Digital Sovereignty and Trust in European Public Services: A Mixed-Methods Study on the Adoption of Sovereign Cloud Infrastructure

Jan Maximilian Nour El Nayal

Dissertation written under the supervision of Professor Peter V. Rajsingh.

Dissertation submitted in partial fulfilment of requirements for the MSc in International Management at the Universidade Católica Portuguesa, 04.01.2026

Abstract

The pursuit of "Digital Sovereignty" has evolved from a regulatory preference to a constitutional necessity for European states, driven by geopolitical instability and the legal risks of extraterritorial surveillance. To maintain legitimacy, public administrations must navigate a critical trade-off: securing jurisdictional immunity for data while delivering the seamless, high-performance digital services citizens expect. However, current strategies often rely on a compliance-first approach that risks degrading service utility.

This study employed a mixed-methods approach, including 12 expert interviews and a survey of 242 European citizens, to investigate the drivers of Sovereign Cloud adoption. The findings revealed a "Sovereignty Paradox": perceived sovereignty drives institutional trust but is insufficient to drive adoption. The results also identified an "Orchestration Gap," where the state possesses the legal asset of sovereignty but lacks the dynamic capability to deploy it effectively. Consequently, citizens perceive a "Sovereignty Tax," a trade-off in which increased security comes at the expense of lower performance. The study concluded that for the state to resolve this dilemma, sovereignty must be redefined from a static legal status to a dynamic operational capability, ensuring that digital independence does not come at the cost of public value.

Keywords: Digital Sovereignty, Cloud Computing, Public Administration, Trust, Technology Adoption, Dynamic Capabilities, Resource-Based Theory.

Title: Digital Sovereignty and Trust in European Public Services: A Mixed-Methods Study on the Adoption of Sovereign Cloud Infrastructure

Author: Jan El Nayal

Resumo

A procura pela soberania digital evoluiu de uma preferência regulatória para uma necessidade constitucional para os Estados europeus, impulsionada pela instabilidade geopolítica e pelos riscos legais de vigilância extraterritorial. Para manter a legitimidade, as administrações públicas devem gerir um compromisso crítico: garantir a imunidade jurisdicional dos dados e, simultaneamente, oferecer os serviços digitais de alto desempenho que os cidadãos esperam. No entanto, as estratégias atuais baseiam-se frequentemente numa abordagem de estrita conformidade, o que corre o risco de degradar a utilidade do serviço.

Este estudo adota uma abordagem de métodos mistos, com 12 entrevistas a especialistas e um inquérito a 242 cidadãos europeus, para investigar os fatores que impulsionam a adoção da nuvem soberana. Os resultados revelam um "Paradoxo da Soberania": embora a soberania percebida aumente significativamente a confiança institucional, por si só ela é insuficiente para garantir a adoção. O estudo identifica uma "Lacuna de Orquestração", em que o Estado possui o ativo legal da soberania, mas carece da capacidade dinâmica para implementá-la eficazmente. Consequentemente, os cidadãos percecionam uma "Taxa de Soberania", um compromisso no qual o aumento da segurança resulta em menor desempenho. O estudo conclui que, para resolver este dilema, a soberania deve ser redefinida de um estatuto legal estático para uma capacidade operacional dinâmica, garantindo que a independência digital não seja alcançada à custa do valor público.

Palavras-chave: Soberania Digital; Computação em Nuvem; Administração Pública; Confiança; Adoção Tecnológica; Capacidades Dinâmicas; Teoria Baseada em Recursos.

Título: Digital Sovereignty and Trust in European Public Services: A Mixed-Methods Study on the Adoption of Sovereign Cloud Infrastructure

Autor: Jan El Nayal

Acknowledgments

The completion of this dissertation was made possible by the contributions and support of several individuals to whom I am deeply grateful. I want to extend my sincere appreciation to my supervisor, Professor Peter V. Rajsingh. His constructive criticism, consistent availability, and sharp guidance were pivotal in helping me navigate the theoretical complexities of this research.

I am also indebted to the 12 industry experts who trusted me with their time and candor. Their willingness to discuss the practical realities of the public sector provided the empirical depth this study required. Furthermore, I thank the 242 European citizens who participated in the survey, as well as the colleagues and peers who helped distribute it, allowing me to capture a truly diverse range of perspectives.

On a personal note, I thank my family for their enduring patience and encouragement, which served as my foundation throughout this demanding academic chapter. I am equally grateful to my friends and my girlfriend, Victoria, for their motivation and for providing the necessary balance during this process.

Finally, I value the connections I have made and the experiences I have gained during this program. These interactions have shaped my worldview just as much as the academic curriculum, making this period a defining chapter of my life.

I would also like to acknowledge that selected AI tools were used in accordance with Academic Guidelines to support the efficiency and accuracy of this research. AI was employed for language refinement, specifically for grammar and stylistic suggestions, and to help structure content more clearly. Additionally, AI was used to support the transcription of expert interviews, which were then manually reviewed and revised.

At no point did AI replace the core analytical tasks of conceptual development, critical interpretation, or hypothesis formation, as all intellectual contributions and data evaluations were carried out independently. I recognize the limitations of AI systems, including the potential for inaccuracies and bias, and took care to verify all outputs used. Full responsibility for the content, findings, and conclusions of this dissertation remains with the author.

Jan El Nayal

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
BSI	Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
CIO	Chief Information Officer
CJEU	Court of Justice of the European Union
CoE	Center of Excellence
DC	Dynamic Capabilities
EEA	European Economic Area
EFA	Exploratory Factor Analysis
EU	European Union
FISA	Foreign Intelligence Surveillance Act
GDPR	General Data Protection Regulation
IT	Information Technology
M	Mean
OSI	Online Services Index
PaaS	Platform as a Service
PII	Personally Identifiable Information
RBT	Resource-Based Theory
SaaS	Software as a Service
SCS	Sovereign Cloud Stack
SD	Standard Deviation
UTAUT	Unified Theory of Acceptance and Use of Technology
UX	User Experience
VIF	Variance Inflation Factor
VRIN	Valuable, Rare, Inimitable, Non-substitutable

1. Introduction

President Macron's declaration that "Europe has what it takes to lead the digital age" underscores the EU's strategic ambition to regain technological independence (Bundesregierung, 2025). These words echo similar statements from former German Chancellor Angela Merkel - "Now is the time for Europe to be digitally sovereign" and mark the culmination of a decade-long debate regarding Europe's strategic autonomy (World Economic Forum, 2025). This poses the question: why now?

Amidst growing geopolitical instability, a critical technological dependence has emerged. Leaders such as the United States and China dominate the domains of Cloud and AI, creating a strategic vulnerability for Europe. Legal milestones, including the US CLOUD Act and the Schrems II ruling, have further exposed the risks of relying on non-European infrastructure, pushing "Cloud Sovereignty" to the forefront of the policy agenda (BfDI, 2020). Sovereignty is thus no longer merely a technical specification, but a strategic imperative to ensure that critical data remains secure and subject to European jurisdiction.

However, this imperative creates a dilemma for public administration. As digital public services become the norm, citizens expect the government to deliver seamless, flexible, and cost-efficient services; benefits typically realized through global public cloud solutions (Hinkley, 2023). European governments, therefore, face a dual challenge: they must expand digital services to meet rising performance expectations while simultaneously ensuring that data remains within EU jurisdiction.

Sovereign Cloud solutions appear to satisfy the latter demand by ensuring data residency and enhanced auditability. Yet, these benefits come with trade-offs. Sovereign services are often costlier than global public-cloud offerings and may limit access to the most advanced hyperscaler technologies. As noted by industry analysis, stricter sovereignty controls can lead to higher prices and "waste" if not managed efficiently (Boston Consulting Group, 2025b). This creates a critical uncertainty: does the pursuit of sovereignty ultimately strengthen the digital state by building trust, or does it weaken it by degrading service performance?

To date, Digital Sovereignty has been predominantly framed as an institutional imperative, a matter of state power, legal jurisdiction, and geopolitical resilience. However, this macro-level

discourse often overlooks the citizens' micro-level perspective. This oversight is critical because, ultimately, a sovereign infrastructure is of little value if citizens, the end-users, refuse to adopt it.

While governments do not compete for profits, they must strive for institutional legitimacy and citizen engagement (Moore, 2021). Citizens benchmark public digital services against the seamless experiences offered by the private sector, and the EU monitors this progress closely through the “Digital Decade Reports” (European Commission, 2025). From this perspective, success is defined not just by regulatory compliance, but by willingness-to-use. Despite intense policy debate, there is little empirical evidence on whether Digital Sovereignty serves as a genuine driver of adoption for the average citizen or whether users prioritize performance above all else. Most existing reports describe adoption rates or compliance frameworks but stop short of testing these behavioral outcomes.

To address this gap, this thesis poses the following Research Question: How do perceptions of Digital Sovereignty influence European citizens’ willingness-to-use sovereign digital public services?

To answer this, the study employs a mixed-methods approach, combining expert interviews with a comprehensive survey of European citizens. By testing the direct influence of functional utility (performance) against normative values (sovereignty), this research seeks to determine whether Digital Sovereignty is a valid driver of adoption or merely a political imperative.

2. Literature Review

The digitization of the public sector represents a fundamental shift in the social contract between the state and the citizen (Mergel et al., 2020). Historically, public administration was constrained by physical geography; tax records, health files, and identification documents were stored in physical archives within national borders. Today, governance operates in a digital ecosystem in which data flows instantaneously across jurisdictions, often processed by servers owned by transnational corporations and subject to foreign legal regimes (Mergel et al., 2020). This chapter establishes the theoretical and empirical foundation for investigating the impact of Digital Sovereignty on Public Sector Performance and Citizen Adoption.

The review is structured to provide a comprehensive analysis of the phenomenon. Section 2.1 traces the historical and strategic evolution of Digital Sovereignty, moving from early data protection regulations to the current era of constitutional necessity. Section 2.2 critically examines the technological architecture, contrasting the efficiency of the "global commons" with the security of the "Sovereign Cloud." Section 2.3 dissects the drivers of citizen adoption by integrating the Privacy Calculus Theory (Dinev & Hart, 2006) with the Commitment-Trust Theory (Morgan & Hunt, 1994), identifying trust as the critical mediator of relationship commitment. Finally, Section 2.4 applies Resource-Based Theory (RBT) and Dynamic Capabilities (DC), drawing on Teece (2007), Barreto (2010), and Chen et al. (2024), to explain the organizational mechanisms required to navigate the trade-off between sovereignty and efficiency.

2.1 Digital Sovereignty: From Political Rhetoric to Strategic Imperative

The concept of sovereignty has traditionally been rooted in the Westphalian system of territorial integrity (1648), defined as the state's monopoly over authority within a defined territory. However, the rise of the internet has detached sovereignty from physical borders, creating a new domain of conflict centered on digital infrastructure and data flows (Couture & Toupin, 2019).

2.1.1 Historical Evolution: The Three Waves of European Governance

The European conception of Digital Sovereignty is the result of a long-term legal and geopolitical evolution. This progression can be viewed in three distinct stages:

- **Phase 1 |** Regulatory Era (1995–2013): Europe approached digital governance primarily through a regulatory lens. The Data Protection Directive (95/46/EC) established privacy as a fundamental right but assumed that data could flow freely across borders to "safe" jurisdictions. As noted by Pohle and Thiel (2020), this early stage was characterized by a post-sovereign outlook that prioritized market integration over strict national control.
- **Phase 2 |** The Snowden Catalyst (2013–2018): Edward Snowden's 2013 revelations marked a paradigm shift. The disclosure that US intelligence agencies systematically accessed European data stored in US cloud services, regardless of their physical location, challenged the ideal of a borderless "global internet" (Pohle & Thiel, 2020). This period culminated in the implementation of the General Data Protection Regulation (GDPR) in 2018, which asserted broad extraterritorial scope, requiring any entity that processes the data of EU residents to comply with European standards regardless of where the processing occurs (Celeste, 2021).
- **Phase 3 |** The Constitutional Era (2018–Present): The vulnerability of EU data was legally cemented by the Court of Justice of the European Union (CJEU) in the landmark Schrems II (2020) ruling, which invalidated the "Privacy Shield" agreement. The court found that U.S. surveillance laws (specifically, FISA Section 702) did not provide a level of protection equivalent to that guaranteed under EU law (Hildén, 2021). Consequently, Digital Sovereignty has evolved into a legal necessity. As Celeste (2021) argues, the rationale for Digital Sovereignty lies in the need to preserve the 'European DNA of values and rights'. He contends that, without regaining control over digital assets, European citizens are left at the mercy of foreign technology firms, thereby risking the erosion of fundamental rights.

2.1.2 The Economic Imperative and Strategic Dependency

Beyond the legal imperative, there is a significant economic driver: the European public sector is currently undergoing a massive modernization effort (Bauer et al., 2025). A complete "Cloud-First" implementation could unlock up to €450 billion in annual fiscal savings and productivity gains. Restrictions imposed by the COVID-19 pandemic forced governments to acknowledge the 'necessity' of digital public services (Filip, 2023). This shift led the European Commission to establish digitalization as a primary objective for the current decade, viewing it as essential for ensuring a 'performant digital public administration' (Filip, 2023).

However, this value is currently primarily captured by non-European actors. As of 2020, non-European servers hosted about 80 per cent of European Data (Rone, 2024). This creates a "strategic dependency" in which European governments rely on foreign infrastructure for critical state functions, rendering them vulnerable to geopolitical coercion or service denial (Blancato, 2023).

2.1.3 The Philosophical Dimension: Sovereignty vs. Digital Fealty

Recent scholarship has expanded the definition of sovereignty beyond state control to individual agency. Drawing upon Crawford's (2025) analysis of the "Ownership of the Means of Thinking," this thesis terms the resulting condition "Digital Fealty." Crawford warns that when states rely on proprietary platforms for basic cognition, they enter a state of submission and dependency, contingent on the "continued solvency and goodwill" of private enterprises (Crawford, 2025).

Consequently, the Sovereign Cloud debate emerged not as a technical innovation but as a political necessity that attempts to impose public control onto private infrastructure.
This perspective reframes the Sovereign Cloud debate as a struggle over the material conditions of agency. Blancato and Carr (2024) define this as a trust deficit, a fundamental friction caused by the EU's dependence on foreign providers. Thus, Digital Sovereignty acts as a countermeasure to this subscription model (Crawford, 2025), attempting to reclaim the power that tech companies currently hold over the 'control of the digital' (Floridi, 2020).

2.1.4 Divergent National Strategies

While the EU provides the regulatory impetus, the implementation of sovereignty varies significantly across member states (Rone, 2024; Veneziano, 2025):

- **France:** Adopts a "Dirigiste" approach, prioritizing strict industrial independence. The "Cloud de Confiance" label requires not only data residency but also that the cloud operator is majority-owned by European entities to ensure immunity to non-EU law (Rone, 2024). This has led to joint ventures like Bleu (Orange/Capgemini & Microsoft), where US technology is licensed, but French entities operate the services.
- **Germany:** Adopts a "Federalist" approach. Germany's strategy focuses on projects such as the Sovereign Cloud Stack (SCS), which aims to develop a federatable, fully

open software stack (Rone, 2024). However, while the state seeks sovereignty, globally oriented German corporations have opposed strict sovereignty criteria to avoid restrictions on their global operations (Rone, 2024).

- **Italy:** Adopts a "Pragmatic" approach centered on the National Strategic Hub (Polo Strategico Nazionale). Italy's strategy expresses a tension between "Autonomy and Pragmatism." Recognizing a lack of domestic resources, Italy created a state-steered infrastructure that nevertheless relies on the technology of non-EU hyperscalers to deliver high-performance services (Veneziano, 2025).

2.2 The Technological Architecture of the Sovereign Cloud

To comply with rigorous legal standards while capturing economic value, governments are transitioning from standard cloud computing to Multi-Cloud architectures that incorporate Public, Private, and Sovereign Cloud offerings.

2.2.1 Standard Cloud Deployment Models

The ISO/IEC 22123-2:2023 standard formalizes the term cloud computing and distinguishes between various cloud deployment models (ISO/IEC, 2023):

- **Public Cloud:** Infrastructure shared across multiple tenants. While this provides access to high-scale innovation, it creates a trust deficit due to the extraterritorial reach of non-EU laws (Blancato, 2023).
- **Private Cloud:** Infrastructure dedicated to a single organization. Exclusive reliance on legacy (on-premises) systems creates a technological gap, as these systems lack the R&D scale of global hyperscalers and are eventually subject to technological obsolescence (Bauer et al., 2025).
- **Multi-Cloud:** Rather than a single label, states are adopting a multi-provider strategy (Rone, 2024). Decentralized government systems are increasingly adopting Multi-Cloud strategies that include public and private cloud services to manage big data workflows and AI applications, enabling flexibility and compliance across different jurisdictions (Putri, 2025).

"Sovereign Cloud" is often defined not as a distinct deployment model but as a governance framework in which "Digital Sovereignty requirements can be met" (Bauer et al., 2025). This approach shifts the focus from physical location to protective capacity, enabling provider-

managed, separate cloud-like installations within local data centers. Crucially, this mandates both Data Residency and Operational Sovereignty, effectively immunizing the infrastructure against extraterritorial laws like the U.S. CLOUD Act. The transition to Sovereign Cloud architectures is not merely a legal compliance exercise but a strategic reshaping of national data security postures (Boston Consulting Group, 2025a).

2.2.2 The Conflict Over Sovereignty Requirements

Defining a Sovereign Cloud reveals a fundamental tension between political security goals and economic reality. While national strategies in Italy and France (as highlighted in 2.1.4) establish stricter barriers to regain control (Rone, 2024; Veneziano, 2025), these same measures impose disproportionate restrictions that risk fragmenting the European market (Bauer et al., 2025).

- **The Push for Data Localization:** Data and service localization is a central pillar of Italy's strategy to ensure national control (Veneziano, 2025). But data localization also limits access to global technologies. Cutting off foreign data flows could affect key government functions by preventing the use of advanced global cloud technologies that enable AI-driven automation and data analytics (Bauer et al., 2025).
- **The Push for Jurisdictional Immunity (Ownership):** To prevent the extraterritorial application of U.S. law, the French strategy (exemplified by the SecNumCloud label) imposes strict immunity requirements. Sovereignty requirements mandate that cloud providers be majority-owned by European entities and headquartered within the EU to preclude foreign jurisdiction (Bauer et al., 2025). This has been characterized as a dirigiste approach, in which the state actively intervenes to foster 'industrial independence' through national champions (Rone, 2024).
- **The Dilemma of Technological Autonomy:** The overarching goal is "technological autonomy" with the ability to maintain infrastructure independent of non-EU providers. This creates a paradox: the pragmatism required to actually digitize the public sector forces states to rely on the very non-EU hyperscalers they seek to exclude (Veneziano, 2025).

2.2.3 The Limits of Pan-European Initiatives

The European Union attempted a collective response through the Gaia-X initiative. As Rone (2024) explains, this initiative was intended to create a federated secure data cloud infrastructure and a completely open software stack to reduce reliance on foreign providers. However, Gaia-X illustrates the practical limits of Digital Sovereignty (Rone, 2024). The initiative was marred by internal conflict after "Big US Tech companies... secured a place on the managing board," leading to the departure of European providers who felt the project had lost its focus on sovereignty. The market appears to have settled into a trade-off where sovereignty is asserted "de iure" (through legal contracts) while the infrastructure remains "de facto" dependent on the oligopolistic position of non-EU hyperscalers (Veneziano, 2025).

2.3 Drivers of Adoption: Trust, Performance, and the Privacy Calculus

While the strategic logic for sovereignty is driven by law and geopolitics, its success ultimately depends on adoption by both the state and the citizenry. The literature identifies a complex trade-off at both levels. Public administrations must weigh the benefits of modernization from cloud adoption against the risks of strategic dependence. Simultaneously, citizens engage in a psychological interaction between the service's functional utility and the perceived risks of data handling.

2.3.1 Theoretical Foundations: The Utility-Risk Trade-off

To understand citizen adoption, this study synthesizes two complementary theoretical frameworks: the efficiency-driven UTAUT model and the risk-oriented Privacy Calculus.

The Imperative of Performance

Traditional adoption research is anchored in the Unified Theory of Acceptance and Use of Technology (UTAUT) proposed by Venkatesh et al. (2003). By consolidating previous acceptance models, Venkatesh et al. identified "Performance Expectancy," defined as the degree to which using a system will provide benefits to the user, as the single strongest predictor of behavioral intention.

In the context of digital public services, this theory implies that normative values (like sovereignty) are secondary to functional utility. If a sovereign service fails to deliver the

efficiency gains citizens expect (e.g., speed, reliability), Venkatesh et al. (2003)'s model predicts that adoption will fail regardless of how secure the data is. This establishes Service Performance not merely as a convenient feature, but as a structural prerequisite for adoption.

The Counterweight: Privacy Calculus

However, this study explores whether utility alone is sufficient for the public sector, where citizens are often compelled to share sensitive personal data. To account for this, the study integrates the Privacy Calculus Theory. Rooted in the foundational work of Culnan and Bies (2003), this theory posits that individuals engage in a rational trade-off, disclosing personal information only when the perceived benefits outweigh the risks.

Dinev and Hart (2006) extended the model to the online context, creating a direct theoretical link to the sovereignty debate:

- **The Enticement (Utility)**: They identify Personal Internet Interest, defined as "cognitive attraction," as a powerful intrinsic motivator. Analogous to Venkatesh's "Performance Expectancy," their findings suggest that if the Enticement (Utility) is high enough, it can override privacy concerns.
- **The Risk (Sovereignty Concerns)**: Crucially, "Privacy Risk" encompasses the fear that personal information could be disclosed to unauthorized parties or government agencies (Dinev & Hart, 2006). This confirms that sovereignty concerns, specifically the fear of surveillance, are a measurable component of user hesitation that impedes adoption.

2.3.2 Structural Barriers: The Skills Gap

Even if the privacy calculus is positive, adoption is limited by structural factors. A critical counter-perspective to the technological optimism of 'build it, and they will come' is provided by Doran et al. (2023). In their cluster analysis of EU member states, they found that simply providing Online Services does not guarantee efficiency. In fact, in less digitized countries, the OSI (Online Services Index) negatively affected government effectiveness because Human Capital did not match. The authors attribute this to a digital divide in skills, where the population lacks the capacity to use the tools provided. This suggests that a Sovereign Cloud initiative will fail if the state focuses only on the technology (Sovereignty) and ignores the Human Capital required to use it (Doran et al., 2023).

2.3.3 Trust in the Public Sector: A Fiduciary Relationship

Trust acts as the mediator in this calculus. To understand its mechanism, this study relies on the integrative model of Mayer et al. (1995). Trust is not merely a prediction of behavior but is "the willingness of a party to be vulnerable" to the actions of another, irrespective of the ability to monitor or control that other party (Mayer et al., 1995). This is critical for the cloud context, where citizens are technically unable to monitor where their data flows, rendering them vulnerable to the state's infrastructure choices.

Mayer et al. (1995) decompose this trustworthiness into three distinct pillars, which this thesis maps to the Digital Sovereignty debate:

- **Ability:** The group of skills and competencies that enable a party to influence within some specific domain. In this context, it represents the state's technical competence to secure data against cyber threats or outages.
- **Benevolence:** The extent to which a trustee is believed to want to do good to the trustor. This reflects the citizens' belief that the government is adopting Sovereign Cloud to protect them (public interest), rather than to increase state surveillance power.
- **Integrity:** The trustor's perception that the trustee adheres to a set of principles that the trustor finds acceptable. For Digital Sovereignty, this is the strongest signal: by rejecting the US CLOUD Act and enforcing the GDPR, and complying with the Schrems II ruling, the state signals adherence to the 'Rule of Law' values.

While Mayer provides the theoretical architecture, Gupta and Chauhan (2024) offer the empirical validation in the public sector. In their meta-analysis of e-government adoption, they find that perceived privacy and perceived security are among the strongest antecedents of trust. Crucially, they identify that when users perceive high risks (e.g., foreign surveillance), the reliance on institutional trust increases. This confirms that Digital Sovereignty, which functions as a signal of high privacy and integrity, is a structural necessity for building the trust required to mitigate the vulnerability defined by Mayer et al. (1995).

Deepening this, Morgan and Hunt (1994) argue in their Commitment-Trust Theory that trust is vital because it fosters Relationship Commitment. However, they distinguish genuine commitment from mere acquiescence driven by power or dependence. In the monopoly context of the citizen-state, if citizens feel 'locked-in' to digital services without the mediating buffer

of Trust, the relationship risks degrading into a state of dependency and submission (Crawford, 2025).

2.3.4 The Sovereignty Tax on Performance

This creates the central tension, referred to in this study as the "Sovereignty Tax." Strict exclusionary requirements, such as data localization and foreign ownership bans, create operational inefficiencies and significantly limit access to advanced technologies and global innovation (Bauer et al., 2025).

AI-powered SaaS solutions are revolutionizing governance by automating repetitive tasks and enabling predictive analytics for better resource allocation (Ajayi et al., 2024). However, because these tools often rely on global training data and hyperscale infrastructure, strict data localization rules frequently delay or prohibit their deployment. The citizen is thus caught in a functional paradox: they desire the convenience of proactive, AI-driven, digitized services (Performance), yet demand the protection that technically precludes such services (Sovereignty) (Ajayi et al., 2024).

2.3.5 The Disconnect Between Political Rhetoric and Technical Reality

Finally, the literature identifies a fundamental disconnect between the political goals of sovereignty and the technical reality of its implementation.

Ultimately, European policy discourse lacks a consistent definition of Digital Sovereignty (Roberts et al., 2021). The term is primarily used as a normative tool to project European values (e.g., privacy, fairness) onto the digital market (Roberts et al., 2021). This conceptual fluidity allows sovereignty to function as a form of political rhetoric, a flexible container term that promises autonomy while masking the reality of continued dependence on non-European infrastructure (Rone, 2024).

European states are caught in a capabilities gap. They aggressively champion sovereignty in public discourse, yet remain structurally dependent on US hyperscalers (e.g., AWS, Microsoft Azure, Google Cloud) for critical operations due to the lack of domestic alternatives that can match global performance standards (Bauer et al., 2025).

This ambiguity creates risk for the citizen. If sovereignty is promised as a protective value (Roberts et al., 2021) but operates on dependent infrastructure (Bauer et al., 2025), it generates an expectation gap. This suggests that for sovereignty to drive trust, the state must clearly communicate how this normative promise is translated into concrete technical measures, rather than relying on vague political signaling.

2.4 Theoretical Frameworks: The Organizational Capability to Adapt

To explain how public administrations can resolve the trade-off between sovereignty and performance, this study draws on two complementary perspectives from strategic management: Resource-Based Theory (RBT) and Dynamic Capabilities (DC).

Although these are traditionally firm-level theories, they may inform understanding of the public sector (Piening, 2013). Public organizations are not static bureaucracies but entities operating in turbulent environments characterized by rapid technological change and shifting political mandates. Consequently, the state must develop dynamic capabilities, defined as the ability to integrate, build, and reconfigure internal competencies, not to maximize profit, but to sustain public value and effectiveness in the face of disruption (Piening, 2013). In this sense, the state monopolizes certain functions but competes in a quasi-marketplace for a variety of abstract currencies, such as trust, legitimacy, and operational efficiency.

2.4.1 Resource-Based Theory: Sovereignty as the Strategic Resource

To understand the strategic value of the public cloud, this study applies Resource-Based Theory (RBT) from J. B. Barney et al. (2021).

Strategic Framework Selection: Why VRIN?

This study uses the original VRIN framework (1991) rather than VRIO (1995) because the "non-substitutable" dimension best captures the conflict between technical security and legal standing. In the context of the Schrems II ruling, assessing whether one can substitute for the other is the central analytical challenge.

The analysis identifies Digital Sovereignty, defined as the capacity for autonomous digital action free from external interference, as the critical VRIN resource.

- **Valuable:** A resource is valuable if it neutralizes threats. Digital Sovereignty neutralizes the existential threat posed by extraterritorial surveillance (e.g., the US CLOUD Act), thereby preserving state legitimacy.
- **Rare (Market Scarcity):** In the European cloud market, sovereign infrastructure is rare. As noted above, the market is dominated by non-EU hyperscalers. Providers capable of delivering high-performance services without legal exposure to foreign jurisdictions are a scarce economic commodity (Bauer et al., 2025).
- **Inimitable (Structural Disqualification):** Competitors (specifically US Hyperscalers) cannot imitate this resource because they are structurally disqualified by their domestic laws (FISA). No matter how secure their technology, they cannot replicate the sovereign operating model required to guarantee independence. This creates a structural moat that protects the resource from imitation by the dominant market players.
- **Non-substitutable (The Immunity Factor):** Finally, technical measures are not a substitute for legal standing. As established by the CJEU (Schrems II), encryption does not override statutory obligations to foreign intelligence agencies. Therefore, true Digital Sovereignty is non-substitutable because it provides Jurisdictional Immunity, the only mechanism that guarantees legal certainty.

The Paradox of Execution

However, if Digital Sovereignty is a perfect and monopolistic strategic resource, why does its adoption often lead to performance declines? The answer lies in a limitation of traditional RBT: it is frequently criticized for being "static," assuming that merely possessing a valuable resource automatically confers an advantage.

To resolve this paradox, RBT must be understood through a "Multilayered Framework" rather than a flat list of resources (Chen et al., 2024). The authors posit three distinct layers of value creation:

1. **IT-Related Assets** (**Foundational Layer**): The tangible infrastructure and informational resources (e.g., the Sovereign Cloud itself) where ownership of these assets is merely the "foundation" and is insufficient on its own to generate sustainable performance.
2. **Operational IT Competence** (**Execution Laye**r): The ability to "mobilize and deploy" these assets effectively. This requires "functional routines" and "practical know-how" to translate the asset into business value.

3. **Dynamic IT Capabilities** (**Adaptation Layer**): The capacity to reconfigure these competencies in response to environmental shifts.

This hierarchy provides the theoretical mechanism for the Sovereignty Tax. The efficiency loss occurs because the public sector has focused almost exclusively on Level 1 (Acquiring the Sovereign Asset) while neglecting Level 2 (Developing the Operational Competence) and subsequently Level 3.

However, possessing diverse IT-related assets may be insufficient without the corresponding competence to deploy them (Chen et al., 2024). Public Administrations often lack the investments and skills to deliver digital services independently (Veneziano, 2025). Consequently, while the state possesses the asset, its inability to mobilize and deploy it independently forces a reliance on foreign Operational Competence, effectively negating the autonomy that the Sovereign Cloud was intended to secure.

2.4.2 The Constraint of Structural Rigidity

Applying this framework to the public sector reveals a critical barrier: lack of 'IT Infrastructure Competence' (Chen et al., 2024).

This competence is essential because it enables an organization to build and modify its IT infrastructure assets to meet changing strategic demands. Without this competence, IT assets cannot be effectively realigned to support new business objectives, thereby constraining the organization’s existing technical setup (Chen et al., 2024).

This theoretical insight explains the frictions in the debate around Digital Sovereignty. Public administrations often rely on legacy systems and lack the technical and human components required to modify them. Consequently, when the state introduces a new Sovereign Cloud (Asset), it lacks the 'Dynamic IT Business Transformation Capability,' defined as the capacity to continuously reconfigure infrastructure required to integrate the new asset into existing operations (Chen et al., 2024). The result is a structural disconnect (“Asset-competence Gap”: the sovereign asset is acquired but remains underutilized because the organization lacks the internal flexibility to assimilate it into the established workflow.

2.4.3 Dynamic Capabilities: The Framework for Adaptation

To address this trap and the volatile nature of the digital environment, this study employs the Dynamic Capabilities (DC) framework. Teece et al. (1997) originally defined these capabilities as the firm's ability to integrate, build, and reconfigure internal and external competencies to address rapidly changing environments.

Later, Teece (2007) disaggregated this definition into three capacity clusters: Sensing, Seizing, and Transforming. Muhic and Bengtsson (2021) explicitly apply this tripartite framework to Cloud Sourcing, arguing that firms must progress through these three distinct stages to adopt cloud technologies successfully. Applying their model to the context of Digital Sovereignty yields the following Micro foundations:

- **Sensing (Scanning)**: The ability to identify opportunities and threats in the ecosystem. In this study, this corresponds to the public sector's capacity to monitor regulatory risks, such as the extraterritorial reach of the US CLOUD Act.
- **Seizing (Mobilizing)**: The ability to mobilize resources to capture value. This corresponds to the strategic decision to procure and implement Sovereign Cloud architectures rather than standard public cloud services.
- **Transforming (Reconfiguring)**: The ability to reorganize the workforce and assets. As Muhic and Bengtsson (2021) note, this is the critical phase where the organization must "reconfigure" its internal routines to manage the new digital stack effectively.

2.4.4 Dynamic Capabilities: The Failure of Systematicity

Crucially, true Dynamic Capabilities must be distinguished from mere ad hoc problem-solving (Barreto, 2010). DCs are the firm's potential to systematically solve problems through established routines, rather than through improvised, one-off actions (Barreto, 2010). This distinction is vital: a capability exists only when the response is repeatable and embedded in the organization's structure.

Applying Barreto's (2010) lens exposes a structural flaw in current sovereignty strategies. This study argues that the public sector frequently adopts an episodic approach, treating sovereignty as a one-time procurement project, a distinct event where a compliant cloud is purchased, rather than developing the continuous internal processes required to manage it.

Veneziano (2025) provides the empirical basis for this assessment. He finds that European administrations often lack the investments and skills to manage digital services independently, forcing a “de facto” reliance on external providers.

By Barreto’s (2010) standard, this reliance relegates the initiative to the status of a static resource rather than a true Dynamic Capability. Since a Sovereign Cloud is often acquired as a standalone asset, lacking the organizational agility that Atobishi et al. (2024) identify as the critical mediator between digital capabilities and performance, the state struggles to generate the value it seeks. Without this agile operational layer, a sovereignty project remains a technical procurement rather than a strategic capability.

2.5 Conclusion: The Capability Gap and the Citizen’s Dilemma

In summary, the literature review establishes a transparent conceptual chain that defines the “Sovereignty Paradox.”

First, the review demonstrates that Digital Sovereignty has evolved from a regulatory preference to a constitutional necessity (Schrems II). However, a disconnect remains between the “de iure” legal assertions and the “de facto” technical reality, where European public administrations remain structurally dependent on non-EU hyperscalers (Veneziano, 2025).

Second, the root cause of this dependency is an Asset-Competence Gap (Chen et al., 2024). The state has focused on acquiring Sovereign Infrastructure while neglecting the Operational Competence required to mobilize it. This episodic procurement approach fails to constitute a true Dynamic Capability capable of responding to threats and opportunities in a timely manner (Barreto, 2010). The latter would encompass everything from exogenous cyber threats to technological innovations as technology advances. Without organizational agility as the mediator between technology and performance, the Sovereign Cloud remains a static asset rather than a functional service (Atobishi et al., 2024).

Finally, this organizational failure forces a critical trade-off upon the citizen. As established by the Privacy Calculus (Dinev & Hart, 2006) and Mayer et al.’s (1995) model of Trust, citizens are caught in a pincer movement. They demand Integrity (Data Sovereignty) to mitigate risk, yet require Benevolence (Service Utility), which is currently hampered by the Sovereignty Tax.

The resolution of this tension forms the core of this study. To empirically test how citizens navigate this trade-off, the following chapter begins by proposing a Conceptual Framework that maps the relationships between Sovereignty, Trust, and Performance, before detailing the methodological design used to validate it.

3. Methodology

This chapter outlines the methodological framework adopted to investigate the relationship between Digital Sovereignty, trust, and the adoption of digital public services. The chapter begins by establishing the Conceptual Framework and Hypotheses derived from the literature. It then details the Research Philosophy, Research Design, and the specific data collection and analysis procedures used to test this model.

3.1 Conceptual Framework and Hypotheses

Based on the literature review and refined through preliminary expert insights, this study proposes a perception-based conceptual framework that operates at the citizen level.

While the core constructs are derived from established theory, the specific focus on the trade-off between Sovereignty and Performance was corroborated by the qualitative strand (Section 3.4). The experts identified this tension, the Sovereignty Tax, as the defining practical challenge, justifying its central placement in the model.

3.1.1 Theoretical Justification

To justify the application of firm-level theories (Resource-Based Theory and Dynamic Capabilities) to the public sector, this study draws on Piening's (2013) validation.

As established in the Literature Review (Section 2.4), Piening (2013) argues that public organizations are not static bureaucracies but are increasingly exposed to turbulent environments characterized by rapid technological change and shifting political mandates.

Consequently, Dynamic Capabilities is an appropriate framework for analyzing how the state must integrate, build, and reconfigure its internal competencies to maintain legitimacy and performance. This justifies applying strategic management logic to the analysis of the digital state.

3.1.2 From Theory to Variables: Operationalizing the Model

To translate the strategic logic of Piening (2013) into a testable model, the abstract concepts of Legitimacy and Capabilities are operationalized into specific citizen-centric variables:

- **Willingness-to-Use (Dependent Variable)**: In the public sector context, the state often holds a monopoly on service provision. Therefore, performance is not measured by market share against private competitors, but by the successful migration of citizens from analog to digital channels. If citizens reject the sovereign digital service due to friction or mistrust, they revert to costly manual processes (e.g., in-person office visits), negating the efficiency gains of digital services. Thus, this study measures success through the citizens' behavioral intention to adopt the digital channel.
- **Perceived Sovereignty & Service Performance (The Drivers)**: These represent the two conflicting resources identified in the Literature Review. Service Performance represents the enticement (Utility) described in the Privacy Calculus, while Perceived Digital Sovereignty represents the Integrity signal required to mitigate risk.
- **Trust (The Mediator)**: According to the Trust-Commitment Theory, Trust is the essential mechanism that translates the abstract attribute of sovereignty into the behavioral intention to use the service.

3.1.3 The Conceptual Model

As illustrated in Figure 1, the framework treats Perceived Digital Sovereignty and Service Performance as primary drivers. Trust acts as a mediator, theorized to transmit the normative value of sovereignty onto the behavioral outcome of adoption.

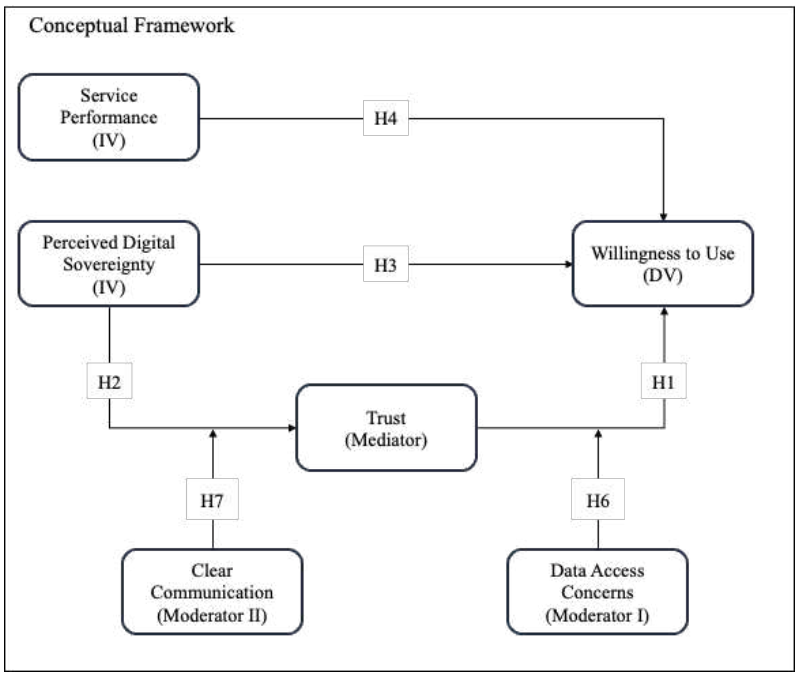


Figure 1: Conceptual Framework

3.1.4 Hypotheses Development

Based on the conceptual framework and the reviewed literature, the following hypotheses guide the empirical analysis. To maintain clarity and reflect the conceptual model's structure, the hypotheses are divided into two groups. The primary Hypotheses capture the central causal relationships required to answer the Research Question regarding willingness-to-use. The Supplementary Hypotheses extend this model by testing additional moderating mechanisms that, although not essential for addressing the core Research Question, enrich the analysis's explanatory depth.

Primary Hypotheses
H1: Higher citizen trust in online public services is positively associated with willingness-to-use them.
H2: Higher perceived Digital Sovereignty increases citizens' trust in online public services.
H3: Perceived Digital Sovereignty positively affects citizens' willingness-to-use online public services.
H4: Perceived service performance is positively associated with willingness-to-use online public services.
H5: Trust mediates the relationship between perceived Digital Sovereignty and willingness-to-use online public services.
Secondary Hypotheses
H6: Concerns about data access outside Europe weaken the positive effect of trust on willingness-to-use online public services.
H7: Clear communication about data protection strengthens the effect of perceived Digital Sovereignty on trust.

These hypotheses reflect the theorized relationships between sovereignty, trust, and performance, and enable structured testing of the Research Question using the collected survey data.

In summary, the framework functions as a bridge between theory and evidence. It structures the forthcoming methodological design and provides analytical coherence across both empirical components, ensuring that the study remains focused on uncovering how Sovereign Cloud adoption enhances public-sector digital performance through institutional and organizational processes.

3.2 Research Philosophy and Approach

To address the Research Question effectively, this study adopts a pragmatist approach where the question is the primary determinant of the methodology, ignoring debates over positivism

versus interpretivism (Clark & Ivankova, 2017). This supports a pluralistic approach combining the contextual depth of qualitative expert insights with the generalizable patterns of citizen behavior gathered in a quantitative survey (Saunders et al., 2019).

Consistent with this philosophy, the study employs an abductive research approach. Unlike pure deduction (theory-testing) or induction (theory-building), abduction allows for a continuous interplay between theory and empirical data (Dubois & Gadde, 2002). The initial literature review informed the theoretical framework, while qualitative insights helped refine the context of Digital Sovereignty, which was subsequently tested via the quantitative survey.

3.3 Research Design

This thesis utilizes a convergent mixed-methods design (Creswell, 2009). This design involves collecting and analyzing both qualitative and quantitative data to provide a comprehensive triangulation of the research problem.

- **Qualitative:** Semi-structured expert interviews were conducted to understand the institutional strategies and governance challenges of Sovereign Cloud adoption.
- **Quantitative:** A cross-sectional online survey was administered to European citizens to assess perceptions of sovereignty, trust, and willingness to use digital services.

Triangulation ensured that the limitations of one method are offset by the strengths of the other two, providing a more robust understanding of the phenomenon (Bryman & Bell, 2015). Specifically, while the expert interviews provided the supply-side perspective (infrastructure, strategy, and technical feasibility), the quantitative citizen survey was deemed necessary to capture the demand-side perspective (adoption intentions and trust formation). Coupled with secondary data from the literature review, this tripartite approach enabled data triangulation, ensuring that the theoretical benefits of sovereignty identified by experts are validated against end-users' actual perceptions. The research design is illustrated in Figure 2.

While secondary datasets, such as the EU eGovernment Benchmark, provide valuable metrics on service availability and technical usability, they were excluded from this study because they currently lack specific indicators on Data Sovereignty and citizen trust formation, which are the central foci of this research.

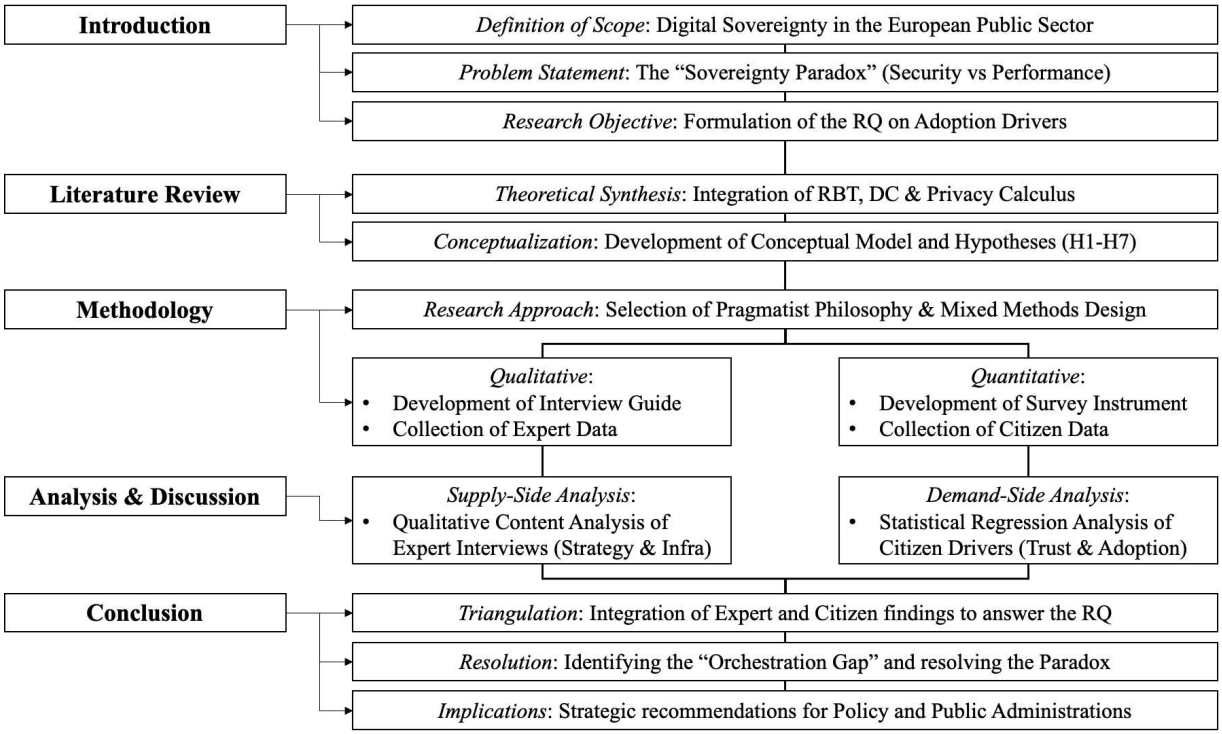


Figure 2: Research Design

3.4 Qualitative Data Collection and Analysis

To gain insights into the strategic imperatives of Sovereign Cloud adoption, qualitative data was gathered through interviews with industry professionals.

3.4.1 Sampling Strategy and Participants

Purposive and snowball sampling were used to select experts based on their specific knowledge of European digital policy, cloud infrastructure, and public administration (Etikan, 2016). Initial contacts were identified through professional networks (LinkedIn) and previous work relationships in the cloud consulting space, with subsequent participants recruited via referrals.

The final sample consisted of 12 experts ($n = 12$), including consultants specializing in technology and strategy from major consulting firms, alongside experts in Sovereign Cloud architecture and digital policy. Qualitative data adequacy was achieved with the 12-person sample. To ensure anonymity, participants are referred to by IDs throughout the analysis. The sample composition ensures a balance between strategic oversight and technical implementation expertise.

Table 1: Expert Interview Participants

ID	Role	Organization Type	Focus Area
P01	Leader Cloud CoE	Public Sector (Federal Agency)	Cloud Competence Center
P02	Deputy Director IT	Public Sector (Federal IT Provider)	Federal Infrastructure
P03	Cloud Lead	Public Sector (Social Insurance)	Sovereign Procurement
P04	Head of IT Security	Public Sector (Health Insurance)	Sensitive Data & Security
P05	CIO	Public Sector (Federal Agency)	Strategic Decision Making
C01	Director	Technology Consulting	Former Sovereign Cloud Provider
C02	Manager	Technology Consulting	Public Sector Transformation
C03	Senior Manager	Technology Consulting	Healthcare & Public Sector
C04	Senior Manager	Technology Consulting	Cloud Operating Models
C05	Manager	Technology Consulting	Digital Strategy
C06	Senior Manager	Technology Consulting	Migration & Architecture
C07	Director	Technology Consulting	Technology Strategy
Total	12 Experts	Mixed (Public & Private)	Avg. Duration: 35 min

3.4.2 Data Collection and Analysis

- **Collection:** Semi-structured interviews were conducted via Microsoft Teams between November and December 2025. This platform facilitated the recording and subsequent transcription of the discussions. The interviews lasted between 30 and 40 minutes on average. An interview guide (See Appendix A) derived from the literature review was used to structure the conversation, covering key themes such as trade-offs between sovereignty and efficiency, while allowing flexibility for experts to elaborate on emerging topics (Kallio et al., 2016).
- **Analysis:** The interviews were transcribed and analyzed using Qualitative Content Analysis following Mayring (2014). Specifically, a structured content analysis approach was employed using Microsoft Excel. A category system was developed deductively based on the theoretical framework (e.g., 'Sovereignty', 'Trust', 'Performance'), while allowing inductive subcategories to emerge from expert insights (see Appendix B for the Coding Manual). This systematic, rule-based approach ensured that the qualitative interpretations were reproducible and inter-subjectively verifiable (Mayring, 2014).

3.5 Quantitative Data Collection (Citizen Survey)

The quantitative phase empirically tested the conceptual model and hypotheses (H1–H7).

3.5.1 Sampling and Distribution

A non-probability convenience sampling strategy was employed to reach a broad demographic of European citizens (Etikan, 2016). The survey was hosted on Qualtrics and distributed via digital channels, including professional networks (LinkedIn), community forums, and personal networks. The survey was active from November 20th to December 4th, 2025.

3.5.2 Data Cleaning and Sample Size

A total of 305 responses were initially recorded. Rigorous data cleaning was performed to ensure data quality:

- **Incomplete Responses:** 35 respondents who did not complete the survey were removed.
- **Speeders:** 16 respondents were excluded for completing the survey significantly faster than the average time per question.
- **Attention Checks**: 12 respondents failed the embedded attention check question and were removed. This process resulted in a final sample size of $n = 242$ valid responses.

3.5.3 Demographic Profile

To ensure a comprehensive understanding of the respondent pool, data were collected on gender, age, education, and digital skills. The respondents were predominantly young professionals, with 42.6% in the 25–34 age bracket and a further 20.2% in the 35–44 age bracket. The sample was skewed towards male respondents (64.0%). Regarding human capital, participants were highly educated: 64.9% held a bachelor's degree, and 23.6% held a master's degree. This indicated a sample that was likely more digitally literate than the general European population, a factor considered during the interpretation of results (see Table 2).

Table 2: Sample Demographic Table

Category	Sub-Category	Percentage (%)
Gender	Male	64.0%
	Female	36.0%
Age Group	18-24	8.7%
	25-34	42.6%
	35-44	20.2%
	45-54	11.2%
	55-64	12.8%
	65+	4.5%
Highest Education	Secondary Education	2.9%
	Vocational Training	5.0%
	Bachelor's Degree	65.4%
	Master's Degree	23.8%
	PhD / Doctorate	2.9%
Employment Status	Full-time Employed	63.6%
	Part-time Employed	21.1%
	Student	5.8%
	Unemployed	1.7%
	Retired	7.4%
	Other	0.4%
Self-Assessed Digital Skills	Low	2.5%
	Moderate	24.4%
	High	48.3%
	Very high	24.8%

3.6 Instrument Design and Operationalization

The survey instrument operationalized the "Utility vs. Risk" tension established in the literature. To ensure internal consistency, the efficiency-related constructs were derived from the UTAUT framework, while the sovereignty-related constructs were synthesized from privacy and governance literature.

The Dependent Variable

- **Willingness-to-Use:** Adapted from Venkatesh et al. (2003) to measure Behavioral Intention. Items focused on the respondent's intention to use online government channels over in-person alternatives and their likelihood of relying on these services in the future.

The Drivers and Mediator

- **Service Performance (The Utility Driver):** To ensure theoretical alignment with the dependent variable, this construct operationalizes the "Performance Expectancy" scale from Venkatesh et al. (2003). Items measured the perceived speed, reliability, and efficiency gains of the service.
- **Perceived Digital Sovereignty (The Normative Driver):** As no standard scale exists, items were developed based on the conceptual definitions provided by Celeste (2021) and Blancato (2023). Sovereignty was measured through tangible attributes: Data Residency (e.g., 'data stored in Europe') and Jurisdictional Control.
- **Trust in Digital Public Services:** Functioning as a mediator, this was measured using items adapted from the seminal work of Mayer et al. (1995) and the public-sector context provided by Gupta and Chauhan (2024). Questions assessed Ability, Benevolence, and Integrity.

The Moderators

- **Data Access Concerns:** Measured by adapting risk perception items regarding extraterritorial surveillance. This explicitly operationalizes the "Privacy Risk" component described by Dinev and Hart (2006).
- **Clear Communication:** Operationalized as a response to the conceptual ambiguity described by Roberts et al. (2021) and Rone (2024**)**. Since citizens cannot technically verify the complex legal mechanisms of sovereignty (e.g., cloud contracts), this variable measures the clarity of the "rhetorical signal" sent by the state. Items assessed whether the government's explanation of data protection was transparent and understandable to the citizen.

Measurement Scale

All items were measured on a 5-point Likert scale ranging from "Strongly Disagree" (1) to "Strongly Agree" (5). This scale was selected because it is the standard in social science research for measuring latent attitudes, offering a balance between respondent ease of use and statistical variance for regression analysis (Likert, 1932).

3.7 Quality Criteria: Validity and Reliability

To ensure the quantitative instrument's rigor, validity, and reliability were rigorously assessed.

3.7.1 Validity

Construct validity was ensured by deriving survey items from established theoretical frameworks. Furthermore, a pilot test was conducted with 5 participants before complete distribution. This process confirmed face validity, ensuring that question wording was precise, the flow was logical, and no technical issues existed within the Qualtrics platform (Hair et al., 2010).

3.7.2 Reliability Analysis (Internal Consistency)

Internal consistency was assessed using Cronbach's Alpha (α). While a threshold of 0.70 is typically recommended for established scales, Hair et al. (2010) note that in exploratory research involving novel constructs, values between 0.60 and 0.70 are considered acceptable. The analysis yielded the following results:

- **Trust** ($\alpha = 0.811$): Demonstrated good internal consistency.
- **Service Performance** ($\alpha = 0.787$): Demonstrated sufficient consistency.
- **Data Access Concerns** ($\alpha = 0.738$) and **Perceived Sovereignty** ($\alpha = 0.734$): Demonstrated sufficient consistency.
- **Clear Communication** ($\alpha = 0.680$)**:** Fell slightly below the standard 0.7 threshold but remains within the acceptable range for exploratory constructs.
- **Willingness-to-use** ($\alpha = 0.652$): This score indicated questionable consistency. The lower alpha suggested that the items within this scale may not be entirely homogenous or interchangeable. From a methodological standpoint, this raised a concern that if different items were used (e.g., phrasing "I prefer online services" differently), the results might deviate. This implied a potential issue with the measure's stability (test-retest reliability). However, given that Digital Sovereignty is a novel topic and this study is exploratory, this value was deemed acceptable for analysis, though it is acknowledged as a limitation regarding the robustness of the dependent variable.

3.8 Data Analysis Strategy

The quantitative data were analyzed using IBM SPSS Statistics. The analysis followed a multi-stage process:

1. **Data Preparation:** Before hypothesis testing, the latent constructs (Trust, Sovereignty, Performance, etc.) were computed into composite variables. This was achieved by

calculating the arithmetic mean of the respective multi-item 5-point Likert scales (e.g., Trust_Composite = Mean of Trust_1 to Trust_8). This aggregation was performed only after confirming internal consistency via Cronbach's Alpha.

2. **Descriptive Statistics:** To profile the sample demographics and assess the distribution of variables (Mean, Standard Deviation).
3. **Factor Analysis:** Exploratory Factor Analysis (EFA) was conducted to verify the construct validity of the measurement scales.
4. **Hypothesis Testing:** Multiple Linear Regression was performed to test the direct relationships (H1, H2, H3, H4) and the moderating effects (H6, H7).
5. **Mediation Analysis:** Mediation testing was conducted to assess the role of Trust as a mediator between Perceived Sovereignty and Willingness (H5).

3.9 Ethical Considerations

Participation in both the interviews and the survey was voluntary. Informed consent was obtained from all participants, and anonymity was guaranteed. Data storage and processing adhered to GDPR guidelines, ensuring that no personally identifiable information (PII) was stored without consent. The experts involved in the qualitative strand were anonymized to prevent professional repercussions, allowing for open and critical discussion of current policy limitations.

4. Results

This chapter presents the study's empirical findings. Section 4.1 details the qualitative insights gathered from expert interviews, while Section 4.2 reports the quantitative results from the citizen survey.

4.1 Semi-structured Interviews: Expert Perspectives

The findings from the semi-structured interviews are grouped into four main themes derived from the qualitative content analysis (Mayring, 2014): The shifting conceptualization of Digital Sovereignty from data location to operational capability; the divergence between institutional compliance measures and citizen trust formation; the performance trade-offs inherent in sovereign adoption; and finally, the structural drivers and barriers defining the current market landscape.

4.1.1 Conceptualization: From Data Location to Operational Control

A central consensus across the expert panel was that the definition of Digital Sovereignty is currently fluid and often instrumentalized. While public discourse frequently equates sovereignty with data residency (e.g., storing data in Germany), the experts argued for a more complex definition rooted in operational control.

Consultants (C01, C07) described sovereignty as a "container term," often used interchangeably with resilience or compliance, depending on the stakeholder's agenda. However, a deeper definition emerged from public sector experts (P02, P04, P05), who rejected the notion of absolute autonomy. P05 explicitly framed sovereignty not as independence, but as the "ability to stand up from the negotiation table," implying that sovereignty is the power to manage dependencies rather than eliminate them.

This view was corroborated by C02 and C06, who argued that "absolute sovereignty" is technically impossible given Europe's reliance on non-European hardware supply chains. Instead, the experts aligned on the concept of Operational Sovereignty. P02, P03, and P04 emphasized that sovereignty is a capability, not a product status. As P04 stated: "A Sovereign Cloud without operational capacity is a sovereign logo." This suggests that, without the internal capabilities to manage, encrypt, and migrate workloads, legal jurisdiction over data provides

false security. C01 and C07 further nuanced this by introducing Reversibility as a proxy for sovereignty. They argued that true sovereignty is defined by the existence of an "exit strategy". If a public organization cannot migrate away from a provider due to technical lock-in, it is not sovereign, regardless of where the data is stored.

4.1.2 The Disconnect Between Institutional and Citizen Trust

The analysis revealed a sharp distinction between how trust is constructed at the institutional and citizen levels.

Institutional Trust via Compliance

For public administrations, trust is predominantly a function of compliance and certification. Experts P01, P03, and P04 agreed that frameworks like the BSI C5 catalogue or GDPR compliance are the "base layer" for any cloud adoption. P01 noted that these certifications serve to satisfy internal auditors and legal departments. However, consultants C01 and C05 critiqued this "checklist approach," noting a "compliance paradox" in which fully certified solutions may still lack genuine technical trust due to supply-chain opacity (e.g., foreign access to source code).

Citizen Trust via Experience

In contrast, the experts unanimously agreed that citizens rarely, if ever, evaluate technical sovereignty or certifications (P02, P05, C07). P04 and C04 argued that citizen trust is outcome-based, driven primarily by reliability and usability. P01 provided the critical insight that "outages destroy trust immediately," suggesting that service availability is a stronger predictor of trust than data location. Furthermore, P04 noted that trust is sector-dependent: while citizens may accept risks for administrative services, health data is viewed as "sacred," where a single breach could permanently erode trust. Figure 3 visualizes this structural divergence, highlighting the gap between the supply-side focus on compliance and the demand-side expectation of performance. Experts identified that institutional trust is supply-driven (compliance), while citizen trust is demand-driven (experience).

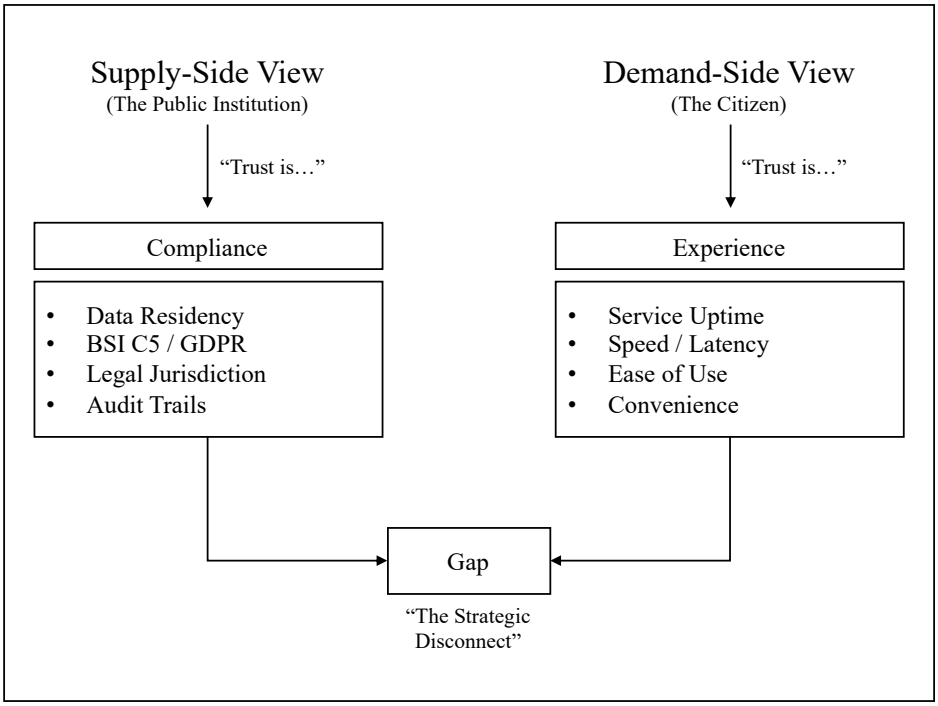


Figure 3: Divergent Trust Models

The Transparency Dilemma

Interestingly, C01 and P03 challenged the assumption that transparency always builds trust. They argued that revealing the full complexity of data flows (e.g., knowing data is encrypted but processed on US hardware) might decrease citizen confidence due to a lack of technical literacy. P03 summarized this tension: "Transparency is tricky; if we show how complex data flows are, trust might drop."

4.1.3 Performance Trade-offs and the Sovereignty Tax.

Experts acknowledged a significant tension between the strategic desire for sovereignty and the practical necessity of performance.

Consultants C02, C06, and Public Sector Expert P04 agreed that European sovereign offerings currently lag behind global hyperscalers (AWS, Microsoft, Google) in terms of feature maturity and scalability. C02 described a "maturity gap," where Sovereign Clouds lack the advanced PaaS (Platform as a Service) capabilities required for modern AI and automation use cases.
This gap creates a trade-off that C01 described as a potential "Sovereignty Tax", the idea that choosing sovereign solutions may result in slower innovation or poorer user experience. P05 and C07 warned that this has direct implications for adoption: if a sovereign service is slow or

cumbersome, citizens will lose trust in the digital state. As C07 noted: “User-friendly services get adopted. People are lazy and choose what is easiest.”

However, P05 offered a counter perspective, arguing that cloud-native architectures (e.g., microservices) enable greater resilience. If implemented correctly, a Multi-Cloud strategy could theoretically offer both sovereignty and performance, though P01 and P02 countered that it would dramatically increase operational complexity.

4.1.4 Drivers and Obstacles for Sovereign Cloud Adoption

To structure the strategic landscape, the drivers and barriers identified in the interviews were aggregated and ranked by frequency of mention.

Table 3: Drivers for Sovereign Cloud Adoption

Rank	Driver	Mentioning Experts	Context / Key Insight
1	**Regulatory Compliance**	P01, P02, P04, C03, C04, C05, C07	Adoption is primarily forced by BSI, GDPR, and sector-specific mandates rather than a voluntary strategy. Compliance is the “base layer.”
2	**Resilience & Scalability**	P01, P02, P05, C01, C05	The need to handle peak loads (e.g., pandemics, elections) drives cloud usage; sovereignty is secondary to the need for operational resilience.
3	**Geopolitical Risk**	C01, C02, P05	External shocks (e.g., war, trade tensions) make dependency reduction a priority; sovereignty is framed as “national resilience.”
4	**Modernization Needs**	C02, C03	Legacy systems are retiring; AI and automation require cloud infrastructure, pushing organizations to accept Sovereign Cloud as a compliant path.

As shown in Table 3, Regulation is the dominant driver. P01 and C04 emphasized that without regulatory mandates, the public sector’s inertia would likely prevent adoption. P05 added that geopolitical risk has recently accelerated this, shifting the narrative from “cost efficiency” to “national resilience.”

Table 4: Obstacles to Sovereign Cloud Adoption

Rank	Obstacle	Mentioning Experts	Context / Key Insight
1	**Skills Shortage**	P01, P02, P03, P04, P05, C01, C06	A critical lack of cloud architects in the public sector prevents "Operational Sovereignty." Organizations cannot manage the stack independently.
2	**Vendor Lock-in**	C01, C02, C03, C07, P03	Structural dependency on US hyperscalers. Lack of "Exit Strategies" undermines the autonomy that sovereignty aims to achieve.
3	**Sovereign Maturity Gap**	C02, C03, C06, P04	European alternatives lack the feature richness (PaaS, AI) of global hyperscalers, creating a trade-off between sovereignty and performance.
4	**Regulatory Ambiguity**	P03, C05	Unclear interpretations of laws (e.g., Data Act) paralyze decision-making; regulation often stops projects rather than enabling them.

Table 4 highlights that the primary obstacle is Organizational Capability, not technology. P04 stated, "We lack cloud architects. Skills are harder to build than infrastructure." This validates the conceptual finding that without the skills to operate the cloud, sovereignty is impossible. Additionally, Vendor Lock-in was heavily emphasized by consultants (C01, C07). They argued that the European market lacks the "industrial scale" (C01: "Europe needs an Airbus moment") required to compete, thereby forcing dependence on non-sovereign vendors that undermines long-term autonomy.

4.1.5 Future Projections: The Hybrid Reality

Looking forward, the consensus among experts (P05, C02, C03, C06) is that a "purist" Sovereign Cloud (100% European hardware and software) is unlikely to become the standard for all workloads. Instead, they project a hybrid Multi-Cloud future.

In this model, outlined by C06 and P05, data is classified by sensitivity: highly critical data (e.g., health, social security) remains in strictly sovereign environments, while commoditized workloads utilize hyperscalers to benefit from innovation. However, P03 and P01 warned that this approach doubles the complexity of governance, requiring a level of organizational maturity that many public agencies currently lack. C07 concluded that sovereignty might eventually become a "quality label" for citizens, but only if the public sector demonstrates that sovereign services are as reliable and user-friendly as their commercial counterparts.

Recent developments in late 2025 suggest the push for independence is accelerating. Experts point to the implementation of the EU Data Act and the scaling of 'AI Gigafactories' as evidence that Europe is moving from regulation to production. Furthermore, initiatives like 'OpenDesk' are emerging as sovereign alternatives to Microsoft, potentially offering the public sector a viable strategy as highlighted by P03.

4.2 Quantitative Findings: Citizen Survey

Following the qualitative expert phase, a quantitative survey was conducted to test the conceptual model on a broader sample of European citizens ($n = 242$). This section details the empirical results, utilizing hierarchical regression analysis to test the direct, mediating, and moderating hypotheses. Prior to hypothesis testing, assumption checks confirmed that multicollinearity was not a concern for the main effects, with Variance Inflation Factors (VIF) remaining well below the threshold of 3.0 for all core constructs.

4.2.1 Descriptive Statistics and Data Distribution

The descriptive analysis of the six core constructs provides the baseline for understanding citizen sentiment (see Table 5).

- **The "Universality of Privacy Risk":** The variable Data Access Concerns yielded the highest mean ($M = 3.96, SD = 0.60$), with a strong negative skewness (-1.20). This confirms that anxiety regarding foreign surveillance is a near-consensus view among the sample. Furthermore, the relatively low standard deviation (SD=0.60) indicates that this is a structural fear shared across demographics, rather than a polarized issue.
- **The "Performance Gap":** In terms of satisfaction levels, Service Performance received the lowest mean rating ($\mathrm{M} = 3.75$). While still positive, respondents rated the current performance of services lower than their perceived trust ($\mathrm{M} = 3.89$) or the importance of sovereignty ($\mathrm{M} = 3.94$). This suggested a "sentiment gap" where the functional experience lags behind normative expectations. The standard deviation ($SD = 0.68$) indicated that this assessment is fairly consistent across the sample. This implied that the 'performance gap' is a structural issue perceived by the majority of users, rather than an isolated complaint from a specific demographic.

Table 5: Descriptive Statistics and Reliability Analysis

Descriptive Statistics

	N	Mean	Std. Deviation	Skewness	
	Statistic	Statistic	Statistic	Statistic	Std. Error
Trust	242	3.8895	.62187	-.795	.156
Perceived sovereignty	242	3.9380	.54233	-1.272	.156
Service performance	242	3.7479	.68848	-.884	.156
Willingness to use	242	3.9408	.52698	-1.003	.156
Clear communication	242	3.7955	.89053	-1.175	.156
Data Access Concerns	242	3.9621	.60375	-1.199	.156
Valid N (listwise)	242				

4.2.2 Drivers of Institutional Trust (H2 & H7)

To test the determinants of Trust, a two-step hierarchical regression was performed (see Table 6). This approach allowed for the isolation of the specific contribution of sovereignty, controlling for communication clarity.

- **Model 1 (Baseline):** In the first step, Perceived Digital Sovereignty was entered as the sole predictor. The model proved highly significant ($F(1, 240) = 155.21, p < .001$), explaining 39.3% of the variance in Trust ($R^2 = .393$). The standardized coefficient ($\beta = .627$) confirms H2, indicating that perceptions of jurisdictional control are a primary antecedent of institutional trust.
- **Model 2 (Communication Added):** In the second step, Clear Communication was added. This addition significantly improved the model's explanatory power ($R^2\Delta = .075$; $R^2 = .468$). While Communication itself is a driver ($\beta = .286$), the impact of Sovereignty remained robust ($\beta = .542$). This implied that clear communication explained an additional 7.5% of the variance in trust, highlighting that transparency is a distinct and valuable driver, separate from the structural guarantee of sovereignty.
- **Interaction Test (H7):** A third model tested the interaction term Sovereignty × Communication. However, this term was statistically non-significant ($p = .117$) and introduced severe multicollinearity (VIF > 60). Therefore, H7 was rejected, clear communication acts as an additive benefit, not a multiplier of sovereignty.

Table 6: Hierarchical Regression Analysis for Drivers of Trust

	Model 1 (Baseline)	Model 2 (Comm. Added)	Model 3 (Interaction)
Main Effects			
Perceived Sovereignty	.627***	.542***	.309
Clear Communication	---	.286***	-.170
Interaction			
Sovereignty x Comm.	---	---	.576 (n.s.)
Model Fit Statistics			
R^2	.393	.468	.473
R^2 Change	---	.075	.005
F-Statistic	155.21***	104.99***	71.25***

4.2.3 Determinants of Willingness-to-use (H1, H3, H4)

To isolate the drivers of adoption, a hierarchical regression analysis was conducted (see Table 7).

- **The Baseline Drivers (Model 1):** In the initial model (excluding control variables), Service Performance ($\beta = .321, p < .001$) and Trust ($\beta = .304, p < .001$) acted as the primary drivers of willingness. This confirmed H1 and H4 as baseline prerequisites. As shown in Figure 4, functional utility and trust initially carry equal weight in driving adoption.
- **The Sovereign Shift (Model 2):** When Perceived Sovereignty was introduced in the final model, the hierarchy of drivers shifted. Sovereignty emerged as the strongest predictor ($\beta = .235, p < .006$), validating H3.
- **Robustness of Performance:** Service Performance remained highly stable and statistically significant ($\beta = .302, p < .001$) even after controlling for sovereignty. This minimal change from the baseline model demonstrates that functional utility is the strongest, most robust driver of adoption. Empirically, this confirmed that if sovereignty measures result in degraded performance, adoption intentions will decline significantly, regardless of the user's ideological preference for data residency.
- **The Trust Redundancy:** Notably, the influence of Trust dropped to non-significance ($\beta = .123, p = .128$) in the whole model. This suggested that sovereignty is such a dominant value proposition that it effectively absorbs the variance previously attributed to general trust.

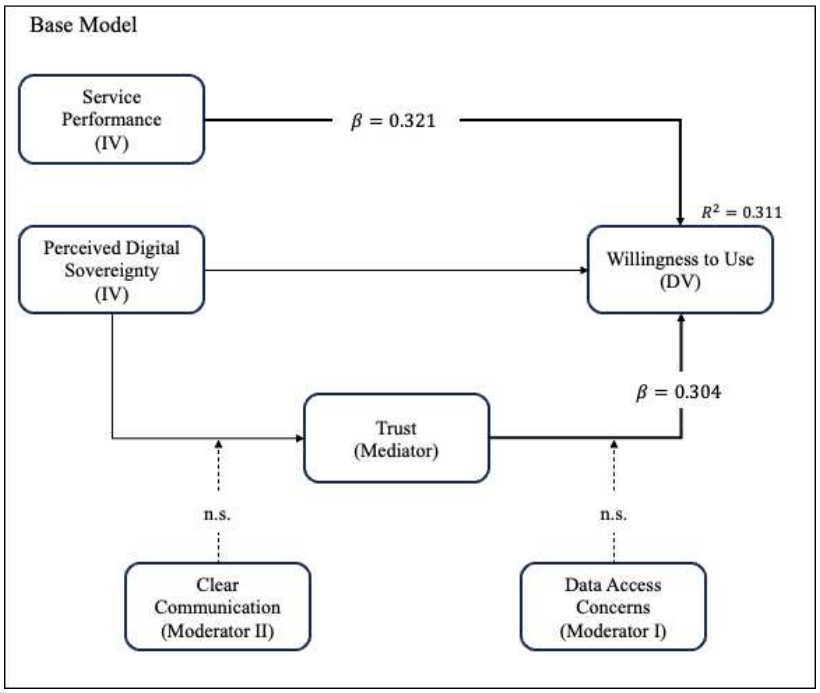


Figure 4: Baseline Path Model (Model 1)

Note: This model illustrates the drivers of willingness before controlling for Perceived Sovereignty. Standardized beta coefficients are shown ($R^2 = .31$).

4.2.4 Mediation Analysis (H5)

H5 posited that Trust mediates the relationship between Perceived Sovereignty and Willingness. To test this, the causal paths were examined using the procedures established by Baron and Kenny (1986). While the first path (Sovereignty → Trust) was significant ($\beta = .627, p < .001$), the second path (Trust → Willingness) became statistically non-significant ($\beta = .123, p = .128$) in the final regression model (see Table 7).

For mediation to be supported, the mediator must remain a significant predictor of the outcome when controlling for the independent variable. Since this condition was not met, H5 was not supported. This indicated that Perceived Sovereignty acts as a dominant driver that supersedes the influence of general institutional trust.

Table 7: Hierarchical Regression Analysis for Willingness-to-use

	Model 1 (Baseline)	Model 2 (Full)
Controls		
Age / Education / Gender	---	Included (n.s.)
Main Effects		
Service Performance	.321***	.302***
Trust	.304***	.123
Sovereignty Effect		
Perceieved Sovereignty	---	.235***
Model Fit		
R^2	.311	.408
R^2 Change	---	.077

4.2.5 Robustness Check: The Impact of Demographics and Risk

To validate the stability of these findings, the model underwent a robustness check by introducing demographic controls (Age, Education) and the risk variable, Data Access Concerns (see Table 7).

- **Insignificance of Demographics:** As shown in the final model, none of the demographic variables (Age groups, Education levels) exerted a significant direct effect on willingness ($p > .200$ for all). This indicated that the positive relationship between sovereignty, performance, and adoption intentions was consistent across the sample, regardless of the respondent's generational cohort or educational background.
- **Rejection of H6 (Risk Moderation):** The hypothesis that Data Access Concerns would weaken the link between trust and adoption (H6) was rejected. The interaction term Trust × AccessConcerns was statistically non-significant ($\beta = .373, p = .384$). This implied that even respondents with high concern regarding foreign surveillance did not significantly alter their usage intentions when trust was present (See Appendix D).

4.2.6 Summary of Quantitative Findings

The empirical analysis culminated in the revised path model shown in Figure 5. The hierarchical regression results highlighted a clear hierarchy of drivers for digital adoption in Europe, characterized by three key findings:

- **Performance is the Primary Driver:** Service Performance emerged as the strongest and most stable predictor of willingness-to-use ($\beta = 0.302$). This indicated that

functional utility (speed, reliability, ease of use) acts as a prerequisite for adoption. While sovereignty is significant, the data suggested it cannot compensate for a lack of basic service performance.

- **Sovereignty is a Direct, Not Just Indirect, Driver:** Contrary to the expectation that sovereignty only builds trust, the results confirmed a significant direct effect of Perceived Digital Sovereignty on adoption ($\beta = 0.235$). Citizens valued the "sovereignty" attribute in its own right, making it a distinct value proposition alongside performance.
- **The Redundancy of General Trust:** The mediation analysis revealed that Trust does not mediate the relationship between Sovereignty and Willingness. In the final model, the influence of general Trust became statistically non-significant ($\beta = .123, p = .128$) when Sovereignty was included. This suggested that the specific assurance of sovereignty effectively absorbs the explanatory power typically attributed to general institutional trust in this context.

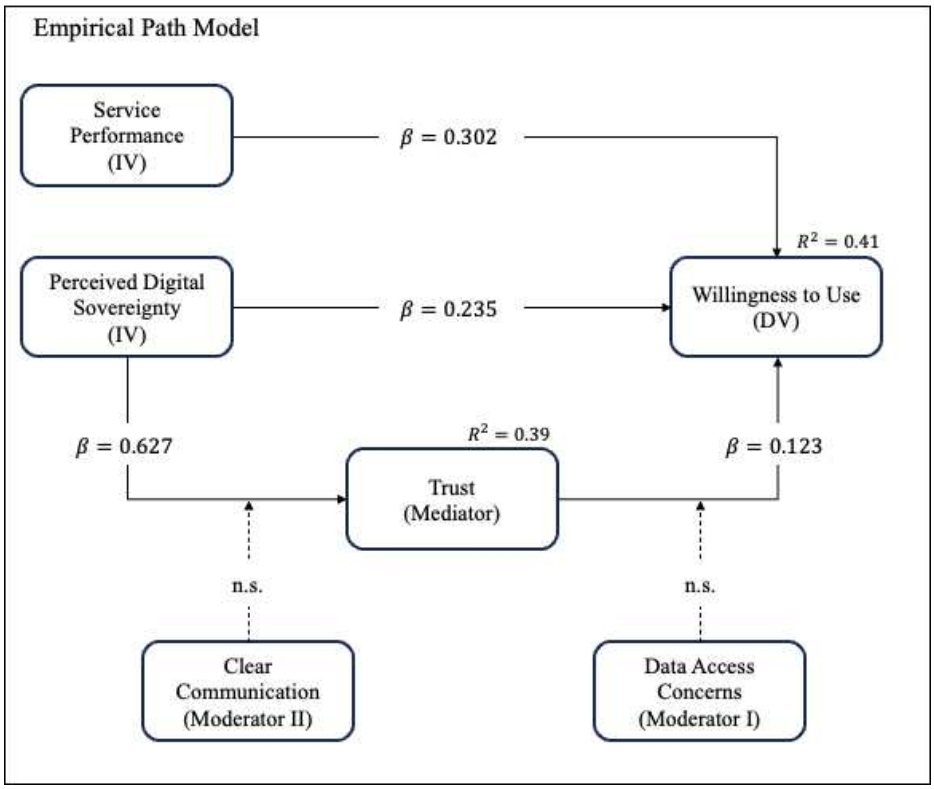


Figure 5: Empirical Path Model

5. Discussion

This chapter integrates the qualitative and quantitative findings to answer the Research Question, interpreting the results through the theoretical lenses of Resource-Based Theory and Dynamic Capabilities.

5.1 Summary of Key Findings

This thesis aimed to answer the Research Question "*How do perceptions of Digital Sovereignty influence European citizens' willingness-to-use sovereign digital public services?"* By adopting a mixed-methods design, the study triangulated the supply-side strategic perspective of industry experts ($n = 12$) with the demand-side perceptions of citizens ($n = 242$). The answer to the Research Question is twofold, revealing a complex Sovereignty Paradox.

First, Digital Sovereignty acts as a primary antecedent of Trust. The quantitative analysis confirmed that Perceived Digital Sovereignty is the strongest driver of Institutional Trust (H2; $\beta = .627, p < .001$). This validates the normative framework proposed by Roberts et al. (2021), who argue that sovereignty is fundamentally about safeguarding European values (such as privacy and the rule of law). The empirical results extend this research by demonstrating that citizens implicitly accept this premise: they interpret the Sovereign label as a credible heuristic for safety, accepting the state's assertion of control as a sufficient basis for trust.

Second, Sovereignty is a direct driver of Adoption, independent of Trust. Crucially, the mediation hypothesis (H5) was not supported. The regression analysis revealed that the direct influence of Perceived Sovereignty ($\beta = .235$) rendered the effect of general Trust non-significant ($\beta = .123, p = .128$). This challenges the assumption often implied in e-government models (based on Mayer et al., 1995) that trust is the sole gateway to adoption. Instead, the results suggest that Digital Sovereignty functions as a distinct value proposition: citizens adopt sovereign services because they value the independence itself, effectively overriding the need for general institutional trust.

5.2 Integration and Interpretation of Findings

To provide a comprehensive answer to the research question, this section combines findings from the interviews, survey, and the literature. By triangulating the supply-side perspective

(strategy and infrastructure) with the demand-side perspective (adoption and trust), four critical themes emerge that define the current state of Digital Sovereignty in Europe.

5.2.1 The Conceptual Ambiguity of Digital Sovereignty: Container Term vs. Trust Signal

A recurrent theme in the literature is the disconnect between the definition of sovereignty and its implementation. As stated in the Literature Review above, Rone (2024) describes sovereignty as a fluid, container term often used in political rhetoric to mask divergent national interests. This linguistic ambiguity was starkly mirrored in the qualitative findings, where experts C01 and C07 criticized sovereignty as a vague signaling device.

However, the quantitative results offer a critical counter-narrative. Despite experts' skepticism about the term's clarity, citizens exhibited a highly coherent response to it. The strong correlation between Perceived Sovereignty and Trust ($\beta = .627$) suggests that the conceptual ambiguity identified by Rone (2024) may be strategically sound. The broadness of the term allows it to function as a catch-all trust signal. This effectively masks the technical dependency described by Bauer et al. (2025), where the rhetorical promise of sovereignty conceals the reality of continued reliance on non-European infrastructure. Citizens appear to trust the label's intent, even if the underlying architecture remains hybrid.

5.2.2 The Primacy of Performance and the Sovereignty Tax

The literature posits a strategic tension between autonomy and efficiency. As stated earlier, Bauer et al. (2025) warn that prioritizing full independence (Digital Autarky) restricts access to advanced hyperscaler technologies, potentially degrading service quality. This trade-off was explicitly termed the “Sovereignty Tax” by Expert C01.

The quantitative results empirically support this trade-off. Service Performance was the single strongest predictor of Willingness-to-use ($\beta = .321$), exerting a significantly larger effect than Sovereignty. This finding empirically validates Venkatesh et al.’s (2003) theoretical assertion that Performance Expectancy is the dominant predictor of intention. It implies that citizens are pragmatic: while they value the normative promise of sovereignty, they will not adopt a service that fails on functional grounds. Consequently, sovereignty cannot serve as a substitute for

utility; legal immunity alone is insufficient to guarantee adoption if the resulting service fails to meet the performance standards of the commercial web.

5.2.3 The Dominance of Sovereignty (Rejection of H5)

H5 posited that Trust would mediate the relationship between sovereignty and adoption. The empirical rejection of this hypothesis offers a compelling insight into the hierarchy of citizen drivers.

The finding that Perceived Sovereignty remains significant while Trust fades suggests a Direct Sovereignty Effect. European citizens appear to view Digital Sovereignty not merely as a background condition for safety, but as a distinct product feature they actively prefer. This implies that the demand for digital independence is ideological rather than purely utilitarian. Strategically, this means governments do not need to wait for “trust to be rebuilt” to drive adoption; they can drive it directly by delivering and clearly labeling sovereign infrastructure.

5.2.4 The Universality of Digital Expectations (Analysis of Controls)

A critical finding is the statistical non-significance of demographic control variables (Age, Education, Gender) within this sample. While "Digital Divide" literature often posits that privacy concerns are stratified by age or education, this study found no significant differences ($p > .200$).

However, given the high digital literacy of the sample (see Section 3.5.3), this does not necessarily disprove the Digital Divide in the broader population. Instead, it suggests a convergence of concern among digitally active citizens.

This implies that for the users of these services, the "Privacy Risk" construct defined by Dinev and Hart (2006) is universal. The fear that foreign entities might access personal data is not limited to niche privacy activists; it appears to be a structural baseline fear shared by both the digital native and the digitally literate older generations. Consequently, for the target demographic of e-government services, the expectation of sovereignty is homogeneous.

5.2.5 Conceptual Overlap: Why Interactions Failed

The rejection of the interaction hypotheses (H6, H7), coupled with high multicollinearity with the "Clear Communication" variable, offers a methodological insight. It suggests that citizens do not view transparency as a separate moderator. In the user's mind, Sovereignty includes Communication. A government that claims to be engaging in a sovereign activity but fails to explain how this is the case is perceived as less sovereign. This implies that communicative transparency is intrinsic to the construct of sovereign actions.

5.3 Theoretical Implications

This study advances theoretical understanding of digital government by empirically validating the distinction between a strategic resource (RBT) and operational capability (DC).

5.3.1 RBT: Validating the VRIN Attributes

By applying Resource-Based Theory (Barney et al., 2021) to the public sector, this study empirically validates that Digital Sovereignty functions as a VRIN resource (Barney, 1991). The findings confirm three specific dimensions of the framework:

1. **Validating Non-Substitutability (The Demand for Immunity)**
   Section 2.4 theorized that Sovereignty is "Non-substitutable" because technical measures cannot replace legal immunity. The quantitative findings confirmed this. The high "Data Access Concerns" score ($M = 3.96$) indicates that citizens do not view technical security alone as sufficient. The finding that Perceived Sovereignty drives adoption ($\beta = .235$) independently of performance proved that citizens treat the legal condition of immunity as a distinct, non-substitutable value that cannot be replaced by the technical measures (e.g., encryption) offered by US hyperscalers.
2. **Validating Inimitability (The Social Complexity Link)**
   Second, the results confirmed that Sovereignty is "Inimitable" due to Social Complexity. The expert interviews revealed that the Sovereign Operating Model requires deep institutional competence to manage. The positive impact of sovereignty on adoption suggested that citizens value this complex management regime. They recognize that while US firms can replicate the infrastructure, they cannot replicate the legal condition of immunity due to their structural disqualification under FISA. The

state leverages this inimitability to establish a unique institutional legitimacy, offering a “Safe Harbor” for sensitive data.

3. **Validating Rarity (The Performance Gap)**
   Finally, the observed “Performance Gap” (Section 4.2.3) empirically validated the Rarity dimension. Because high-performance sovereign providers are scarce in the European market (Supply-Side Scarcity), the state is currently forced to pay a Sovereignty Tax on performance to access this rare resource.

5.3.2 Dynamic Capabilities: Explaining the “Failure” (The Orchestration Gap)

While the RBT explains the strategic intent (acquiring the asset), the DC framework enables the elaboration on operational failure. The results indicated that while the state possesses the resource of Digital Sovereignty (providing Jurisdictional Immunity), it fails to deploy it effectively. This study diagnosed this as an Orchestration Gap where the public sector's strategy breaks down at the execution layer.

The Diagnosis of Failure

First, the identification of the Sovereignty Tax provided empirical evidence of the Asset-Competence Gap theorized by Chen et al. (2024). They argue that possessing an IT asset (Level 1) is useless without the operational competence (Level 2) to mobilize it. The expert interviews (e.g., P04, C01) confirmed this precise gap: the public sector has successfully seized the Level 1 Asset (Sovereign Cloud contracts) but lacks the Level 2 Operational Competence (cloud architecture skills) required to integrate it. As Chen et al. predict, this gap results in a failure to generate value, manifesting here as the trade-off between security and usability.

The Process Failure

Second, applying Teece’s (2007) Micro foundations revealed that this is not a total strategic failure, but a specific breakdown in the “Transforming” stage.

- **Sensing:** The state successfully identified the external threat (e.g., US CLOUD Act).
- **Seizing:** The state successfully mobilized resources to procure sovereign infrastructure (e.g., “Cloud de Confiance”).
- **Transforming (The Failure):** The state failed to “reconfigure” its internal human capital and organizational routines to manage this new infrastructure. By procuring the

tool without restructuring the workforce to operate it, the state stalls at the "Seizing" phase.

The Structural Flaw

Finally, the "episodic" nature of this procurement, viewing sovereignty as a one-time purchase rather than a continuous process, violates Barreto's (2010) criterion of "systematicity." Barreto argues that a true dynamic capability must be an embedded, repeatable routine. The reliance on external consultants and the lack of internal "exit strategies" (Expert C07) indicated that sovereignty has not yet become a systematic organizational capability. Instead, it remains a static asset, leaving the state unable to adapt to the rapid evolution of the cloud market.

5.4 Policy and Practical Implications

1. **Managing the Sovereignty Tax:**
   The dominance of Service Performance ($\beta = .321$) implied that public sector leadership and digital strategists must avoid "Sovereignty-at-all-costs" approaches. If a strictly sovereign solution results in poor User Experience (UX), citizens will reject it. The pragmatic path is a Hybrid Cloud architecture: strictly sensitive data remains in sovereign silos, while non-sensitive interactions leverage the speed of commercial hyperscalers.
2. **Sovereignty as a Communication Strategy:**
   The "Conceptual Overlap" finding (Section 5.2.5) implied that transparency is a core component of the product. Public administrations should implement standardized "Sovereignty Labels" (e.g., "Hosted in EU") to clearly communicate the value proposition. Since citizens cannot distinguish between technical reality and communicated promise, explicit signaling is necessary to convert legal sovereignty into citizen trust.
3. **Addressing the Universal User:**
   Policy narratives must shift from complex legalistic arguments to simple value propositions. The lack of demographic variance suggested that sovereignty is a baseline requirement for the general population, not just a niche concern for the "digital elite." Therefore, sovereign features should be marketed as a standard guarantee of quality for all users, rather than a premium feature for privacy-conscious experts.

5.5 Limitations and Future Research

5.5.1 Methodological Limitations and Sample Bias

First, the quantitative sample ($n = 242$) showed a demographic bias toward highly educated (65% with a bachelor's degree) and male (64%) respondents. This range restriction likely explains why demographic controls were non-significant in Section 5.2.4.

Although the results suggest that privacy concerns are uniform among digitally literate users, they cannot be generalized to the offline or lower-literacy population. Future research should target a broader cross-section of the citizenry to determine whether a Sovereignty Gap exists among socioeconomic groups.

Second, the qualitative expert sample ($n = 12$) was heavily concentrated in the German public sector ecosystem. Furthermore, several of these experts collaborate closely as part of a voluntary, cross-agency initiative advocating for Sovereign Cloud adoption. This professional interconnectedness implies that the strong consensus observed regarding the Sovereignty Tax and operational challenges may be partially attributable to a shared institutional narrative, or "groupthink," within this specific network, which may not fully reflect the views of unconnected agencies.

5.5.2 Construct Ambiguity and Measurement

The study encountered challenges in operationalizing "Digital Sovereignty," mirroring the container term ambiguity found in the literature. While internal consistency was acceptable (Cronbach's $\alpha > .70$), the extreme multicollinearity with Communication suggests the constructs were not empirically distinct to citizens. Future research should refine these scales to distinguish between legal sovereignty (jurisdiction) and operational sovereignty (technical control).

5.5.3 Research Design and Causality

Finally, the cross-sectional design of the quantitative survey limits causal inference. While the regression models identified significant associations between sovereignty, trust, and willingness-to-use, they could not definitively establish the direction of causality. For instance, it is theoretically possible that citizens with higher pre-existing trust are more likely to perceive the state as sovereign. Future studies could employ longitudinal designs or experimental setups (e.g., A/B testing different sovereignty labels) to isolate the causal impact of sovereign attributes on user adoption.

6. Conclusion

This final chapter synthesizes the study's findings to address the core tension between state security and citizen adoption.

6.1 The Sovereignty Paradox Resolved

This thesis set out to explore the tension between the strategic pursuit of Digital Sovereignty by European states and the adoption determinants of their citizens. While the political discourse has largely framed Digital Sovereignty as a legal and diverse container term, this study provides empirical clarity on its actual role in the digital society. The research revealed a Sovereignty Paradox: while sovereignty is the primary architect of institutional trust, it is insufficient on its own to drive digital adoption.

The triangulation of data confirmed that European citizens are not indifferent to the geopolitical origin of the cloud infrastructure underpinning public services. They view Digital Sovereignty as a distinct value proposition, a "trust signal" that the state is acting as a protective guardian. This finding corrects the prevailing expert assumption that sovereignty is merely a backend compliance issue; instead, the data reveal that for citizens, it is a foreground product feature that directly influences adoption. However, the study also exposed a critical Orchestration Gap within the public sector. The state has successfully secured the resource of legal sovereignty but lacks the dynamic capability to deliver it without compromising service performance. As a result, citizens are currently forced to trade usability for security, a Sovereignty Tax that ultimately depresses adoption.

6.2 Implications for the Digital State

The findings imply that the current "compliance-first" approach to Digital Sovereignty is strategically incomplete. For the European public sector, the era of defining sovereignty solely through data residency and legal jurisdiction must end.

- **From Law to Operations**: Sovereignty must be redefined as an operational capability. A Sovereign Cloud that crashes or lags is, in the eyes of the citizen, a failed state service. Investments must shift from legal audits to cloud architecture skills.
- **From Ideology to Utility**: Among digital users, the generation gap regarding privacy has closed. The demand for sovereign, high-performing services is consistent across demographics. Governments can no longer treat privacy-preserving infrastructure as a

niche product for the "digital elite"; it must be the standard quality baseline for all citizens engaging with the digital state.

6.3. Final Outlook

Ultimately, this thesis argued that Strategic Management logic applies to the public sector: the state must compete for digital engagement. As supported by Piening's (2013) application of dynamic capabilities to public organizations, possessing a resource is insufficient without the capability to deploy it. Digital Sovereignty offers Europe a unique, inimitable resource, but only if it is orchestrated effectively.

If Europe continues to view sovereignty merely as a defensive shield, it risks building a "Fortress Europe" of secure but unused digital services. However, if it can close the capability gap and deliver Sovereignty with Performance, it has the potential to establish a social contract for the digital age, proving that a democracy can be both sovereign and perform effectively.

References

Ajayi, A. J., Agbede, O. O., Akhigbe, E. E., & Egbuhuzor, N. S. (2024). Enhancing Public Sector Productivity with AI-Powered SaaS in E-Governance Systems. *International Journal of Multidisciplinary Research and Growth Evaluation*, *5*(1), 1243–1259. https://doi.org/10.54660/.ijmrge.2024.5.1-1243-1259

Atobishi, T., Bakir, S. M. A., & Nosratabadi, S. (2024). How do digital capabilities affect organizational performance in the public sector? The mediating role of the organizational agility. *Administrative Sciences*, *14*(2), 37. https://doi.org/10.3390/admsci14020037

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99–120. https://doi.org/10.1177/014920639101700108

Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, *51*(6), 1173–1182. https://doi.org/10.1037/0022-3514.51.6.1173

Barney, J. B., Ketchen, D. J., & Wright, M. (2021). Resource-Based Theory and the Value Creation framework. *Journal of Management*, *47*(7), 1936–1955. https://doi.org/10.1177/01492063211021655

Barreto, I. (2010). Dynamic Capabilities: a review of past research and an agenda for the future. *Journal of Management*, *36*(1), 256–280. https://doi.org/10.1177/0149206309350776

Bauer, M., Dugo, A., Pandya, D., Sharma, V., & Sisto, E. (2025). Boosting efficiency and quality in EU public services: The need for a European multi-cloud-first strategy. In *ECIPE Occasional Paper* (Report No. 04/2025). European Centre for International Political Economy (ECIPE). Retrieved December 27, 2025, from https://hdl.handle.net/10419/315166

BfDI. (2020). *Datenübermittlungen in die USA und Schrems II Urteil*. BFDI. Retrieved December 23, 2025, from https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Auswirkungen-Schrems-II-Urteil.html

Blancato, F. G. (2023). The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. *Policy & Internet*, *16*(1), 12–32. https://doi.org/10.1002/poi3.358

Blancato, F. G., & Carr, M. (2024). The trust deficit. EU bargaining for access and control over cloud infrastructures. In *Journal of European Public Policy* [Journal-article]. https://doi.org/10.1080/13501763.2024.2441418

Boston Consulting Group. (2025a, June 25). *https://www.bcg.com/publications/2025/sovereign-clouds-reshaping-national-data-security*. BCG. Retrieved December 23, 2025, from https://www.bcg.com/publications/2025/sovereign-clouds-reshaping-national-data-security

Boston Consulting Group. (2025b, July 29). *Cloud cover: price swings, sovereignty demands, and wasted resources*. BCG. Retrieved December 23, 2025, from https://www.bcg.com/publications/2025/cloud-cover-price-sovereignty-demands-waste

Bryman, A., & Bell, E. (2015). *Business research methods*. Oxford University Press, USA.

Bundesregierung. (2025, November 18). *Summit on European Digital Sovereignty Delivers Landmark Commitments for a more competitive and sovereign Europe*. Die Bundesregierung. Retrieved December 27, 2025, from https://www.bundesregierung.de/breg-de/aktuelles/summit-on-european-digital-sovereignty-delivers-landmark-commitments-for-a-more-competitive-and-sovereign-europe-2394368

Celeste, E. (2021). Digital Sovereignty in the EU: challenges and future perspectives. In Federico Fabbrini, Edoardo Celeste and John Quinn (Ed.), *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*. https://doras.dcu.ie/25498/1/Celeste_DigitalSovereigntyintheEU.pdf

Chen, C. S., Liu, G., Roushan, G., & Nguyen, B. (2024). Exploring Information Technology Capabilities from Multiple Aspects of the Resource-Based Theory. *Information Systems Frontiers*, *27*(3), 1013–1043. https://doi.org/10.1007/s10796-024-10490-1

Clark, V. L. P., & Ivankova, N. V. (2017). *Mixed Methods Research: A Guide to the field*. https://doi.org/10.4135/9781483398341

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Crawford, M. B. (2025, December 10). Ownership of the means of thinking. *Commonplace*. https://www.commonplace.org/p/matthew-b-crawford-ownership-of-the

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf

Culnan, M. J., ∗, & Bies, R. J. (2003). Consumer Privacy: Balancing economic and justice considerations. In The Society for the Psychological Study of Social Issues, *Journal of Social Issues* (Vol. 59, Issue 2, pp. 323–342).

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Doran, N. M., Puiu, S., Bădîrcea, R. M., Pirtea, M. G., Doran, M. D., Ciobanu, G., & Mihit, L. D. (2023). E-Government Development—A key factor in government administration effectiveness in the European Union. *Electronics*, *12*(3), 641. https://doi.org/10.3390/electronics12030641

Dubois, A., & Gadde, L. (2002). Systematic combining: an abductive approach to case research. *Journal of Business Research*, *55*(7), 553–560. https://doi.org/10.1016/s0148-2963(00)00195-8

Etikan, I. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1. https://doi.org/10.11648/j.ajtas.20160501.11

European Commission. (2025). State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future. In *European Commission*. Retrieved December 27, 2025, from https://digital-strategy.ec.europa.eu/en/library/state-digital-decade-2025-report

Filip, B. F. (2023). THE DIGITALIZATION PROCESS OF PUBLIC ADMINISTRATION IN EUROPEAN UNION: ADVANCES AND PERSPECTIVES. *Journal of Public Administration Finance and Law*, *29*, 140–149. https://doi.org/10.47743/jopafl-2023-29-13

Floridi, L. (2020). The fight for Digital Sovereignty: what it is, and why it matters, especially for the EU. *Philosophy & Technology*, *33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Gupta, P., & Chauhan, S. (2024). Factors Influencing Trust in E-government Services: A Meta-analytic Review. In *Tenth International Conference on eDemocracy & eGovernment (ICEDEG)* (pp. 1–10). https://doi.org/10.1109/icedeg61611.2024.10702083

Hair, J. F., Black, W., Babin, J., & Anderson, E. (2010). *Multivariate data analysis*. Pearson.

Hildén, J. (2021). Mitigating the risk of US surveillance for public sector services in the cloud. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1578

Hinkley, S. (2023, January 10). *Technology in the public sector and the future of government work*. UC Berkeley Labor Center. Retrieved December 23, 2025, from https://laborcenter.berkeley.edu/technology-in-the-public-sector-and-the-future-of-government-work/

ISO/IEC. (2023). *Information technology — Cloud computing — Part 2: Concepts*.

Kallio, H., Pietilä, A., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965. https://doi.org/10.1111/jan.13031

Likert, R. (1932). A technique for the measurement of attitudes. *Medical Entomology and Zoology*, *140*, 5–55. https://ci.nii.ac.jp/naid/10020252871

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review*, *20–20*(3), 709–734. https://www.jstor.org/stable/258792

Mayring, P. (2014). Qualitative content analysis: theoretical foundation, basic procedures and software solution. *Social Science Open Access Repository (GESIS – Leibniz Institute for the Social Sciences)*, 143. http://www.ssoar.info/ssoar/handle/document/39517

Mergel, I., Ganapati, S., & Whitford, A. B. (2020). Agile: a new way of governing. *Public Administration Review*, *81*(1), 161–165. https://doi.org/10.1111/puar.13202

Moore, M. H. (2021). Creating public value: the core idea of strategic management in government. *International Journal of Professional Business Review*, *6*(1), e219. https://doi.org/10.26668/businessreview/2021.v6i1.219

Morgan, R. M., & Hunt, S. D. (1994). The Commitment-Trust theory of relationship Marketing. *Journal of Marketing*, *58*(3), 20. https://doi.org/10.2307/1252308

Muhic, M., & Bengtsson, L. (2021). Dynamic capabilities triggered by cloud sourcing: a stage-based model of business model innovation. *Review of Managerial Science*, *15*(1), 33–54. https://doi.org/10.1007/s11846-019-00372-1

Piening, E. P. (2013). Dynamic capabilities in public organizations. *Public Management Review*, *15*(2), 209–245. https://doi.org/10.1080/14719037.2012.708358

Pohle, J., & Thiel, T. (2020). Digital Sovereignty. *Internet Policy Review*, *9*(4). https://ssrn.com/abstract=4081180

Putri, A. (2025). Multi-Cloud strategies for managing big data workflows and AI applications in decentralized government systems. In *Journal of Computational Intelligence for Hybrid Cloud and Edge Computing Networks* (pp. 1–2).

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with Digital Sovereignty: an analysis of statements and policies. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1575

Rone, J. (2024). 'The Sovereign Cloud' in Europe: diverging nation state preferences and disputed institutional competences in the context of limited technological capabilities. *Journal of European Public Policy*, *31*(8), 2343–2369. https://doi.org/10.1080/13501763.2024.2348618

Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students, 8th ed. In *Pearson eBooks*. http://dspace.uniten.edu.my/handle/123456789/18304

Teece, D. J. (2007). Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, *28*(13), 1319–1350. https://doi.org/10.1002/smj.640

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, *18*(7), 509–533. https://doi.org/10.1002/(sici)1097-0266(199708)18:7

Veneziano, M. (2025). Pragmatism over sovereignty? The Italian policy response to the infrastructuralization of non-EU cloud service providers. *Critical Policy Studies*, *19*(3), 395–413. https://doi.org/10.1080/19460171.2024.2384605

Venkatesh, V., Morris, G., Davis, B., & Davis, D. (2003). User acceptance of information Technology: toward a unified view. *MIS Quarterly*, *27*, 425–478. https://www.jstor.org/stable/30036540

World Economic Forum. (2025, January 10). *What is Digital Sovereignty and how are countries approaching it?* Retrieved December 23, 2025, from https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

Appendices

Appendix A: Expert Interview Guide

The following semi-structured interview guideline served as the basis for the data collection. While the core questions remained consistent to ensure comparability, the specific focus was adapted based on the expert's background (Strategic Consultant vs. Public Sector IT Decision Maker). The guide focuses on five thematic blocks: Strategy, Trade-offs, Trust, Organization, and Future Outlook.

Block	ID	Main Question	Intention / Probe
1. Introduction & Context	**1.1**	Could you briefly outline your role and your organization's specific touchpoints with cloud infrastructure?	*Context setting: Decision-maker vs. Advisor.*
	1.2	"Digital Sovereignty" is a term interpreted differently by almost everyone. How is the term defined or operationally understood in your specific environment?	*To capture variation: Data residency (legal) vs. Operational independence (technical).*
	1.3	Has the strategic importance of this topic changed in the last 3–5 years? If so, what was the "trigger event"?	*Probe: Impact of geopolitical shifts, COVID-19, or regulations (Schrems II).*
2. Drivers & Motivation	**2.1**	What are the primary reasons for your organization (or your clients) to consider "Sovereign Cloud" solutions right now?	*Differentiation: Is it strictly Compliance (GDPR) or Strategic Autonomy?*
	2.2	To what extent is the move to the cloud driven by a "Modernization Imperative" (e.g., retiring legacy systems) rather than sovereignty itself?	*To identify if sovereignty is just a constraint in a broader modernization project.*
	2.3	How do you balance the need for "Resilience" (technical uptime) against the need for "Sovereignty" (legal immunity)? Are these goals ever in conflict?	*To explore if sovereignty measures (e.g., isolation) are perceived to reduce resilience.*
3. Market & Trade-offs	**3.1**	How do you assess the current maturity of European Sovereign Cloud offerings compared to US Hyperscalers (AWS/Azure)?	*To let the expert identify "performance gaps" or "feature parity" naturally.*
	3.2	In practice, do you see a "functional gap"? For example, are there advanced features (AI, PaaS) that are simply not available in sovereign environments?	*To probe for the "Sovereignty Tax" concept without using the term directly.*

	3.3	How does your organization handle the risk of "Vendor Lock-in" or dependency? Is there a tangible "Exit Strategy"?	*To discuss Multi-Cloud strategies and the feasibility of switching providers.*
4. Trust & The Citizen	**4.1**	From your perspective, does the physical location of data storage play a role in the trust citizens have in digital public services?	*To test the link between Sovereignty and Citizen Trust.*
	4.2	Do you believe citizens differentiate between a "Sovereign Cloud" and a standard cloud, or do they prioritize other factors like Usability or Speed?	*To probe if "Performance/UX" outweighs "Sovereignty" for the end-user.*
	4.3	Does transparency regarding data flows (e.g., explaining encryption) build trust, or does complexity potentially erode it?	*To explore the "Transparency Paradox" (complexity = distrust).*
5. Implementation Barriers	**5.1**	It is often said, "You are only sovereign if you can operate it yourself." Does the public sector currently have the internal skills to manage these environments?	*To identify the "Skills Gap" and "Orchestration" challenges.*
	5.2	Beyond technology, what are the organizational hurdles? (e.g., Procurement processes, Governance structures, Cultural resistance).	*To identify non-technical barriers like rigid tender processes.*
	5.3	How do certifications like BSI C5 influence the decision-making process? Are they helpful guidance or bureaucratic hurdles?	*To assess the role of regulation as a barrier or enabler.*
6. Future Outlook	**6.1**	Do you believe Europe will ever develop a hyperscaler competitive on a global scale (an "Airbus for Cloud"), or is that window closed?	*To capture market pessimism vs. optimism.*
	6.2	Looking 5 years ahead: Will the public sector be "Sovereign," or will we see a "Managed Dependency" model where we live with US providers?	*To capture the predicted end-state.*

Appendix B: Qualitative Coding Manual

This appendix outlines the category system used to analyze the expert interviews (n=12). Table B.1 details the coding rules and exclusion criteria to ensure inter-coder reliability. Table B.2 provides examples of how raw interview data were mapped to these categories.

Table B.1 *Category System, Coding Rules, and Exclusion Criteria*

Category / Subcategory	Definition	Anchor Example	Coding Rule (Use when...)	Exclusion Rule (Do not use when...)
A. Digital Sovereignty				
A1 – Interpretation	Definitions of meaning (jurisdiction, autonomy, control).	*"There is no universal definition..." (C01)*	Interviewees describe what sovereignty *is* .	Exclude reasons to adopt (see A2).
A2 – Drivers	Why sovereignty is pursued (resilience, dependency).	*"COVID was a big trigger." (C01)*	Motivations, benefits, or triggers are expressed.	Exclude specific blockers (see A3).
A3 – Barriers	Feasibility limitations (cost, uncertainty).	*"C5 compliance is confusing." (C01)*	Concerns or feasibility limitations are mentioned.	Exclude adoption incentives (see A2).
A4 – Operational Capability	Ability to operate independently (skills, governance).	*"A sovereign cloud without operations is just a logo." (P04)*	Sovereignty is linked to capability/maturity.	Exclude pure definitions (see A1).
B. Trust				
B1 – Trust-Building	Mechanisms that increase trust (transparency, certs).	*"Trust comes from proven operation." (C01)*	Mechanisms that strengthen trust appear.	Exclude signals that erode trust (see B2).
B2 – Trust Erosion	What reduces trust (complexity, fear).	*"Unclear data handling reduces trust." (P02)*	Risk perception, doubt, or distrust signals.	Exclude positive trust signals (see B1).
C. Service Performance				
C1 – Advantages	Reliability, scalability, speed benefits.	*"Performance from hyperscalers is impressive." (P04)*	Performance/Utility advantages are highlighted.	Exclude fear of outages (see C2).
C2 – Concerns	Integration challenges, technical limitations.	*"Sovereign solutions lag behind." (P03)*	Technical weaknesses or gaps are described.	Exclude pure trust risks (see B2) or dependency (see G2).
D. Citizen Impact				
D1 – Trust Response	How outcomes affect citizen trust.	*"Outages destroy trust immediately." (P01)*	Explaining citizen trust behavior/reaction.	Exclude internal institutional trust (see B1).
D2 – Concerns & Fears	Perceived public worries (foreign control, UX).	*"People want digital services fast." (P04)*	Fears or specific citizen concerns are foregrounded.	Exclude technical risks unless linked to citizens (see C2).
E. Adoption Willingness				
E1 – Drivers	Factors increasing likelihood of usage.	*"User-friendly services get adopted." (C07)*	Approval or willingness conditions are stated.	Exclude pure performance evaluation (see C1).
E2 – Barriers	Factors decreasing citizen willingness.	*"If transparency shows complexity, trust drops." (C01)*	Rejection conditions or reluctance are stated.	Exclude general concerns unless linked to adoption.
F. Org. Readiness				
F1 – Skills & Maturity	Talent, architecture readiness.	*"We lack cloud architects." (P04)*	Skills or internal maturity are mentioned.	Exclude political focus.
F2 – Change Ability	Migration, procurement, governance.	*"The organization is the blocker." (P02)*	Organizational resistance/change issues appear.	Exclude market ecosystem issues (see G).
G. Market & Strategy				
G1 – Landscape	Competition balance, EU vs US scale.	*"Europe needs an Airbus moment." (C01)*	Power balance or ecosystem competition.	Exclude lock-in specific risks (see G2).
G2 – Lock-In	Exit limitations, dependency risk.	*"Vendor lock-in leaves no exit options." (C01)*	Dependency or exit risk is central.	Exclude technical failure (see C2).
H. Regulation				
H1 – Drivers	Compliance pushing adoption.	*"Compliance drives decisions." (P04)*	Laws/Mandates push sovereignty.	Exclude internal motivation.
H2 – Ambiguity	Legal uncertainty blocking progress.	*"Regulation stops more projects than tech." (P03)*	Regulation slows or blocks progress.	Exclude capability issues (see F).

Table B.2 *Coding Application Examples (Excerpt)*

ID	Original Quote	Code	Memo / Interpretation
P05	*"Digital sovereignty is the ability to stand up from the negotiation table."*	**A1**	Sovereignty re-framed not as autarky, but as "Strategic Negotiation Power" (Managed Dependency).
C02	*"Full technological independence is unrealistic due to global supply chains."*	**A1**	Codes "Realism" vs. "Purism" - rejection of the absolute sovereignty definition.
C01	*"COVID was a big trigger - resilience suddenly became a priority."*	**A2**	Identifying "External Shocks" (Pandemic) as the primary catalyst for adoption, shifting from legal to operational drivers.
P04	*"A Sovereign Cloud without operational capacity is just a sovereign logo."*	**A4**	Distinction between "Nominal Sovereignty" (Label) and "Operational Sovereignty" (Capability).
C06	*"True sovereignty is the ability to operate without the provider - and that is rare."*	**A4**	Sovereignty linked to "Reversibility" and exit capability.
C01	*"Trust comes from proven operation, not just certifications."*	**B1**	Trust formation linked to empirical evidence (uptime) rather than formal labels (C5).
P03	*"Transparency is tricky - if we show how complex data flows are, trust might actually drop."*	**B2**	The "Transparency Paradox": Complexity acts as a trust erosion factor.
P01	*"Cloud helps us scale services when demand explodes - elections, pandemics."*	**C1**	"Elasticity" identified as the functional advantage overriding sovereignty concerns.
C01	*"A hyperscaler with encryption is better than a German provider without know-how."*	**C1**	Performance/Competence trade-off: Functionality is prioritized over strict jurisdiction.
C03	*"Local sovereign providers are still behind hyperscalers in technical maturity."*	**C2**	The "Sovereignty Tax": Identifying the functional gap/cost of choosing sovereign options.
P01	*"Outages destroy trust immediately. Users remember that for years."*	**D1**	Citizen trust is coded as "Fragile" and "Outcome-based" (Reliability) rather than "Origin-based".
C07	*"Citizens don't think in sovereignty terms - they think security, simplicity, availability."*	**D2**	Rejection of the hypothesis that sovereignty is a direct citizen demand.
C07	*"User-friendly services get adopted - people are lazy and choose what is easiest."*	**E1**	"Usability" (UX) coded as the primary determinant of adoption willingness.

P04	*"We lack cloud architects - skills are harder to build than infrastructure."*	**F1**	The "Orchestration Gap": Internal human capital identified as the binding constraint.
P02	*"The technology is not the blocker - the organization is."*	**F2**	"Organizational Inertia" coded as a stronger barrier than technical feasibility.
C01	*"Europe needs an Airbus moment - we lack scale to compete."*	**G1**	Market structural analysis: Sovereignty requires industrial scale.
C03	*"Vendor lock-in is a real concern - exit capability matters."*	**G2**	Dependency risk coded as the strategic counterargument to hyperscaler adoption.
P03	*"Regulation stops more projects than technology ever did."*	**H2**	"Regulatory Ambiguity" coded as a paralysis factor in public sector decision-making.

Appendix C: Survey Design

Appendix C.1: Survey Instrument Items

#	Question	Question Type	Answer Options
Welcome & Screening			
1	Do you agree to take part in this anonymous survey?	Multiple choice	No (1); Yes (2)
2	Do you currently live in a country of the European Union (EU) or the EEA?	Multiple choice	No (1); Yes (2)
Use of Online Public Services			
3	In the past 12 months, have you used any online public services?	Multiple choice	Yes (1); No (2); Not sure (3)
4	How often do you use online public services?	Multiple choice	Never (1); Once a year (2); A few times a year (3); Monthly (4); Weekly or more (5)
5	Which types of online public services have you used in the past 12 months?	Multiple choice (multiple selection)	Filing taxes online; Accessing health insurance/records; Applying for social benefits; Requesting documents; Municipal services; Scheduling appointments; Other; I have not used any
Trust - Ability & Reliability			
6	How much do you agree with the following statements about online public services? • Online public services usually function as expected. • The government has the technical ability to keep my data secure. • Online public services work reliably. • Problems with online services are resolved in a reasonable amount of time.	5-point Likert scale matrix	Strongly disagree (1) – Strongly agree (5)
Trust - Honesty & Fairness			
7	How much do you agree with the following statements? • The government tries to handle personal information responsibly. • Rules about data protection are followed properly. • The government aims to protect citizens' rights. • Rules are applied fairly.	5-point Likert scale matrix	Strongly disagree (1) – Strongly agree (5)
Digital Sovereignty			
8	How much do you agree with the following statements? • My data in online public services is mainly stored in Europe. • European laws decide who can access my data.	5-point Likert scale matrix	Strongly disagree (1) – Strongly agree (5)

	• It is important to me that access to my data is governed by European laws. • It should be possible to see who has accessed my data. • I would feel more comfortable if my data stayed in Europe. • The government should not rely on a single technology provider. • The government should be able to switch providers if needed.		
9	Before today, how familiar were you with the idea of your data being stored inside or outside Europe?	5-point Likert scale	Not familiar at all (1) – Extremely familiar (5)
Concerns			
10	How much do you agree with the following statements? • I am concerned that non-European companies might access my data. • I am concerned that my data could be moved outside Europe. • News about data breaches makes me more cautious about using online services. • I prefer European providers even if I do not know them well. • I am concerned about dependency on a single technology provider. • I am concerned that foreign laws could influence who can access my data.	5-point Likert scale matrix	Strongly disagree (1) – Strongly agree (5)
11	Have you ever avoided using an online public service because of privacy or security concerns?	Multiple choice	Yes (1); No (2); Not sure (3)
Service Performance			
12	How much do you agree with the following statements about online public services? • Online services are fast. • Online services are easy to use. • Tasks can generally be completed without errors. • I am satisfied with the online public services I have used. • Online services are available when I need them.	5-point Likert scale matrix	Strongly disagree (1) – Strongly agree (5)
13	Compared to in-person services, do you expect online public services to work better or worse?	5-point Likert scale	Much worse (1) – Much better (5)
Willingness to Use			
14	How much do you agree with the following statements? • I prefer using online services when possible. • I would recommend online public services to others. • Knowing that my data stays in Europe would increase my willingness to use online services.	5-point Likert scale matrix	Strongly disagree (1) – Strongly agree (5)

	• I am comfortable using online services for sensitive data if security is strong. • If an online service is very easy and fast, I might use it even if I do not know exactly where the data is stored.		
15	How likely are you to use online public services more often in the next 12 months?	5-point Likert scale	Very unlikely (1) – Very likely (5)
Communication & Experience			
16	How much do you agree with the following statements? • I have seen clear explanations of how my data is protected. • I understand my rights regarding how my data is handled. • Public services should communicate more clearly where data is stored and under which laws.	5-point Likert scale matrix	Strongly disagree (1) – Strongly agree (5)
17	In the past year, have your experiences with online public services been mostly positive?	Multiple choice	Yes (1); No (2); Mixed (3); I have not used them (4)
18	Have you ever received an official message explaining how your data is protected?	Multiple choice	Yes (1); No (2); Not sure (3)
Open Questions			
19	What would most increase your trust in online public services?	Text input	-
20	If you avoid some online public services, what is the main reason?	Multiple choice (multiple selection possible)	I prefer in-person services; Privacy concerns; Security concerns; Not user-friendly; I don't know how to use them; I don't trust the government; Other
Attention Check			
21	Which color is a ripe tomato?	Multiple choice	Red; Green; Blue; Yellow; I don't know
Demographics			
22	What is your age group?	Multiple choice	18-24; 25-34; 35-44; 45-54; 55-64; 65+
23	What gender do you identify with?	Multiple choice	Male; Female; Non-binary/third gender; Prefer not to say
24	What is your highest completed level of education?	Multiple choice	Primary education; Secondary education; Vocational training; bachelor's degree; master's degree; Doctorate (PhD); Other
25	What is your current employment status?	Multiple choice	Full-time employed; Part-time employed; Student; Unemployed; Retired; Other
26	How would you rate your own digital skills?	5-point Likert scale	Very low (1) – Very high (5)

Appendix C.2: Variable Operationalization & Mapping

ID	Construct / Variable	Question Text
Q1	**Screening**	Do you agree to take part in this anonymous survey?
Q2	**Screening**	Do you currently live in a country of the European Union (EU) or the EEA?
Q3	**Usage Status**	In the past 12 months, have you used any online public services?
Q4	**Usage Frequency**	How often do you use online public services?
Q5	**Service Context**	Which types of online public services have you used in the past 12 months?
Q6	**Trust (Ability & Reliability)**	**How much do you agree with the following statements?**
6_1	*Trust: Functionality*	Online public services usually function as expected.
6_2	*Trust: Competence*	The government has the technical ability to keep my data secure.
6_3	*Trust: Reliability*	Online public services work reliably.
6_4	*Trust: Responsiveness*	Problems with online services are resolved in a reasonable amount of time.
Q7	**Trust (Honesty & Fairness)**	**How much do you agree with the following statements?**
7_1	*Trust: Benevolence*	The government tries to handle personal information responsibly.
7_2	*Trust: Integrity (Rules)*	Rules about data protection are followed properly.
7_3	*Trust: Benevolence*	The government aims to protect citizens' rights.
7_4	*Trust: Integrity (Fairness)*	Rules are applied fairly.
Q8	**Digital Sovereignty**	**How much do you agree with the following statements?**
8_1	*Sovereignty: Residency*	My data in online public services is mainly stored in Europe.
8_2	*Sovereignty: Jurisdiction*	European laws decide who can access my data.
8_3	*Sovereignty: Importance*	It is important to me that access to my data is governed by European laws.
8_4	*Sovereignty: Transparency*	It should be possible to see who has accessed my data.

8_5	*Sovereignty: Preference*	I would feel more comfortable if my data stayed in Europe.
8_6	*Sovereignty: Independence*	The government should not rely on a single technology provider.
8_7	*Sovereignty: Exit Capability*	The government should be able to switch providers if needed.
Q9	**Awareness**	Before today, how familiar were you with the idea of your data being stored inside or outside Europe?
Q10	**Concerns (Perceived Risk)**	**How much do you agree with the following statements?**
10_1	*Risk: Foreign Access*	I am concerned that non-European companies might access my data.
10_2	*Risk: Data Offshoring*	I am concerned that my data could be moved outside Europe.
10_3	*Risk: Breach Sensitivity*	News about data breaches makes me more cautious about using online services.
10_4	*Risk: Provider Origin*	I prefer European providers even if I do not know them well.
10_5	*Risk: Dependency*	I am concerned about dependency on a single technology provider.
10_6	*Risk: Legal Interference*	I am concerned that foreign laws could influence who can access my data.
Q11	**Risk Avoidance**	Have you ever avoided using an online public service because of privacy or security concerns?
Q12	**Service Performance**	**How much do you agree with the following statements?**
12_1	*Performance: Speed*	Online services are fast.
12_2	*Performance: Ease of Use*	Online services are easy to use.
12_3	*Performance: Error-Free*	Tasks can generally be completed without errors.
12_4	*Performance: Satisfaction*	I am satisfied with the online public services I have used.
12_5	*Performance: Availability*	Online services are available when I need them.
Q13	**Perf. Expectancy**	Compared to in-person services, do you expect online public services to work better or worse?

Q14	**Willingness-to-Use (WTU)**	**How much do you agree with the following statements?**
14_1	*WTU: Preference*	I prefer using online services when possible.
14_2	*WTU: Recommendation*	I would recommend online public services to others.
14_3	*WTU: Sovereignty Driver*	Knowing that my data stays in Europe would increase my willingness to use online services.
14_4	*WTU: Confidence*	I am comfortable using online services for sensitive data if security is strong.
14_5	*WTU: Trade-off (Conv)*	If an online service is very easy and fast, I might use it even if I do not know exactly where the data is stored.
Q15	**Adoption Intention**	How likely are you to use online public services more often in the next 12 months?
Q16	**Communication**	**How much do you agree with the following statements?**
16_1	*Comm: Clarity*	I have seen clear explanations of how my data is protected.
16_2	*Comm: Understanding*	I understand my rights regarding how my data is handled.
16_3	*Comm: Demand*	Public services should communicate more clearly where data is stored and under which laws.
Q17	**Experience (General)**	In the past year, have your experiences with online public services been mostly positive?
Q18	**Transparency**	Have you ever received an official message explaining how your data is protected?
Q19	**Trust (Qualitative)**	What would most increase your trust in online public services?
Q20	**Barriers**	If you avoid some online public services, what is the main reason?
Q21	**Attention Check**	Which color is a ripe tomato?
Q22	**Demographics: Age**	What is your age group?
Q23	**Demographics: Gender**	What gender do you identify with?
Q24	**Demographics: Edu**	What is your highest completed level of education?
Q25	**Demographics: Job**	What is your current employment status?
Q26	**Control: Digital Skills**	How would you rate your own digital skills?

Appendix D: Supplementary Statistical Analysis

This appendix presents statistical output supporting the quantitative findings. Table D.1 presents the regression results for the moderation analysis (H6). Table D.2 displays the full Pearson correlation matrix for all six measured constructs. Figures D.1–D.4 illustrate the distribution of the key variables (normality).

Table D.1 Hierarchical Regression Analysis: Moderation Effect (Model 3)

Dependent Variable: Willingness-to-Use. Source: SPSS Output, Coefficients Table (Model 3).

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	2.018	.189		10.669	.000		
	Trust	.257	.057	.304	4.551	.000	.647	1.546
	Service performance	.246	.051	.321	4.810	.000	.647	1.546
2	(Constant)	1.507	.211		7.139	.000		
	Trust	.165	.058	.194	2.856	.005	.572	1.749
	Service performance	.225	.049	.295	4.588	.000	.642	1.558
	Data Access Concerns	.239	.051	.274	4.723	.000	.785	1.274
3	(Constant)	2.196	.818		2.684	.008		
	Trust	-.027	.228	-.032	-.120	.905	.037	27.219
	Service performance	.216	.050	.282	4.280	.000	.611	1.638
	Data Access Concerns	.066	.205	.075	.320	.749	.048	20.918
	Trust x AccessConcerns	.050	.058	.373	.872	.384	.014	69.165

[a]. Dependent Variable: Willingness to use

Note: Interaction term (p = .384) is statistically non-significant, confirming the rejection of H6

Table D.2 *Pearson Correlation Matrix (n=242)*

Correlations

		Trust	Perceived sovereignty	Service performance	Willingness to use	Clear communication
Perceived sovereignty	Pearson Correlation	.627**				
	Sig. (2-tailed)	.000				
	N	242				
Service performance	Pearson Correlation	.594**	.370**			
	Sig. (2-tailed)	.000	.000			
	N	242	242			
Willingness to use	Pearson Correlation	.495**	.529**	.502**		
	Sig. (2-tailed)	.000	.000	.000		
	N	242	242	242		
Clear communication	Pearson Correlation	.446**	.294**	.435**	.347**	
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	242	242	242	242	
Data Access Concerns	Pearson Correlation	.457**	.697**	.334**	.461**	.223**
	Sig. (2-tailed)	.000	.000	.000	.000	.000
	N	242	242	242	242	242

**. Correlation is significant at the 0.01 level (2-tailed).

D.3. Normality Checks (Histograms)

The following histograms visually confirm the normal distribution of the dependent and independent variables, satisfying the assumptions for regression analysis.

Figure D.1: *Distribution of Willingness-to-Use*

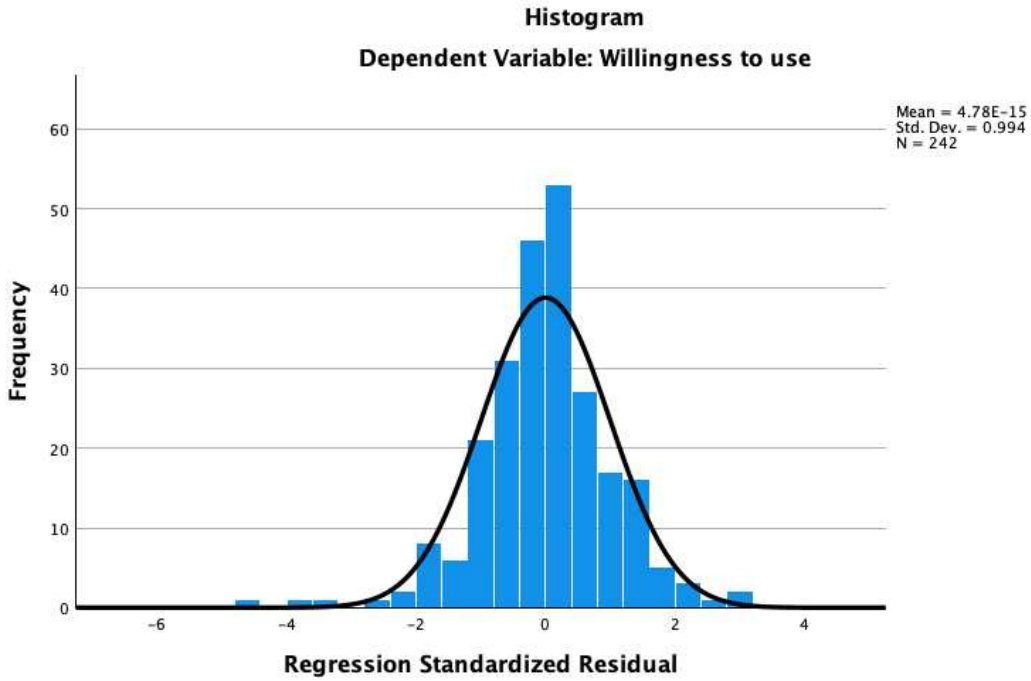


Figure D.2: *Distribution of Perceived Sovereignty*

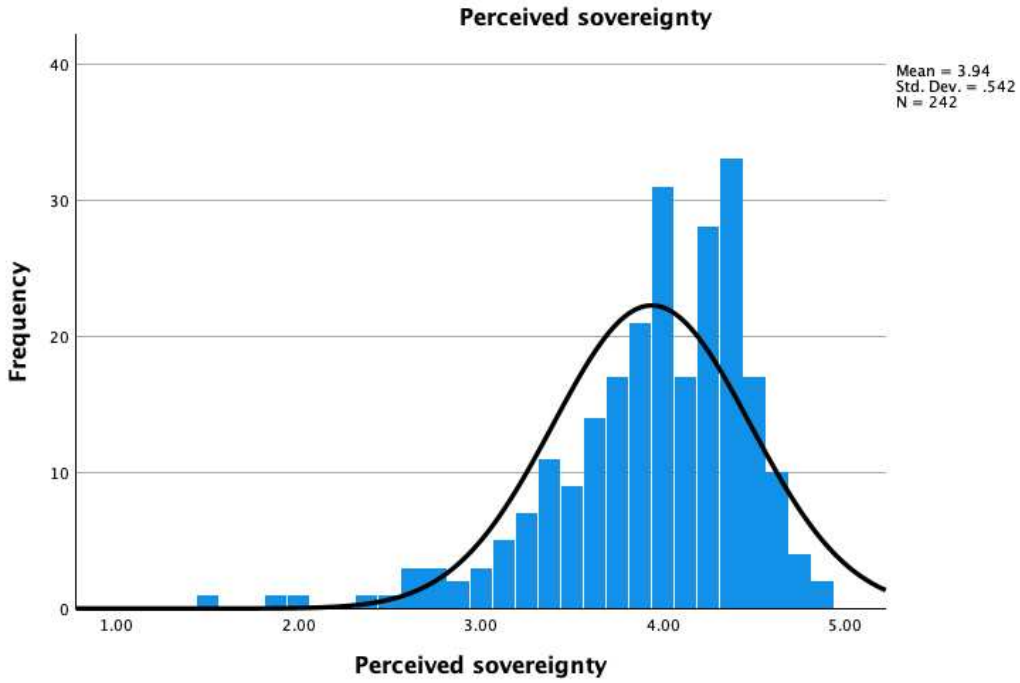


Figure D.3: *Distribution of Service Performance*

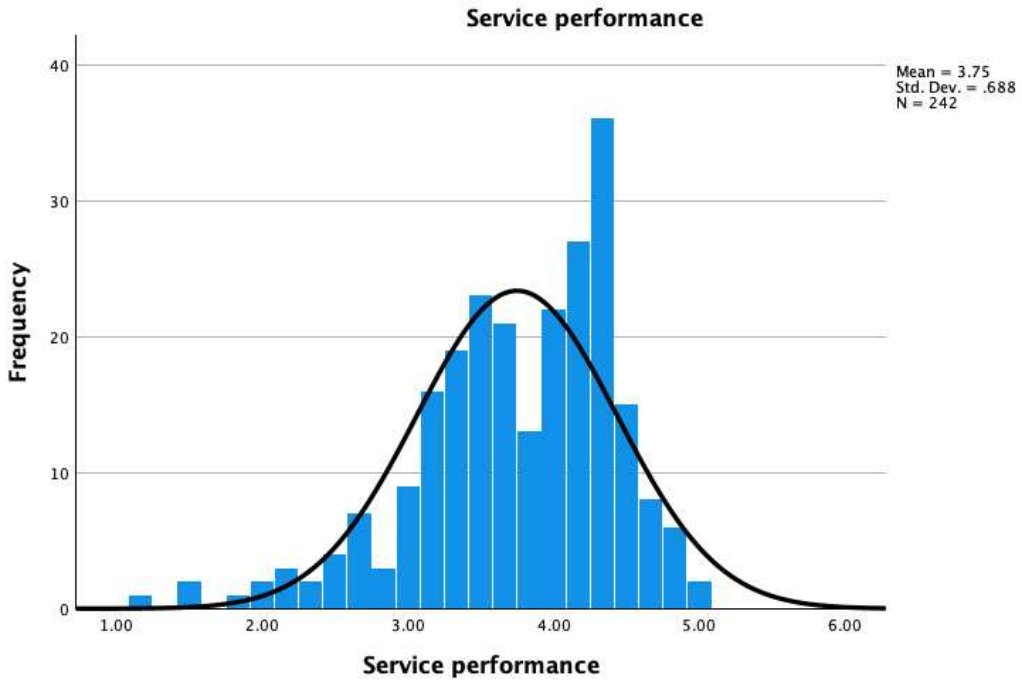


Figure D.4: *Distribution of Trust*

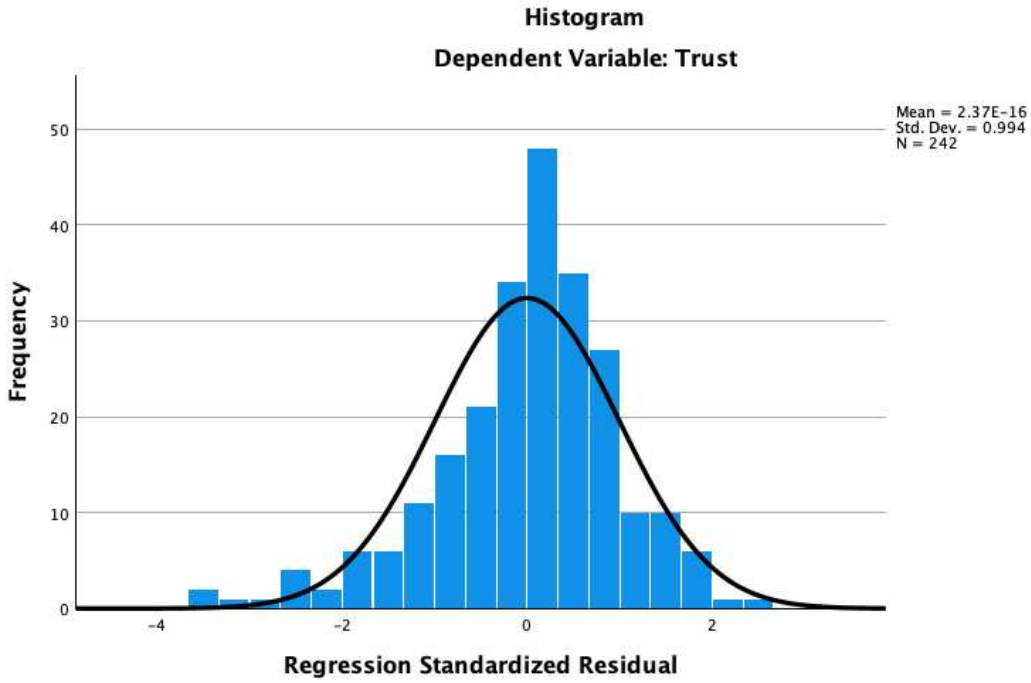
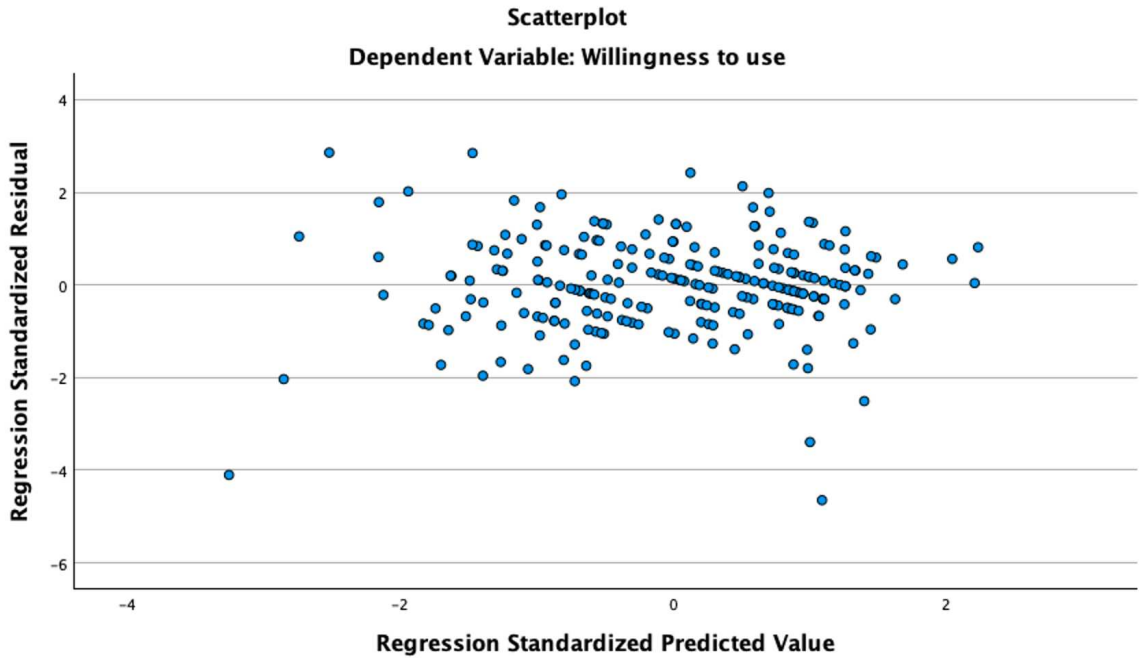


Figure D.5: *Residuals Scatterplot (Homoscedasticity Check)*



Appendix E: Expert Interview Data

This appendix provides a consolidated overview of the expert interviews conducted for this study.

E.1 Expert Overview Table

ID	Role	Strategic Perspective	Core Insight
C01	**Director** Intl. Consultancy	**Resilience & Scale** Sovereignty is driven by crisis resilience rather than just compliance.	*"Sovereignty is not static; it changes based on external factors like geopolitical threats."*
C02	**Manager** Intl. Consultancy	**Realism** Full independence is impossible; advocates for a balanced Multi-cloud strategy.	*"We need a Multi-Cloud strategy to manage dependencies without blocking innovation."*
C03	**Senior Manager** Intl. Consultancy	**Anti-Lock-in** Focuses on technical sovereignty (e.g., open source) to avoid vendor dependency.	*"Vendor lock-in is the real threat to sovereignty, not just the nationality of the provider."*
C04	**Senior Manager** Intl. Consultancy	**Organizational Blockers** Culture and demographic change (skills gap) are bigger barriers than technology.	*"Introducing cloud is easy- integrating it sustainably into the organization is the hard part."*
C05	**Manager** Intl. Consultancy	**Market Dynamics** Public sector is forced to follow vendor moves (e.g., Microsoft stopping on-prem support).	*"Microsoft moving Office to the cloud forces the public sector to follow, regardless of strategy."*
C06	**Senior Manager** Intl. Consultancy	**Technical Gap** Sovereign providers still lag behind hyperscalers in feature breadth (e.g., AI, PaaS).	*"True sovereignty is the ability to operate without the provider- and that is currently rare."*
C07	**Director** Intl. Consultancy (Audit/Strategy)	**Trust Asymmetry** State relies on contracts; citizens must trust blindly due to monopoly.	*"Citizens don't think in sovereignty terms- they think security, simplicity, and availability."*
P01	**Leader Cloud CoE** Large Federal Agency	**Operational Maturity** Sovereignty is a journey of internal capability building, not just a product.	*"Outages destroy trust immediately. Performance failure damages legitimacy more than sovereignty issues."*
P02	**Deputy Director Tech** Federal IT Service Provider	**Strict Control** Sovereignty defined as Operational Independence and autarky for critical data.	*"Trust is nice, control is better. Without exit strategies, sovereignty is an illusion."*

P03	**Cloud Lead** Pension Authority	**Situational Sovereignty** High relevance for social data; less for administrative/public tasks.	The Transparency Paradox: *"If we show citizens the complexity of data flows, trust might decrease."*
P04	**Head of IT Security** Statutory Health Insurer	**Pragmatism** Focus on functional security over geopolitical labels. "Outcome-oriented."	*"A Sovereign Cloud without operational capacity is just a sovereign logo."*
P05	**CIO** Large Federal Agency	**Managed Dependency** Sovereignty as negotiation power, not total isolation.	*"Sovereignty is the ability to stand up from the negotiation table."*

E.2 Expert Interview Summaries

Category	Detailed Summary
Participant	**C01: Strategic Director (Intl. Consultancy)**
Background & Context	C01 possesses a dual perspective, having advised government clients on strategy while also working directly with Sovereign Cloud providers (e.g., Delos Cloud). He focuses on the gap between European industrial ambition and technological reality.
Definition of Sovereignty	He reframes sovereignty from a legal concept to Resilience. He argues the discourse has shifted from "compliance" (GDPR) to "Security of Supply." He defines sovereignty not merely as data residency, but as the capability to maintain operations during geopolitical shocks. He warns against "Fake Sovereignty," arguing that true sovereignty requires control over the entire supply chain.
Drivers & Barriers	**Driver**: The "Zeitenwende" (Geopolitical Resilience) is the primary driver; reliance on single external partners is now viewed as a strategic risk. **Barrier**: He applies the "Airbus Analogy," arguing Europe lacks the industrial scale to compete with US hyperscalers. Without a consolidated champion, solutions remain fragmented. **Barrier**: The "Sovereignty Tax", Sovereign Clouds often lack advanced features (AI, PaaS), forcing agencies to trade functionality for compliance.
Trust & The Citizen	C01 differentiates between Institutional Trust (audits) and Citizen Trust (UX). He argues citizens are unaware of technical architectures; trust is a function of Competence. If the state enforces strict sovereignty but delivers clunky services, trust diminishes. He suggests citizens implicitly accept US data processing if service quality is high (e.g., Netflix).

Category	Detailed Summary
Participant	**C02: Manager (Intl. Consultancy)**
Background & Context	C02 specializes in public sector cloud transformation. He bridges the gap between political requirements and technical implementation, advocating for "workable" sovereignty solutions that do not block innovation.
Definition of Sovereignty	He defines sovereignty as Strategic Optionality within a Multi-Cloud environment. He rejects the binary view, advocating for a tiered model where strict sovereignty applies only to "Classified Information." He argues that total autarky is an "Innovation Trap", running everything in a government data center isolates the state from global technological progress.
Drivers & Barriers	**Driver:** The need for Capability (modern SaaS/PaaS) drives adoption; agencies cannot build modern AI on legacy stacks. **Barrier**: The lack of a clear Data Strategy causes paralysis. Agencies often default to classifying all data as "high protection," blocking adoption unnecessarily. **Solution**: A "Best-of-Breed" approach using sovereign providers for sensitive data and hyperscalers for administrative workloads.
Trust & The Citizen	C02 views the sovereignty debate as an internal political discourse. For the user, Trust = Availability + Usability. He warns that if "Purist Sovereignty" leads to unstable services, it damages the state's reputation more than using a secured US provider would. Technical autarky is not a value proposition for the citizen.

Category	Detailed Summary
Participant	**C03: Senior Manager (Intl. Consultancy)**
Background & Context	C03 advises healthcare and social security clients. Her perspective is shaped by strict regulatory requirements for "Social Data," focusing on technical reversibility.
Definition of Sovereignty	She defines sovereignty through "Anti-Lock-in" and Interoperability. She critiques the focus on "Data Residency," arguing that "how data is processed" matters more. True sovereignty exists only with Open-Source standards. If an agency uses a domestic data center but runs proprietary software preventing migration, they are "captured." Sovereignty is the "Freedom to Switch."
Drivers & Barriers	**Driver**: Regulatory Coercion (e.g., mandatory Electronic Patient Record rollout) forces confrontation with sovereignty. **Barrier**: The "Convenience Trap." US hyperscalers offer ready-to-use ecosystems with great UX, while sovereign alternatives require complex integration. Under time pressure, agencies prioritize the "path of least resistance," sacrificing long-term sovereignty.
Trust & The Citizen	C03 notes citizens have high Baseline Trust in health insurers. She warns against "Active Transparency" (showing complex data maps), which creates a "Transparency Paradox", confusing citizens breeds suspicion. She advocates for "Passive Transparency": architecture must be audit-proof internally, but the user interface should remain simple.

Category	Detailed Summary
Participant	**C04: Senior Manager (Intl. Consultancy)**
Background & Context	C04 specializes in Cloud Operating Models ("Day 2 Operations"). He highlights the organizational challenges of maintaining sovereign environments after migration.
Definition of Sovereignty	He views sovereignty as a Compliance Discipline generated through Governance. It is a process, not a product. An agency can use a US hyperscaler sovereignly if they control encryption keys and identity management. Conversely, a German provider offers no sovereignty if the agency lacks internal access control processes.
Drivers & Barriers	**Driver**: Modernization is mandatory as legacy systems fail. **Barrier**: The "Demographic Crisis" (Skills Gap). As "Baby Boomers" retire, the public sector loses the staff to run legacy stacks, but also lacks the skills to run complex sovereign private clouds. Without the people to operate it, a Sovereign Cloud becomes a "Zombie Infrastructure."
Trust & The Citizen	C04 implies Stability is the foundation of trust. If strict sovereignty leads to "home-brewed" solutions that crash due to lack of staff, trust is destroyed. He suggests Managed Dependencies (hyperscalers with governance) are safer for trust because they guarantee uptime that the state cannot manage alone.

Category	Detailed Summary
Participant	**C05: Manager (Intl. Consultancy)**
Background & Context	C05 focuses on Digital Strategy, analyzing the tension between political desires and market realities. He provides a realist view on global market dynamics.
Definition of Sovereignty	He defines sovereignty as a Spectrum of Operational Capability. He argues "Digital Sovereignty" is often confused with "Data Privacy." For him, sovereignty is the ability to keep the state running. A state with local data but obsolete infrastructure is not sovereign because it cannot act. True sovereignty implies participation in global technological progress.
Drivers & Barriers	**Driver**: Vendor Push is the strongest force. When vendors (e.g., Microsoft) discontinue on-premise support, the public sector is forced into the cloud to survive. **Barrier**: Regulatory Paralysis. While technology matures, legal frameworks remain ambiguous, causing decision-makers to freeze out of fear of personal liability.
Trust & The Citizen	C05 uses the "Car Brakes Analogy": a driver trusts brakes work without knowing the steel's origin. Similarly, citizens do not care about the "Digital Supply Chain." Trust is built through User Experience (UX). If digital services are smooth (like Netflix), citizens trust the state. Prioritizing data location over functionality risks state legitimacy.

Category	Detailed Summary
Participant	**C06: Senior Manager (Intl. Consultancy)**
Background & Context	C06 is a Technical Architect focusing on the "engine room" of migration. He deals with the practical friction of moving legacy workloads to sovereign environments.
Definition of Sovereignty	He defines sovereignty strictly as "Autarky and Reversibility." True sovereignty is the ability to operate infrastructure without the provider's help. He critiques "Managed Sovereign Clouds" where the agency lacks root access. If the provider cuts the connection and the agency cannot restart elsewhere, sovereignty is an illusion.
Drivers & Barriers	**Driver**: Technical Debt ("crumbling concrete" of legacy data centers). **Barrier**: The "Maturity Gap" (Feature Parity). Sovereign European providers lack the breadth of services (AI, Databases) found in hyperscalers. Technical teams push for hyperscalers because "they just work," while sovereign alternatives require massive custom engineering, creating "Shadow IT" pressure.
Trust & The Citizen	C06 links trust to Digital Competence. Citizens lose trust when the state fails at basic tasks. He suggests sovereignty is secondary; if a non-sovereign solution delivers a working service, it generates more trust than a sovereign solution that fails. Performance is a proxy for Trust.

Category	Detailed Summary
Participant	**C07: Director (Intl. Consultancy)**
Background & Context	C07 specializes in Technology Policy and market strategy. He provides a macro-view of how regulations (Data Act, EUCS) shape the European cloud market.
Definition of Sovereignty	He distinguishes between Nominal Sovereignty (labels) and Effective Sovereignty (control). He focuses on Exit Capability. If a government uses a sovereign hyperscaler but builds apps on proprietary APIs (the "Golden Cage"), they lose sovereignty because the cost of exit is prohibitive. True sovereignty is the Power to Leave.
Drivers & Barriers	**Driver**: Strategic Autonomy (avoiding "Digital Colonialism"). **Barrier**: Vendor Lock-in. The convenience of hyperscaler features lures agencies in; once integrated, they cannot leave. The barrier is not the lack of Sovereign Clouds, but the difficulty of migrating away from established proprietary ecosystems.
Trust & The Citizen	C07 introduces "Trust Asymmetry." Since the state is a monopoly, citizens must trust it. To bridge this, he proposes sovereignty could evolve into a "Nutri-Score" for digital services. Just as consumers trust a "Bio-Label," a "Sovereign Label" could signal safety, acting as a proxy for trust in an invisible supply chain.

Category	Detailed Summary
Participant	**P01: Leader Cloud CoE (Large Federal Agency)**
Background & Context	P01 leads a Cloud Center of Excellence, responsible for "enablement", moving from strategy to practical implementation within a major federal authority.
Definition of Sovereignty	He defines sovereignty as a Maturity Journey, focusing on "Operational Capability." An agency is only sovereign if it has the internal skills to manage its IT stack. He warns against the "Illusion of Control" in on-premise centers: if an agency relies on consultants to run its own basement data center, it is effectively non-sovereign.
Drivers & Barriers	**Driver**: Crisis Response (COVID-19). On-premise systems failed to handle unemployment claim spikes, proving Scalability is a requirement for state function. **Barrier**: The "Skills Gap." The public sector cannot hire "Cloud Architects" due to salary caps. Without these experts, the cloud becomes insecure due to misconfiguration, not technology.
Trust & The Citizen	P01 links trust directly to Reliability, arguing "Outages destroy trust immediately." Citizens are outcome-oriented; they care about the service working, not the "German Cloud" label. Performance is the critical trust factor, with sovereignty acting only as a background "hygiene factor."

Category	Detailed Summary
Participant	**P02: Deputy Director Tech (Federal IT Service Provider)**
Background & Context	P02 is a Vice Director at a Federal IT Service Provider, representing the "Purist" view and ensuring strict adherence to BSI security standards.
Definition of Sovereignty	She defines sovereignty as Operational Independence and Control. Her philosophy is "Trust is nice, control is better." True sovereignty means Autarky, the ability to operate critical infrastructure even if a provider cuts ties. She prioritizes "Security by Design" over "Security by Contract."
Drivers & Barriers	**Driver**: Risk Mitigation (protecting against espionage/US CLOUD Act). **Barrier**: The "Lock-in Trap." She warns agencies are "sleepwalking" into dependency. Without a tested Exit Strategy, sovereignty is an illusion. **Barrier**: Legacy Landscape. Migrating mainframe logic to Sovereign Clouds is technically difficult and expensive.
Trust & The Citizen	P02 believes citizens equate sovereignty with Privacy. They expect the state to be "Paranoid" on their behalf. Strict sovereignty is a mandatory Pre-condition for trust. If the state lost citizen data to a foreign entity, the reputational damage would be catastrophic.

Category	Detailed Summary
Participant	**P03: Cloud Lead (Federal Social Security Authority)**
Background & Context	P03 manages IT strategy for a Federal Social Security Authority. Dealing with "Social Data" (Crown Jewels), his approach is highly cautious.
Definition of Sovereignty	He views sovereignty as Situational and Differentiated. He advocates for a Data Classification Strategy: "Crown Jewels" (Social Data) stay on-premise/private, while administrative data moves to public cloud. This "Hybrid Approach" balances cost/agility with strict protection.
Drivers & Barriers	**Driver**: Demographic Peaks. Public Agencies need cloud flexibility to handle "Baby Boomer" retirement waves. **Barrier**: Regulatory Ambiguity. "Regulation stops more projects than technology." The lack of legal certainty regarding US hyperscalers paralyzes decision-making and prevents the adoption of efficient tools.
Trust & The Citizen	P03 introduces the "Transparency Paradox." While transparency is theoretically good, showing citizens, the full complexity of global data flows would confuse and alarm them. Citizens trust the Brand/Institution, not the technology. They assume the authority "takes care of it."

Category	Detailed Summary
Participant	**P04: Head of IT Security (Statutory Health Insurer)**
Background & Context	P04 is the CISO of a Statutory Health Insurer. His perspective is characterized by extreme Pragmatism and an outcome-oriented focus.
Definition of Sovereignty	He adopts an Outcome-Oriented definition: "I am interested in the result, not the path." He argues that if a US hyperscaler provides superior automated threat detection, using it is the "More Sovereign" choice because the data is safer. He defines sovereignty as the Effective Protection of Data, regardless of server location.
Drivers & Barriers	**Driver**: Business Demand. Internal departments demand modern tools (AI, Analytics) and are unwilling to wait for internal provisioning. **Barrier**: Shadow IT Risk. If the official sovereign offering is too slow or restrictive, departments will use non-compliant tools. Managed hyperscalers are safer than "Shadow IT."
Trust & The Citizen	P04 views trust in healthcare as Binary (one breach destroys reputation). However, citizens trade theoretical sovereignty for Functionality. They will use a convenient app even if it runs on AWS, provided the "Result" (security) is guaranteed. Citizens trust the Brand to vet the supply chain.

Category	Detailed Summary
Participant	**P05: CIO (Large Federal Agency)**
Background & Context	P05 is the CIO of a Large Federal Agency, responsible for overall IT strategy. His perspective is Political, balancing sovereignty mandates with mass service delivery.
Definition of Sovereignty	He defines sovereignty as "Negotiation Power" (Managed Dependency). He rejects autarky as an illusion. Sovereignty is the "Ability to stand up from the negotiation table." It means having enough alternatives and internal competence to say "No" if a vendor changes terms. It is about avoiding Blackmailability, not avoiding foreign technology.
Drivers & Barriers	**Driver**: Geopolitics. The "Zeitenwende" makes digital dependency a national security risk. **Barrier**: Cultural Resistance. He identifies "Not Invented Here" syndrome. Internal IT departments often build inferior custom solutions, justifying them with "sovereignty" arguments to protect their jobs (Protectionism).
Trust & The Citizen	P05 is strictly Outcome-Oriented. "Citizens don't care about Sovereign Cloud; they care if the service works." Performance is Legitimacy. If a digital application is fast, citizens trust the agency. If it crashes due to rigid sovereignty, trust is lost. Sovereignty is a backend insurance policy, not a citizen value proposition.