Designing Digital Identity Infrastructure: A Taxonomy of Strategic Governance Choices

Alexandre Amard
University of Luxembourg
Alexandre.amard@uni.lu

Eduard Hartwich
University of Luxembourg
Eduard.hartwich@uni.lu

Alexandra Hoess
University of Luxembourg
Alexandra.hoess@uni.lu

Alexander Rieger
University of Luxembourg
Alexander.rieger@uni.lu

Tamara Roth
University of Luxembourg
Tamara.roth@uni.lu

Gilbert Fridgen
University of Luxembourg
Gilbert.fridgen@uni.lu

Abstract

Governments around the world increasingly deploy digital identity infrastructure. These initiatives are considered a fundamental building block for their citizens to reap the benefits of digitalization and take part in the digital society and economy. But this outcome is not guaranteed: it considerably hinges upon a range of strategic governance decision domains that institutional actors must act on when designing digital identity infrastructures. To get a better understanding of how governments can approach this critical design aspect, we propose a taxonomy of strategic governance choices for digital identity infrastructures. This taxonomy is the outcome of an analysis of 13 government-led digital identity infrastructures and 12 expert interviews. This paper contributes to the digital government literature by setting a foundation for further research and theory-building on digital identity infrastructure. Practitioners can use the taxonomy to develop governance strategies for their own digital identity infrastructure.

Keywords: Digital identity, digital infrastructure, digital government, eGovernment, governance.

1. Introduction

Digital identity infrastructure is deemed essential for the effective provision of society-wide functions and services provided by the government or private sector (Henfridsson & Bygstad, 2013; DPGA & GiZ, 2022). It is credited with a capacity to support socio-economic development (Addo & Senyo, 2021; Masiero & Bailur, 2021), enable individual agency (Whitley & Schoemaker, 2022), improve social inclusion (Wang & Filippi, 2020) and is commonly viewed as an integral component to reach sustainable development as reflected through the United Nations' Sustainable Development Goal 16.9 "Legal identity for all, including birth registration, by 2030" (UN Legal Identity Expert Group, 2019). It is expected that digital identity systems could "unlock value equivalent to 3 to 13 percent of GDP by 2030" (McKinsey, 2019). In light of these asserted benefits, the development of reliable digital identity infrastructure has become a high priority for governments to enable their citizens to take full advantage of the opportunities that digitalization represents (Gelb & Diofasi, 2018), and a number of countries around the world have built their own digital identity infrastructures, including India, Nigeria, Peru, Singapore and most European countries. Many more commit substantial resources to build or improve their own digital identity capabilities (World Bank, 2022b).

Yet, not all digital identity infrastructure is successful in realizing these benefits (Walke et al., 2023). Many recent initiatives have exhibited varying signs of failure, ranging from low adoption to outright discontinuation, or even citizen rejection prior to implementation. A 2021 PwC survey revealed that Germany's electronic identification scheme had a very low uptake, with only 7% of citizens having used their electronic identity document in 11 years following its introduction (PwC, 2021). In the UK, the GOV.UK Verify infrastructure, that was expected to be taken over by the private sector by 2020, was publicly qualified as a failure (National Audit Office, 2019) and fully discontinued in 2023, a few months after the UK's taxation authority withdrew from the scheme. The total cost for the infrastructure was estimated to be £220m. In Switzerland, the digital identity infrastructure did not even get a chance to start: in March 2021, a referendum saw the adoption of the Electronic Identification Services Act overwhelmingly rejected. This failure was largely attributed to the role that the private sector would have taken in provisioning digital identities. Again in 2021, the Comptroller and Auditor General of India heavily criticized the Unique Identification Authority of

URI: https://hdl.handle.net/10125/106646
978-0-9981331-7-1

India's (UIDAI) national digital identity infrastructure Aadhar, not least because of the poorly established relationship between government and private sector partners (CAG of India, 2021). To build and manage its identity infrastructure, the UIDAI spent Rs 15764.48 Crore (~$1.8bn) from its inception in 2009 until February 2023 (UIDAI, 2023).

In all these cases, failures were widely attributed to strategic design choices made regarding *governance*; conceptualized in this paper as the macro-level choices happening at the intersection between relational governance, corporate governance and infrastructure governance (Saunders et al., 2020). These failures caused public distrust and waste of public resources to replace the positive outcomes that had been expected from the infrastructure. The importance of governance arrangements has long been established, and their mechanisms studied extensively. Public-private links, service diversity, user awareness and acceptance, regulation and organizational structures are governance-related factors that can influence the success of digital identity infrastructure (Walke et al., 2023). Additionally, both organizational and institutional arrangements impact the selection, design and implementation of information technologies in government (Gil-Garcia, 2012; Koppenjan & Groenewegen, 2005; World Bank, 2014), reinforcing their central role in realizing the infrastructure's value.

This challenge is compounded by the fact that institutional actors are confronted with a myriad of governance design options for digital identity infrastructure. These choices will impact the infrastructure, the services that rely on it and its users for years, if not decades.

A detailed look at instantiations around the world reveals wildly different implementations and substantial design complexity. For example, in Scandinavian countries, banks play a crucial role in providing digital identity services to citizens who use their 'BankID' on a daily basis for various identification purposes. On the other hand, some countries such as Spain have built their digital identity capabilities around public sector needs, and the private sector is primarily acting as a subcontractor. The Indian Aadhar system is led by the public sector, with extensive participation of the private sector, including for the enrolment of citizens. These are just a few of the existing governance configurations in an area where disruptive technologies are increasingly deployed. Then, how can institutional actors have confidence that they evaluated the most important governance design options? What are the governance choices available to them that will have substantial impact on the design and ultimate success of the costly infrastructure? Despite their criticality, so far, no consolidated answer to these questions has been offered. While some of the topics at hand are individually addressed in the literature, to our knowledge, there is no systematic guidance and terminology on the strategic governance choices for digital identity infrastructure. In response, we formulate the following research question:

Research Question: *What are the strategic governance choices impacting the design of digital identity infrastructure?*

We answer this research question by developing a multi-layer taxonomy for the governance of digital identity infrastructure. Our development process follows Nickerson et al. (2013) and involved 4 iterations, which included (1) a literature review, (2) interviews with practitioners and (3) with researchers in the field of digital identity infrastructures, and (4) an analysis of governance models of existing digital identity systems. Our final taxonomy consists of three layers, 13 dimensions and 46 characteristics. It establishes a holistic overview of the critical governance decisions required during the design of digital identity infrastructure and consolidates terminology to facilitate collaboration during this process.

This paper is structured as follows. In Section 2, we present the theoretical background regarding digital identity and digital identity infrastructure. We then discuss the implementation of our research method in Section 3, which we used to develop a multi-layer taxonomy presented in Section 4. Finally, in Section 5, we reflect on our findings, acknowledging their implications and limitations, and propose avenues for future research.

2. Theoretical Background

2.1. Digital identity

In this article, we conceptualize *digital identity* as the set of digitalized identity attributes and credentials that describe qualities, characteristics, or assertions of a person (Temoshok et al., 2022). This set of attributes and credentials can be used for the identification and authentication of a person via digital channels, for instance, to provide governmental and private sector services (Nyst et al., 2016). Digital credentials are the means through which a subject can assert their digital identity (Sedlmeir et al., 2021). These credentials can take several forms, ranging from electronic identity documents to smartphone-stored digital documents, and are sometimes enhanced with other authentication factors such as biometrics or passwords to allow for a higher level of authentication assurance (World Bank, 2019a). A digital credential can also simply be a reference to a digital record in a database, or directly

contain identity attributes. Cryptographic methods are employed to ensure the integrity and authenticity of credentials (Sedlmeir et al., 2021), while safeguards and controls are used to support data protection and prevent data leakage and identity theft (McCallister et al., 2010).

Digital identity emanates from entities in charge of collecting and verifying identity data about a subject and translating it into the digital realm. As digital identity is not a monolithic construct, identity data and credentials making up a digital identity can be collected, stored, certified, and issued by different stakeholders (Grassi et al., 2017). These authoritative entities hold data that is accepted as accurate and trustworthy within a particular sector of application (e.g., taxation, criminal records, and health). In many countries, linkability of identity data (e.g., through unique identifiers or mediating entities), which allows for the re-identification of a data subject in different circumstances, is strictly regulated for privacy and data protection purposes (Beduschi, 2019). The capacity to materialize the benefits of digital identity, including the capacity to collect, store and verify identity attributes, enroll and authenticate users, and manage credentials and authorizations, requires the establishment of a digital identity infrastructure (Nyst et al., 2016).

2.2. Digital identity infrastructure

Digital infrastructure refers to digital, socio-technical systems that underlie or support the public interest, as well as universal or quasi-universal services (Plantin et al., 2018). The notion of digital infrastructure conceptualizes the reality of interconnected system collectives, which evolve at the intersection between socio-technical elements, networks of actors and relationships between organized practices (Henfridsson & Bygstad, 2013). Thus, the study on digital infrastructure extends beyond the historic information systems focus, being shared, unbounded, heterogenous and evolving (Hanseth & Lyytinen, 2010). Digital infrastructure (also sometimes called *digital public infrastructure* by practitioners (DPGA & GiZ, 2022)) applies within a society-wide, public service-oriented context, including for digital identity management systems (Boysen, 2019).

Digital identity infrastructures can be defined as systems that construct, control, and commodify (facets of) digital identities and can be formed by both public and private sector actors (Giannopoulou, 2023). Despite many having a national dimension, some digital identity infrastructures target transnational interoperability (e.g., the West Africa Unique Identification for Regional Integration program, or the electronic Identification, Authentication and Trust Services regulation). Others, in turn, operate at the sub-national level (e.g., the Ontario and Alberta provinces). Digital identity infrastructures are credited with various potential benefits, ranging from the "facilitat[ion] and simplif[ication of] access to a wide range of services and thereby contribute to social and economic value" (OECD, 2023), better "inclusion, social protection, healthcare and education, gender equality, child protection", "delivery of public services and programs", and the "reduction of fraud" (World Bank, 2019b). On the other hand, implementation of these systems can also cause adverse impacts, such as "exclusion from access", "distortion of monitoring", "redirection of policy" (Masiero & Arvidsson, 2021), "privacy and security violations" among others (Beduschi, 2019; World Bank, 2019a).

Digital identity infrastructures are to be considered within the complex socio-technical systems that structure them (van Dijck & Jacobs, 2020; Weigl, Barbereau, et al., 2022). It is well-established that organizational and institutional arrangements significantly influence the selection, design and implementation of information technologies in government (Gil-Garcia, 2012; Koppenjan & Groenewegen, 2005; World Bank, 2014), thus playing an important role in the design of digital infrastructure. It follows that considering actors, roles, people and processes is a necessary condition for the development and implementation of useful and sustainable infrastructures (Dawes, 2009; Manny et al., 2022). Digital identity infrastructure design and success are therefore inextricably interlocked with the strategic governance choices that impact them (Gil-Garcia & Flores-Zúñiga, 2020; Medaglia et al., 2022), and their identification and characterization should be a priority.

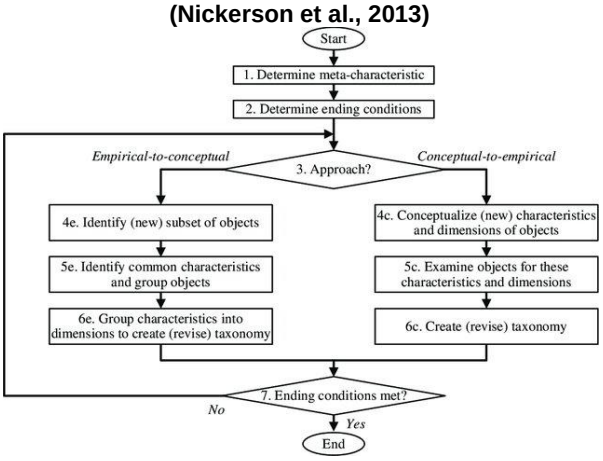
3. Research method

Given the nascent nature and rapid development of digital identity infrastructures, we opted to develop a taxonomy (Bailey, 1994) to understand, classify and systematically structure common characteristics of strategic governance choices when designing digital identity infrastructure. Taxonomies are common means to this end, and they are frequently used across information systems research (Berger et al., 2020; Hartwich et al., 2022). Further, taxonomies can serve as a foundation upon which research and practice can build: as such, we address information systems scholars, policymakers and practitioners in the field of e-government.

In order to develop our taxonomy, we structure our approach following the method outlined by Nickerson et al. (2013). This iterative process, as illustrated in Figure 1, consists of seven steps which are considered completed once defined ending conditions are met. We

rigorously followed this process to ensure reproducibility of our results.

Figure 1. Taxonomy development method (Nickerson et al., 2013)



3.1. Taxonomy development process

Our purpose is to systematically classify the dimensions and characteristics of governance-related decision domains that are key for the design of digital identity infrastructures. We thus selected our meta-characteristic to be "Strategic Governance Choices for Digital Identity Infrastructure". We then determined our objective and subjective ending conditions. Objective ending conditions target the formal aspects of taxonomy building and indicate that the taxonomy building process and its iterations can be concluded once they are met (Nickerson et al., 2013). Subjective ending conditions play an important role as they relate to the usefulness of the taxonomy's content. We set out to validate every objective ending conditions as outlined by Nickerson et al. (2013). These can be broadly classified into 3 categories: (1) the last iteration should not have induced any needed change in the taxonomy, (2) there should be no repetition or duplication between dimensions and characteristics, and there should only be dimensions or characteristics that represent at least one object under analysis, and (3) all objects, or a representative sample thereof, have been analyzed.

These conditions were tested at the end of each iteration, and we devoted the last iteration to specifically analyze a representative sample of objects. An exhaustive analysis of all existing digital identity infrastructures is not feasible, not only because of the important number of instantiations in existence, but also because they evolve rapidly, and limited information is readily available for many of them. We thus selected a sample of 13 instantiations that are widely referred to as archetypes for specific dimensions of digital identity infrastructure governance and thus influenced the governance models of other instantiations: Argentina, Australia, Canada, Chile, Estonia, France, Germany, India, Italy, Morocco, Nigeria, Sweden, United Kingdom. These present particularly interesting and salient characteristics, and their geographical coverage is varied.

As regards subjective ending conditions, we requested an assessment of our taxonomy's usefulness, robustness (i.e., does it enable sufficient differentiation between objects to be of interest), and explanatory character from our interview partners, who would later use this taxonomy in their work and thus are the best placed to provide feedback.

3.2. Iterations

We needed four iterations to meet the ending conditions and reach the final version of the taxonomy. Our first iteration took a conceptual to empirical approach and built on existing academic and practitioner-sourced material dealing with classification of digital identity management systems. We searched the existing body of academic and grey literature dealing with governance of digital identity infrastructure, using the search string "digital identity governance" OR "digital identity infrastructure" OR "digital infrastructure governance". This initial phase was primarily used to identify works of relevance for a second stage of backward and forward searching that allowed us to identify the most relevant work in this area. After screening for eligibility, this process yielded 65 articles and documents, 32 from academic literature and 33 from grey literature. The work of the National Institute of Science and Technology (Grassi et al., 2017), the International Telecommunication Union (ITU, 2018) and the World Bank (World Bank, 2014, 2022a, 2019a) were particularly useful during this iteration. It laid down the foundations of the taxonomy, with the three layers of *ecosystem governance*, *IT governance* and *data governance* emerging. We could additionally identify several dimensions and characteristics that would remain until the final version of the taxonomy. In total, nine dimensions and 28 characteristics were identified. This iteration confirmed that while some useful knowledge supporting the answering of our research question had been synthesized, content was spread out and the vocabulary used varied significantly.

The second iteration took an empirical to conceptual approach and consisted in the interview of eight practitioners. They were selected for their expertise and experience (Mergel et al., 2019) in the design of governance arrangements of digital identity systems. The interviewees came from both the public and the private sector, and the semi-structured

interviews (Schultze & Avital, 2011) lasted between 30 and 90 minutes. Several participants had been involved in the design of multiple digital identity infrastructures, which enabled them to adopt a global, synthetic perspective. This iteration enabled us to both expand the taxonomy and refine it towards meeting our subjective ending conditions. In total, we identified 12 dimensions and 47 characteristics. Towards the end of the iteration, we noticed that we approached theoretical saturation as no new dimensions or characteristics were being identified. All of the interview participants were explicitly asked about the usefulness subjective ending condition, and all agreed that the taxonomy was meeting this criterion. The robustness and explanatory character were evaluated through their intuitive understanding of the taxonomy, and their capacity to easily distinguish between the characteristics identified.

To ensure rigor, we conducted a third iteration with an empirical to conceptual approach, that consisted in the interview of four researchers with high expertise in the field of digital identity infrastructure and e-government. These semi-structured interviews also lasted between 30 and 90 minutes. Aside from bringing back a previously dismissed dimension and clarifying some of the vocabulary, this iteration did not yield any substantial changes to the taxonomy, thus confirming theoretical saturation. This iteration mainly supported us in improving the comprehensiveness, conciseness and explanatory character of the taxonomy (Nickerson et al., 2013). In total, 13 dimensions and 46 characteristics were retained. Subjective ending conditions were assessed in the same way as in the previous iteration, with the same outcome.

Finally, to validate our final ending condition, i.e., the adequate representation of a representative sample of objects, we proceeded with an empirical to conceptual approach, analyzing instantiations of 13 digital identity infrastructures. This iteration did not yield any further change compared to the previous iteration. The fact that, on the basis of the information available to us at the time of writing, all objects fit within our taxonomy and all characteristics were used, confirmed that we had met all the ending conditions and could conclude the taxonomy development process.

4. Taxonomy of digital identity infrastructures

The following section presents the taxonomy as an outcome of the four iterations of our taxonomy building process. It includes three layers, 13 dimensions, 46 characteristics. Except for the first dimension (ID authority governance model), none of the characteristics are mutually exclusive, meaning that a combination thereof is possible. In the following, we illustratively refer to instantiations that we analyzed during the last iteration of the taxonomy development process.

4.1. Ecosystem management layer

The ecosystem management layer is composed of five dimensions: **orchestrating authority**, **scope**, **cross-ecosystem interoperability**, **subjects**, and **roles of private sector actors**.

Orchestrating authority (mutually exclusive): describes how the authority responsible for setting policies and standards, certifying partners and supervising implementation (e.g., the UIDAI in India), is governed. This can take the following forms. *Inter-ministerial entity*: an arrangement in which the authority is shared as part of an inter-ministerial delegation (e.g., France). *Ministerial entity*: the authority is given to an entity within an existing ministry (e.g., the Ministry of Interior and Transportation in Argentina). *Autonomous entity with ministerial board representation*: the authority is given autonomy from a ministry, but the governing board has governmental stakeholder representation (e.g., Nigeria). *Fully autonomous entity*: the authority is autonomous and is only reporting to the highest levels of government (e.g., India).

Scope: describes how the system relates to the sovereign state. It can be *sub-national* (e.g., a region, state or territory), which is typical in federal states such as Canada or Australia. These might have an additional interoperability layer at the national level. *National* systems are common in non-federal states, such as Peru or Morocco. The *transnational* characteristic highlights that some systems are meant to be usable across borders, as is the case for eIDAS in Europe or WURI in Africa.

Interoperability approach: defines if and how interoperability with other systems is approached. It can be the case that *no interoperability* is foreseen. While some digital identity systems do not foresee interoperability with other systems, we identified several digital identity systems that are interoperable with one another (e.g., eIDAS-notified identity schemes).

Strategic Governance Choices for Digital Identity Infrastructure	Layer	Dimension	Characteristics						
	Ecosystem Management	**Orchestrating authority**	Inter-ministerial entity	Ministerial entity	Autonomous entity with ministerial board representation	Fully autonomous entity			
		Scope	Sub-national	National	Transnational				
		Interoperability approach	None	Harmonization	Mutual recognition				
		Subjects	Resident nationals	Non-resident nationals	Resident non-nationals	Non-resident non-nationals	Domestic juridical persons	Foreign juridical persons	Persons without proof of legal identity
		Roles of private sector actors	None	Authoritative source	Registrar	Data manager	Credential provider	Trust and orchestration service provider	Relying party
	IT Management	**Operation and ownership**	Public infrastructure	Private infrastructure					
		Software licensing	Closed source	Open source					
		Standards usage	Compliant	Non-compliant					
		Development funding	Public	Grant	Private				
		Operational financing	Public budget	Charge for identity providers	Charge for relying parties	Charge for data subjects			
	Data Management	**Exchange model**	Identity provider to relying party	Data subject to relying party	Federation through 1 actor	Federation through multiple actors			
		Linkability	Mediated	Non-mediated					
		Trusted data storage	Cross-sectoral repositories	Sectoral repositories	User wallets				

Table 1. Final taxonomy of strategic governance choices for digital identity infrastructures.

One approach to achieve such interoperability is *mutual recognition*, meaning that while there might be discrepancies between the rules and procedures of the digital identity system, a state could still accept to recognize digital identities issued by another state (Davies, 2006), as is the case for eIDAS in its current state. *Harmonization* goes one step further and mandates the implementation of a similar set of rules and procedures (e.g., digital wallets within the upcoming European Digital Identity Framework (Weigl, Amard, et al., 2022)).

Subjects: different categories of subjects can be included in the digital identity system. *Resident nationals* are often the primary target group, but *non-resident nationals* and *resident non-nationals* are also often considered as they maintain a substantial relationship with the country or region. *Non-resident non-nationals* can sometimes also be catered for, as can be seen in Estonia (Sallam et al., 2022). *Domestic* and *foreign juridical persons*, as entities having a legal status similar to that of a natural person, are also covered in this dimension (OECD, 2023), as well as the special category of *persons without proof of identity* (Madon & Schoemaker, 2021).

Roles of private sector actors: while institutional actors are necessarily involved in the orchestration and supervision of the infrastructure and in the certification of digital identity data, the private sector can be authorized to take part in the provision and use of digital identity services in different ways. *No role* means that the digital identity system is seen as a purely public service for government to government, citizen to government and government to citizen use cases, and is fully delivered by the public sector with no involvement from the private sector. *Authoritative source* provides a trusted source of data for use within the digital identity infrastructure (e.g., Banks in Sweden). *Registrar* is the role tasked with collecting and verifying identity data (e.g., PostIdent in Germany, some Aadhar enrolment agencies in India). *Data managers* (also sometimes called data controllers) manage the identity lifecycle, from creation to revocation (e.g., BankID in Sweden). *Credential providers* can generate and manage credentials and attestations of attributes (e.g., Buypass in Norway). *Trust and orchestration services providers* (or intermediaries) provide services, such as authentication, federation, certificate signing, identity access management and wallet provision (e.g., Aggregators in Italy, Orchestrators in the UK). *Relying*

parties consume digital identity-related services in the course of their service delivery activities. A combination of the authoritative source, registrar, data manager and credential provider roles is often referred to as an "identity provider" role.

4.2. IT management layer

The ecosystem layer is composed of four dimensions: **operation and ownership**, **software licensing**, **use of standards**, **development funding** and **operational funding**.

Operation and ownership: the IT infrastructure can be managed primarily by the *public sector* (e.g., Singpass in Singapore) and/or by the *private sector* (e.g., BankID in Sweden). Their combination as part of public-private partnerships arrangements can take several forms, such as concessions or service agreements (GSMA et al., 2016), and are increasingly used when building new infrastructure (e.g., ClaveÚnica in Chile, Aadhar in India).

Software licensing: this dimension describes the choice to be made with regards to the openness of technical development of the various modules composing the digital identity system, going from *closed-source* solutions (currently most cases) to *open-source* (e.g., MOSIP implementation in Morocco).

Standards usage: each building block of the digital identity infrastructure can either be *compliant*, or *non-compliant*, to standards, a characteristic that can significantly influence the ease of enabling interoperability, and avoiding vendor lock-in (Medaglia et al., 2022). The European Telecommunications Standards Institute, the National Institute of Standards and Technology and the World Wide Web Consortium are prime examples of standardization bodies which publish standards for digital identity (ETSI, 2021; Grassi et al., 2017; Sporny et al., 2019; W3C, 2022).

Development funding: describes the infrastructure's funding model for the pre-operational phase. The characteristics are *public funding* (including loans from e.g., international development agencies), *grants* (e.g., from donor organizations), and *private funding*. In developing countries, a mix of these options is often used to reduce the upfront investment required from public bodies (Gelb & Diofasi, 2018).

Operational financing: relates to the financing mode characteristics of the operational phase. It targets financial sustainability of operations, including providing a return on investment to private partners who invested in the building of the capacity, when applicable. The characteristics are *public budget*, *charge for identity providers*, *charge for relying parties*, and *charge for subjects*. Very often, a mix of these characteristics come into play, including for example charges to subjects for specific cases (e.g., emergency delivery of a credential). The charge can be measured according to different metrics, such as volume of transactions.

4.3. Data management layer

The data layer is composed of three dimensions: **exchange model**, **linkability** and **trusted data storage**. Design decisions related to this layer directly impact data protection and privacy, and as such are often the subject of much scrutiny both from data protection authorities and citizens (Beduschi, 2021).

Exchange model: identity data, in the form of attributes or bundled in credentials, can be transmitted through different actors. *Identity provider to relying party*: the relying party retrieves identity information directly from the identity provider or the authoritative source (e.g., healthcare providers requesting data to social security entities). *Data subject to relying party*, also sometimes called "self-sovereign identity" (Pöhn et al., 2021): the data subject holds a credential which is directly shared with the verifier (relying party), without the involvement of an identity provider in the data exchange (e.g., the European Digital Identity Framework). *Federation through one actor*: a singular gateway allows for the exchange of data and oftentimes as an authentication provider (e.g., Aadhar in India). Since all identity transactions go through this one actor, this model presents non-benign risks of surveillance that need to be addressed. *Federation through multiple actors*: several actors can act as federation service providers (e.g., FranceConnect in France). This model gives more choice to users and limits the consolidation of data and power within a single entity.

Linkability: linking of identity data, or identity data matching, can take two main governance configurations. Identity data matching can either be *mediated* by a third-party (e.g., the sourcePin Register Authority in Austria), or *non-mediated* (e.g., through a unique identifier, technological means, or simply comparing datasets for common attributes). A framework that establishes the conditions in which data matching is allowed to take place can help avoid cases of illegitimate data matching and inferences (Wachter & Mittelstadt, 2018).

Trusted data storage: data can be stored in different configurations. *Cross-sectoral repositories* merge identity data that do not belong to the same area (e.g., health, taxation). This configuration is often decried as damaging for data subjects' privacy. *Sectoral repositories* hold identity data for one specific sector. Finally, *user wallets* allow data subjects to hold a trusted

version of their identity data. In most cases involving user wallets, a copy of the data also remains in a repository to mitigate issues linked to credential loss.

5. Discussion and Conclusion

Digital identity infrastructures have seen a rise in interest from governments wanting to enable participation of their citizens in a digital society and economy. However, recent experiences show that misaligned organizational and institutional arrangements can cause project failures even in rich, developed countries, leading to public distrust, and wasted resources. To overcome this challenge and limit the risks of project failure, strategic governance choices of digital identity infrastructure design must be well identified, understood, planned, and communicated. A clear terminology and systematic guidance can support this objective (Janssen & Helbig, 2018).

In response, we developed a taxonomy of strategic governance choices for digital identity infrastructures following the development process proposed by Nickerson et al. (2013). During this process, we conducted four iterations, leveraging existing knowledge disseminated in scientific and practitioner literature, interviewed 12 specialists, and analyzed 13 existing instantiations of digital identity infrastructures. This resulted in a final taxonomy consisting of three layers, 13 dimensions and 46 characteristics of governance decision domains in digital identity infrastructure, providing an answer to the research question of this paper. Several implications are drawn from our results, applicable for both theory and practice.

Our work contributes to theory through a richer understanding of the under-researched field of governance of digital identity infrastructure. Our taxonomy expands the existing body of knowledge through a consolidation of practitioners and academic insights and establish a consensus-based terminology to support a common understanding on this topic (Rana et al., 2011). This contribution is of value to e-government research on digital infrastructure (Janowski, 2015) and can support other research directions within the wider information systems domain at large (Belanger & Carter, 2012). In brief, the contributed taxonomy can be used to distinguish and depict critical governance aspects of digital identity infrastructures in a systematic and comprehensive way, and serve as contextualization basis for theory-building (Bapna et al., 2004).

We contribute to practice on three levels. First, the list of governance characteristics of digital identity infrastructure, along with relevant design choices, can help practitioners during the design and implementation of such infrastructure. Second, given the concise and explanatory character of the provided taxonomy, we provide policymakers with a tool for contextualization to better assess the design choices that they are faced with (Janowski, 2015), thus answering the call for better research and training resources in the area of digital identity (Wimmer et al., 2020). Third, citizens who are impacted by the deployment and use of digital identity infrastructure are provided with a tool to concisely apprehend the impactful characteristics of governance thereof, consequently helping them make better informed decisions and enable them to steer their design through participative action. It also supports approach uniformity when it comes to successful digital identity infrastructure evolution.

Some limitations of this research must be acknowledged. First, the field of digital identity infrastructure is still relatively nascent and, coupled with the accelerating pace of technological innovation in the realm of identity management, it is likely that this taxonomy will have to be extended in the medium-term. Second, the high level of complexity of the topic should lead us to remain humble about the universal character of the taxonomy, as its focus might have been steered in part by the current challenges facing the digital identity community. Indeed, some of the strategic governance choices facing institutional actors today might evolve, and new governance choices might soon need to be considered in a different light. Finally, while our fourth iteration consisted in an analysis of a representative sample of instantiations of digital identity infrastructure, a systematic evaluation of further existing instantiations could potentially reveal rare characteristics that would deserve to be added.

These limitations lead us to call for further research. To better assist practitioners with actionable knowledge that can be applied within their specific context, case-study based evaluation of the impact resulting from these governance decisions could yield significant insights. While we focused on the governance aspects of digital identity infrastructure, there would also be value in delving into the technical elements that compose the infrastructure and the interplay between these two domains. Finally, there is an opportunity to dig deeper into each of the dimensions of the taxonomy, bringing in a more focused and granular view beyond the strategic design choices.

When well designed and implemented, digital identity infrastructures have the potential to promote economic development and socioeconomic inclusion in the digitalized world (Addo & Senyo, 2021; Wang & Filippi, 2020). Building on the outcome of our research, future research may contribute to the successful actualization of these benefits.

Acknowledgements

The authors would like to thank Tom Barbereau, Linda Weigl, Emanuela Podda and Reilly Smethurst for their review and contributions to the references list.

This research was supported in part by Luxembourg's Ministry for Digitalisation, PayPal and the Luxembourg National Research Fund (FNR), Luxembourg (P17/IS/13342933/ PayPalFNR/Chair in DFS/Gilbert Fridgen) and the FNR in the FiReSpARX (grant reference 14783405) project. For the purpose of open access, and in fulfilment of the obligations arising from the grant agreement, the author has applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

References

Addo, A., & Senyo, P. K. (2021). Advancing E-governance for Development : Digital Identification and its Link to Socioeconomic Inclusion. Government Information Quarterly.

Bailey, K. D. (1994). Typologies and taxonomies : An introduction to classification techniques. Sage.

Bapna, Goes, Gupta, & Jin. (2004). User Heterogeneity and Its Impact on Electronic Auction Market Design : An Empirical Exploration. *MIS Quarterly*, *28*(1), 21.

Beduschi, A. (2019). Digital identity : Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society*, *6*(2),

Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies : Data privacy and human rights considerations. *Data & Policy*, *3*.

Belanger, F., & Carter, L. (2012). Digitizing Government Interactions with Constituents : An Historical Review of E-Government Research in Information Systems. *Journal of the Association for Information Systems*, *13*(5), 363-394.

Berger, S., Bürger, O., & Röglinger, M. (2020). Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy. *Computers & Security*, *93*, 101790.

Bijker, W. E., Hughes, T. P., & Pinch, T. (Éds.). (1987). The Social construction of technological systems : New directions in the sociology and history of technology. MIT Press.

Boysen, A. (2019). *The Need for a National Digital Identity Infrastructure* (Governing Cyberspace during a Crisis in Trust, p. 36-40). Centre for International Governance Innovation.

CAG of India. (2021). Report of the Comptroller and Auditor General of India on the Functioning of Unique Identification Authority of India.

Davies, G. (2006). Is Mutual Recognition an Alternative to Harmonization? Lessons on Trade and Tolerance of Diversity from the EU. In L. Bartels & F. Ortino (Éds.), *Regional Trade Agreements and the WTO Legal System* (p. 0). Oxford University Press.

Dawes, S. S. (2009). Governance in the digital age : A research and action framework for an uncertain future. *Government Information Quarterly*, *26*(2), 257-264.

DPGA, & GiZ. (2022, mai). GovStack Definitions : Understanding the Relationship between Digital Public Infrastructure, Building Blocks & Digital Public Goods. https://digitalpublicgoods.net/DPI-DPG-BB-Definitions.pdf

ETSI. (2021). *TS 119 461*.

Gelb, A., & Diofasi, A. (2018). Identification Revolution : Can Digital ID be Harnessed for Development?

Giannopoulou, A. (2023). Digital Identity Infrastructures : A Critical Approach of Self-Sovereign Identity. *Digital Society*.

Gil-Garcia, J. R. (2012). Enacting Electronic Government Success : An Integrative Study of Government-wide Websites, Organizational Capabilities, and Institutions (Vol. 31).

Gil-Garcia, J. R., & Flores-Zúñiga, M. Á. (2020). Towards a comprehensive understanding of digital government success : Integrating implementation and adoption factors. *Government Information Quarterly*, *37*(4), 101518.

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines : Revision 3* (NIST SP 800-63-3; p. NIST SP 800-63-3). National Institute of Standards and Technology.

GSMA, World Bank Group, & Secure Identity Alliance. (2016). Digital Identity : Towards Shared Principles for Public and Private Sector Cooperation.

Hanseth, O., & Lyytinen, K. (2010). Design Theory for Dynamic Complexity in Information Infrastructures : The Case of Building Internet. *Journal of Information Technology*.

Hartwich, E., Ollig, P., Fridgen, G., & Rieger, A. (2022). Probably Something : A Multi-Layer Taxonomy of Non-Fungible Tokens.

Henfridsson, O., & Bygstad, B. (2013). The Generative Mechanisms of Digital Infrastructure Evolution. *MIS Quarterly*, *37*(3), 907-931.

ITU. (2018). Digital Identity Roadmap Guide. ITU.

Janowski, T. (2015). Digital government evolution : From transformation to contextualization. *Government Information Quarterly*, *32*(3), 221-236.

Janssen, M., & Helbig, N. (2018). Innovating and changing the policy-cycle : Policy-makers be prepared! *Government Information Quarterly*, *35*(4, Supplement), S99-S105.

Koppenjan, J., & Groenewegen, J. (2005). Institutional design for complex technological systems. *International Journal of Technology, Policy and Management*, *5*.

Madon, S., & Schoemaker, E. (2021). Digital identity as a platform for improving refugee management. *Information Systems Journal*, *31*.

Manny, L., Angst, M., Rieckermann, J., & Fischer, M. (2022). Socio-technical networks of infrastructure management : Network concepts and motifs for studying digitalization, decentralization, and integrated management. *Journal of Environmental Management*, *318*, 115596.

Masiero, S., & Arvidsson, V. (2021). Degenerative outcomes of digital identity platforms for development. *Information Systems Journal*, *31*(6), 903-928.

Masiero, S., & Bailur, S. (2021). Digital identity for development : The quest for justice and a research agenda. *Information Technology for Development*, *27*(1), 1-12.

McCallister, E., Grance, T., & Scarfone, K. A. (2010). *Guide to protecting the confidentiality of Personally Identifiable Information (PII)* (NIST SP 800-122; 0 éd., p. NIST SP 800-122). National Institute of Standards and Technology.

McKinsey. (2019). Digital identification : A key to inclusive growth.

Medaglia, R., Eaton, B., Hedman, J., & Whitley, E. A. (2022). Mechanisms of power inscription into governance : Lessons from two national digital identity systems. *Information Systems Journal*, *32*(2), 242-277.

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation : Results from expert interviews. *Government Information Quarterly*, *36*(4).

National Audit Office. (2019). *Investigation into Verify*.

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*, 336-359.

Nyst, C., Pannifer, S., Whitley, E. A., & Makin, P. (2016, juin 8). *Digital identity : Issue analysis*. Consult Hyperion.

OECD. (2023). Recommendation of the Council on the Governance of Digital Identity.

Orlikowski, W. J., & Gash, D. C. (1994). Technological frames : Making sense of information technology in organizations. *ACM Transactions on Information Systems*.

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, *20*(1).

PwC. (2021). PwC-Studie : Der Online-Ausweis auf dem Smartphone und die digitale Brieftasche.

Rana, N. P., Williams, M. D., Dwivedi, Y. K., & Williams, J. (2011). Reflecting on E-Government Research : Toward a Taxonomy of Theories and Theoretical Constructs. *International Journal of Electronic Government Research (IJEGR)*, *7*(4), 64-88.

Sallam, M., Lips, S., & Draheim, D. (2022). Success and Success Factors of the Estonian E-Residency from the State and Entrepreneur Perspective (p. 291-304).

Saunders, C., Benlian, A., Henfridsson, O., & Wiener, M. (2020, novembre 23). *IS Control & Governance*. MIS Quarterly.

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization*, *21*, 1-16.

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*, *63*, 603-613.

Sporny, M., Longely, D., & Chadwick, D. (2019). *Verifiable Credentials Data Model 1.0*. W3C Recommendation.

Temoshok, D., Richer, J., Choong, Y.-Y., Fenton, J., Lefkovitz, N., & Regenscheid, A. (2022). *Digital Identity Guidelines : Federation and Assertions* (NIST Special Publication (SP) 800-63C-4 (Draft)). National Institute of Standards and Technology.

UIDAI. (2023). *Finance & Accounts*. Unique Identification Authority of India | Government of India.

UN Legal Identity Expert Group. (2019). United Nations Strategy for Legal Identity for All.

van Dijck, J., & Jacobs, B. (2020). Electronic identity services as sociotechnical and political-economic constructs. *New Media & Society*, *22*(5), 896-914.

W3C. (2022). Decentralized Identifiers (DIDs) v1.0.

Wachter, S., & Mittelstadt, B. (2018). *A Right to Reasonable Inferences : Re-Thinking Data Protection Law in the Age of Big Data and AI* (SSRN Scholarly Paper 3248829).

Walke, F., Winkler, T., & Le, M. (2023). Success of Digital Identity Infrastructure : A Grounded Model of eID Evolution Success.

Wang, F., & Filippi, P. (2020). Self-Sovereign Identity in a Globalized World : Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Frontiers in Blockchain*, *2*, 28.

Weigl, L., Amard, A., Codagnone, C., & Fridgen, G. (2022). The EU's Digital Identity Policy : Tracing Policy Punctuations. *15th International Conference on Theory and Practice of Electronic Governance*, 74-81.

Weigl, L., Barbereau, T., Rieger, A., & Fridgen, G. (2022). The Social Construction of Self-Sovereign Identity : An Extended Model of Interpretive Flexibility. *Proceedings of the Hawaii International Conference on System Sciences 2022*.

Whitley, E. A., & Schoemaker, E. (2022). On the sociopolitical configurations of digital identity principles. *Data & Policy*, *4*, e38. https://doi.org/10.1017/dap.2022.30

Wimmer, M. A., Pereira, G. V., Ronzhyn, A., & Spitzer, V. (2020). Transforming government by leveraging disruptive technologies : Identification of research and training needs. *eJournal of eDemocracy and Open Government*.

World Bank. (2014). Digital Identity Toolkit.

World Bank. (2022a). Federated Ecosystems for Digital ID : Current Approaches and Lessons. World Bank.

World Bank. (2019a). ID4D Practitioner's Guide.pdf.

World Bank. (2019b). Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable. World Bank.

World Bank. (2022b). Identification for Development (ID4D) and Digitalizing G2P Payments (G2Px) 2022 Annual Report