities are drawn directly from the workshops and community engagement activities undertaken by the NGI Commons consortium in Spring 2025.

5.1.1 Priority #1: Establish Collaborative Governance Mechanisms for Digital Commons Communities

The EC should play an active enabling role in the creation and maintenance of formal communities of practice and collaborative governance mechanisms that meaningfully involve Digital Commons communities – particularly the open source ecosystem – in the co-design and development of the OIS and the Building Blocks that comprise it. This requires moving beyond traditional procurement models to embrace participatory design processes that include community representatives in technical advisory boards, funding decision committees, and implementation oversight groups. By embedding Digital Commons communities as genuine partners rather than service providers, the EU can ensure the OIS reflects the collaborative values and technical excellence that have made OSS a cornerstone of global digital infrastructure.

5.1.2 Priority #2: Define Strategic Roles and Responsibilities for Telecommunication Providers

The EC must clearly articulate the role of telecommunication providers within the proposed OIS, establishing whether they will serve as infrastructure enablers, service integrators, or collaborative partners in the broader digital sovereignty ecosystem. This clarification should address how traditional telecom operators will interact with specific capabilities and Building Blocks, particularly for the Foundation Layers of the stack. The OIS framework should establish clear boundaries between telecom infrastructure and open components of the OIS, ensuring that commercial interests do not compromise the stack's openness and interoperability goals.

5.1.3 Priority #3: Adopt a Digital Commons Readiness Assessment Framework for the Open Internet Stack

The first step in realising a Digital Commons-based approach is to define what qualifies as a suitable Building Block for European digital infrastructure. As a result, the EC should adopt a Digital Commons Readiness Assessment Framework that evaluates candidate technologies not only for openness (e.g. licensing) but also for community governance, maintenance models, interoperability, and non-extractive practices.¹⁵⁰ Such considerations must also be considered as new technologies and functionalities are bundled together into larger projects, like Sovereign Digital Workspaces, which themselves function as a sort of Digital Commons.

5.1.4 Priority #4: Update and Refine a Typology of Digital Commons-Based Building Blocks

The taxonomy presented in Section IV categorises capabilities as a way of identifying Building Blocks, demonstrating their natural alignment with Digital Commons. This typology should now be updated and validated through co-creation with Member States, civil society, and – perhaps most importantly – open technical communities represented by people involved in open source and Digital Commons projects. Without this, EU investments risk reproducing extractive models that have characterised much of digital infrastructure investment and undermine the very forms of openness and sovereignty they aim to achieve.

5.1.5 Priority #5: Engage in Dialogue

The EC should prioritise dialogue between public institutions and EU Member States to help them contribute and become effective stewards of Building Blocks-based infrastructure. Commons-literate institutions will be critical not only to implement OIS effectively, but to ensure that Digital Commons logic – openness, collaboration, and shared stewardship – extends across Europe's sovereign digital infrastructure ecosystem. In this sense, the Digital Commons EDIC will be a crucial vehicle for continuing to engage with Member States and opening up new conversations around the possibility of Building Blocks for sovereign digital infrastructure. Moreover, the EC should also continue to engage in dialogue with the ecosystem of commoners supported by the NGI and NGI Commons programmes, and in particular continue to engage with the open source community.

5.2 PRIORITISING BUILDING BLOCKS FOR EUROPEAN SOVEREIGN DIGITAL INFRASTRUCTURE

Based on the extensive analysis presented, the following seven Building Blocks stand out as possibly the most relevant for provisioning sovereign digital infrastructure through the OIS. Each represents a foundational capability with strategic relevance, operational maturity, and clear alignment with Digital Commons principles and functional layers. Below is a short analysis of each. This analysis should not be treated as final or conclusive, but as a starting point for further dialogue, engagement, and conversation.

5.2.1 Priority Building Block #1: Cloud Storage

Cloud storage underpins nearly every modern digital service. Sovereignty over storage infrastructure is critical to ensuring that European data – including that of citizens, public institutions, and strategic industries – remains under EU jurisdiction and beyond the reach of

¹⁵⁰ Note: Meeting any of these criteria individually need not necessarily be a binary, and something should not necessarily be excluded on the basis of one criteria alone.

foreign surveillance laws (e.g. U.S. CLOUD Act). Cloud storage is also a key enabler for emerging domains like AI, edge computing, and smart cities, and forms the backbone of federated public sector IT services.

5.2.2 Priority Building Block #2: Digital Wallets

Digital Wallets are the cornerstone of Europe's ambitions around eIDAS 2.0 and digital identity sovereignty. They support citizen control over personal data, cross-border authentication, and secure delivery of public and private services. When built on open standards, they allow identity systems to reflect European values such as privacy, decentralised governance, and interoperability.

5.2.3 Priority Building Block #3: Vulnerability Management

Security is a precondition for trust in digital infrastructure, and vulnerability management systems are essential for safeguarding sovereign systems. Without visibility into and coordination of responses to vulnerabilities – especially in open source components – the EU remains exposed to systemic risk, particularly across critical sectors like health, finance, and public administration.

5.2.4 Priority Building Block #4: Decentralised Communication Protocols

Decentralised communication protocols like Matrix and ActivityPub enable federated communication systems that break the dependence on foreign-controlled platforms such as WhatsApp, Slack, or X (formerly Twitter). These open protocols underpin sovereign alternatives for secure public sector messaging, civil society coordination, and democratic discourse, all while ensuring alignment with EU privacy and data protection laws.

5.2.5 Priority Building Block #5: Digital Registries

Digital registries form the backbone of public administration, from population and land registries to tax and social security records. As core enablers of cross-border services, harmonised and sovereign registries are essential for compliance with GDPR, the Single Digital Gateway Regulation, and the European Interoperability Framework. Digital registries must be transparent, legally robust, and technically interoperable to serve their public function effectively.

5.2.6 Priority Building Block #6: Civic Assembly Frameworks

Sovereign infrastructure is not just technical – it must reflect the values and democratic governance models of the society it serves. Civic assembly frameworks bring participatory democracy into the governance of digital infrastructure, ensuring legitimacy, accountability, and responsiveness to public needs. Initiatives like Metadecidim provide working examples of such frameworks, embedding citizens directly into decision-making about public digital platforms.

5.2.7 Priority Building Block #7: Public–Commons Partnership Charters

Public–commons partnerships formalise collaboration between institutions and Digital Commons communities, balancing the need for institutional legitimacy with the openness and adaptability of community governance. These charters create frameworks for co-decision, shared investment, and long-term sustainability, which are essential for institutionalising commons-based digital infrastructure in Europe.

6 CONCLUSION

Based on the comprehensive analysis presented in this brief, the transition from NGI to the OIS represents a pivotal moment for European digital sovereignty. The Building Blocks taxonomy outlined here offers a structured pathway for operationalising Digital Commons as the foundation of Europe's sovereign digital infrastructure. By categorising capabilities across Foundational, Intermediation, Interaction and Access, Non-Technical, and Functional layers, this taxonomy provides policymakers with a concrete methodology for identifying, prioritising, and investing in commons-based solutions that align with European values of openness, interoperability, and democratic governance. The taxonomy's emphasis on both technical and non-technical Building Blocks recognises that sustainable digital sovereignty requires not just technological solutions, but also the communities, governance models, and capacity-building mechanisms that enable their long-term success.

The urgency of this moment cannot be overstated. As Europe faces mounting geopolitical uncertainties and growing dependencies on foreign digital infrastructure, the window for building truly sovereign alternatives is narrowing. However, this challenge also presents an unprecedented opportunity for the EU to demonstrate global leadership in developing open, rights-respecting digital infrastructure that can serve as a model for other regions. Success will require sustained commitment to the Digital Commons ecosystem, strategic coordination between public and private sectors, and continued investment in the human capacity that underpins these technologies. By embracing the Building Blocks approach outlined in this brief, Europe can move beyond rhetorical commitments to digital sovereignty and instead create a tangible, replicable approach to provisioning digital infrastructure that truly serves the public interest while strengthening Europe's position in an increasingly digital world.