CYBERNETICA

Data Exchange Technologies Department
Information Security Research Institute

Digital Government Interoperability Platform Reference Architecture

Version 1.0

Taavi Toomere, Sujani Kamalanathan, Margus Freudenthal,
Sandhra-Mirella Valdma, Keegan McBride (Hertie School)

D-2-384 / 2022

Cybernetica research reports are available online at
http://research.cyber.ee/

Mailing address:
Cybernetica AS
Mäealuse 2/1
12618 Tallinn
Estonia

Digital Government Interoperability Platform Reference Architecture

Taavi Toomere, Sujani Kamalanathan, Margus Freudenthal,
Sandhra-Mirella Valdma, Keegan McBride (Hertie School)

Version 1.0

Abstract

Interoperability is a core component for any successful governmental digitalization initiative. Though there are numerous ways to build and enable this interoperability, it is possible to identify commonly occurring building blocks. This short report identifies these building blocks, maps them to relevant and common policy goals, and presents a reference architecture model for a digital government interoperability platform. To identify the relevant components of this architecture, desk research was conducted to identify common policy goals associated with interoperability, a workshop was conducted and a comprehensive systematic and comparative study was conducted that analyzed digital government interoperability platforms in twenty countries. The results of this report represent one of the most comprehensive studies to date on digital government interoperability and should, therefore, be of high interest for governmental practitioners, industry, and academics involved with interoperability studies and initiatives.

Contents

Key Concepts and Definitions

Interoperability can be defined as either the ability to share information and services, or the ability of systems or components to exchange and use information or provide and receive services from other systems [Gro21a].

The European Interoperability Framework (EIF) consists of four different layers of interoperability: legal, organisational, technical and semantic [pro17].

- Legal interoperability is about ensuring that organizations that have different legal strategies, frameworks and policies can work together.
- Organisational interoperability refers to aligning business processes, responsibilities and expectations.
- Semantic interoperability is about ensuring that the format and meaning of data is understood when it is exchanged.
- Technical interoperability refers to having the applications and infrastructures that are linking systems and services be compatible with one another.

Digital Government as defined by the OECD, "refers to the use of digital technologies, as an integrated part of governments' modernisation strategies, to create public value. It relies on a digital government ecosystem comprised of government actors, non-governmental organisations, businesses, citizens' associations and individuals which supports the production of and access to data, services and content through interactions with the government" [OEC14].

E-government interoperability as a concept is not just having networks of organizations share information, but doing so successfully via a set of policy, legislative, management and technological capabilities (Cresswell et al., 2006; Gil-Garcia et al., 2010; Pardo Burke, 2008b; Scholl Klischewski, 2007 as cited in [PNB12]).

Government as a platform (GAAP) is a term first conceptualized by Tim O' Reilly who asked the question of what it would look like if government were organized more like an operating system, "if government is a platform, how can we use technology to make it into a better platform?"[O'R]. It focuses on the idea of government being organized "around shared components, APIs, standards and canonical datasets" [Pop19].

A **digital government interoperability platform** can be seen as a building block for the digital transformation of public administrations. These interoperability platforms "allow public and private sector entities to control which external parties get access to their databases securely" [eE21b]. A digital government interoperability platform defined in a narrow sense may include just government institutions, but the largest positive network effects are created when the platform is also open to other organizations such as the private sector and third parties.

Architecture is defined in two ways by the Open Group, the first being a formal description of a system or a delayed plan of the system (via ISO/ IEC 42010:2007) or as a structure of components, their inter-relationships, as well as the principles and guidelines that govern their design and evolution over time [Gro21a].

Building blocks help specify the scope and approach of how a business problem will be addressed in architecture design, and building blocks may have complex relationships with one another [Gro21a]. In the context of a digital government, architecture provides an overview of the different building blocks and connections between components [SSO11].

Metamodels can also be used to describe the architecture in a structured way [Gro21a].

Digital government architecture exists in several forms and with various architectural patterns. Some of the different ones identified include service-oriented architecture, a one-stop portal service center, semantic web services, layered architectures, enterprise, hybrid and distributed, decentralized, and multi-agent-based architectures [BLS20].

Based on Baheer et al.'s literature review, while there is no uniform agreement on what key concepts are required for the design of digital government infrastructure, it was found that the majority of architecture implements **G2G** and **G2C** and the majority adopted service-oriented architecture or web services [BLS20]. The one that was not seen in the majority of architecture would be **G2B**. Further, in their review, they found there was not a single view or style for interoperability architecture when it came to government [BLS20].

- **Government-to-Government or G2G** involves sharing data and conducting electronic exchanges between government or governmental agencies at any level [Nat21b].
- **Government-to-Consumer / Citizen or G2C** is meant to facilitate citizens' interaction with the government as consumers of public services. This could include receiving or requesting public service delivery or potentially participating in consultation and decision-making processes [Nat21b].
- **Government-to-Business or G2B** involves business-specific transactions and services (e.g. payments, sale and purchase of goods and services) [Nat21b].

Principles are general rules and guidelines that help an organization fulfill its mission. Principles should be future-oriented and easy to understand as they provide a foundation for making the architecture and planning decisions [Gro21a].

1 Introduction

Governments all over are increasingly working on digitalizing their administrations. This is an ongoing and continuous process driven by constantly evolving technologies and policy goals.

For any digitalization initiative, interoperability is crucial. Interoperability is what enables the provision of digital services. It allows data to be shared between governmental organizations and enhances the flow of information which improves the effectiveness of governance [Pro08]. Interoperability is a multifaceted issue, requiring support from policymakers, regulatory changes and uptake from governmental and private sector actors to become truly successful. Thus, interoperability is not only a technical issue.

In the early 2000s, the Organisation for Economic Co-operation and Development (OECD) already noted numerous issues and barriers being faced by governments developing interoperability solutions. This included problems integrating legacy systems, a lack of shared standards and infrastructure, and slow adoption of technological [eGS03]. These issues are often still present. In today's pandemic influenced society, while many governments looked to digital technologies to help continue their normal operations, technological bottlenecks were often struck. Within this context, governments all around the world are increasingly making investments into developing new technological solutions that can help to drive interoperability and whole of government digitalization.

Yet, this development is often happening within a background, with a given country, municipality, or state not being aware of solutions that have been built by others. As reuse of shared components is also a critical aspect of interoperability, it is important to have a holistic understanding of governmental interoperability initiatives and the commonly occurring technical building blocks. Such an understanding would enable anyone to quickly identify components they are missing, gain awareness of the current state-of-the-art when it comes to interoperability, and be able to efficiently and effectively build or procure needed technologies. Unfortunately, there has not been any recent systematic analyses of how governments are currently building their interoperability platforms.

This paper aims to address this gap. The research started by conducting initial desk research into policy goals associated with digital government and current leading interoperability initiatives. This was then followed by a comprehensive comparative analysis of the interoperability solutions in twenty countries: Australia, Belgium, Canada, Croatia, Denmark, Greece, Hungary, Israel, Korea, Netherlands, New Zealand, Norway, Portugal, Singapore, Spain, Sweden, United Kingdom, Uruguay, and the United States. As a result of this comparative analysis, it has been possible to identify key policy goals associated with digital government as well as the core technical building blocks associated with interoperability. By analyzing these insights it has been possible to develop a digital government interoperability reference architecture for the future of governmental interoperability platforms. This is an important contribution and will provide much-needed input to any stakeholder interested in understanding the technical aspects of governmental interoperability.

To create this digital government interoperability platform reference architecture and identify its key building blocks, there was a review of both policies and interoperability architectures. The approach to how the review was done is described in the research methodology in **Section 2**. The key inputs are reviewed in more detail in **Section 3**. Afterwards, there is an introduction to the high-level reference architecture, including a description of the layers present within it in **Section 4**. Then a more detailed description of the reference architecture, including the building blocks are outlined in **Section 5**. Lastly, a summary of the findings and future areas for research are presented in **Section 6**.

2 Research Methodology

This section describes the process used to develop the digital government interoperability platform reference architecture. The process used is shown in Figure 1.

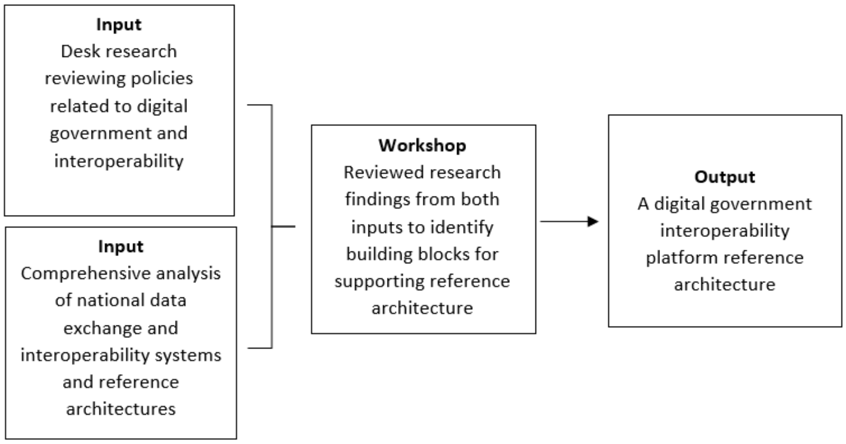
Input
Desk research reviewing policies related to digital government and interoperability
Input
Comprehensive analysis of national data exchange and interoperability systems and reference architectures
Workshop
Reviewed research findings from both inputs to identify building blocks for supporting reference architecture
Output
A digital government interoperability platform reference architecture

Figure 1: Description of inputs used to develop reference architecture

The first step was to identify the inputs for review. The inputs were policies related to digital government and comprehensive comparative analysis of national data exchange and interoperability systems and reference architectures. To review policies, desk research was conducted to understand what policies are currently in place regarding digital government. Policies can vary in scope and can be in place at various levels of government. As the scale of the intended architecture was not specific to one location, a broader scope was chosen. Rather than focusing on national policies, the policies of supranational organizations were reviewed. This was decided as they represented a global perspective on digitalization and served as a strong foundational starting point. Based on the review, it was determined to use the OECD's Digital Government Policy Framework (OECD DGPF) as it was the most comprehensive.

The other input was a comprehensive and comparative analysis of the interoperability and data exchange systems and reference architecture in twenty countries. This review included both already existing systems, those currently being built, and to-be versions published in either white papers or official documents. For this purpose, twenty countries were selected for analysis. The country selection was based on high performers in the Open Services Index in the UN e-Gov survey 2020 [Uni20] and Digital Nations countries [Nat21a]. The specific countries analyzed included: Australia, Belgium, Canada, Croatia, Denmark, Greece, Hungary, Israel, Korea, Netherlands, New Zealand, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, United Kingdom, Uruguay, and the United States.

The purpose of the review was two-fold. The first was to understand what national interoperability platforms (if any) were in place in each of the countries. The second was to identify different building blocks within those systems and determine which building blocks were seen as core building blocks within the platforms. Different sources of evidence were used to identify this information for each country and the amount of available information varied considerably across countries. While some governments directly offered insights into the technical architecture of their data exchange systems, either via interviews or through sufficient technical documentation, this was not possible in a majority of cases. Thus, several secondary sources of data were used, such as conference presentations and slides, procurement documentation, news reports, EU overviews, white papers, reports from NGOs or private sector organizations, academic literature, and other similar forms of secondary resources. In total, more than 100 sources of evidence were used in support of this analysis.

Please note that this research does not cover the enterprise-grade data exchange and API platforms targeted for small or medium-scale data exchange in the scope of one or a few enterprises. The research focuses on technical interoperability and not on semantic, organisational or legal interoperability. It deals mainly with the architecture of technical interoperability at the building block abstraction level. It also shows the relations between the reference architecture layers and the motivation as well as strategy.

After these inputs were gathered, a workshop was conducted internally within Cybernetica, where the research inputs were discussed and analyzed. There were discussions around what should be included as building blocks, the scale and scope of the reference architecture being created, and how the building blocks related to one another. Following the workshop, the digital government interoperability platform reference architecture was created.

In order to develop this architecture, the ArchiMate Enterprise Architecture modelling language tool was used. ArchiMate is "a visual language with a set of default iconography for describing, analyzing, and communicating many concerns of Enterprise Architectures as they change over time" [Gro21b]. It is a helpful tool for demonstrating the links between business goals, needs, and IT. For the purposes of the interoperability framework developed within this research, an ontology map is provided in Figure 2.

Note that not all the ArchiMate layers are not included in the ontology map. It only only depicts the layers most relevant for the reference architecture that was created. This ontology map describes the architecture in a structured way [Gro21a]. As the focus is on a platform, the layer concerning business elements was left out. The mapping of the actors and the operations of the business were also outside the scope of what the model

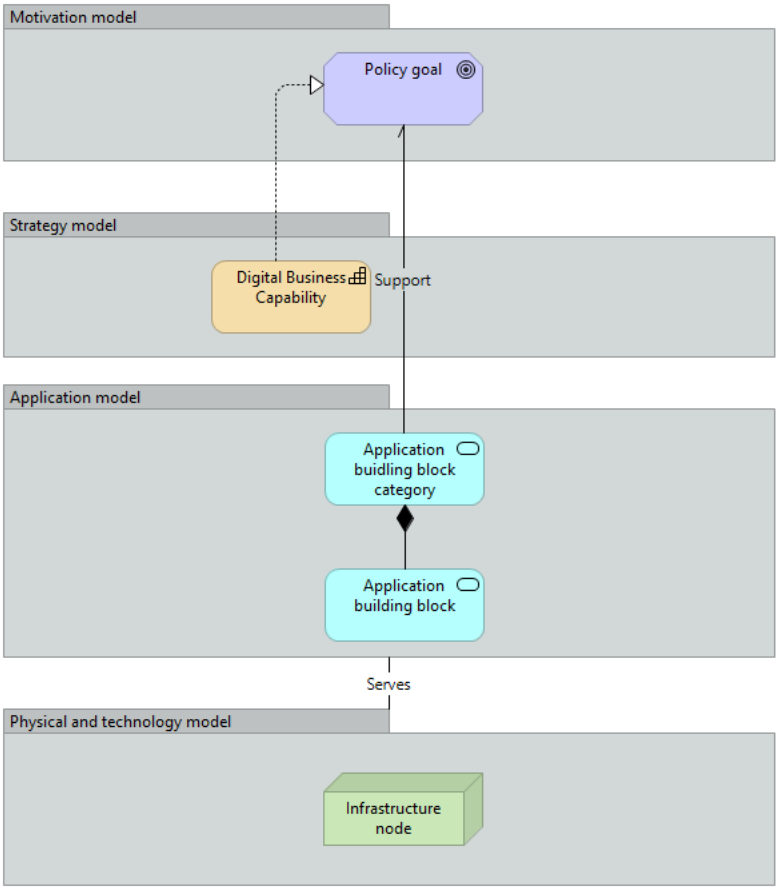
Motivation model
Policy goal
Strategy model
Digital Business Capability
Support
Application model
Application buidling block category
Application building block
Serves
Physical and technology model
Infrastructure node

Figure 2: ArchiMate Ontology Map (high level model)

intended. For this model, the focus was on the impacts of the motivation elements and strategy on the application layer.

The **Motivation layer** is used to model the reasons that guide the design or change of the architecture [Gro21b]. It includes things that can influence the architecture such as stakeholders, goals, principles and drivers to name a few. The **Strategy layer** models the strategic direction of the digital society. In this layer, digital business capabilities are listed. Capabilities can be expressed through a combination of organization, people, processes, business and IT [Gro21b]. In this model, digital business capabilities are assumed to be in place as part of the overarching digital landscape. While these capabilities are not detailed in the reference architecture, they are vital for supporting the implementation of policy goals through the interoperability platform.While this motivation layer and the strategy layer are not explored in further detail in the reference architecture diagram, they are still presented as an important part of the ontology map.

This is because the architecture is designed in a way that supports the achievement of these policy goals as discussed in Section 3.1.

In terms of detail, the application layer will be the one that is expanded upon in most detail as it contains the building blocks for the interoperability platform. **Application layer** elements are used to model the structure, behaviour and interaction of the applications within the enterprise including but not limited to the services, interfaces and components[Gro21b].

The technological and physical layer is also depicted and the building blocks within them are briefly explained. **Technology layer** elements model the technology architecture of the enterprise and describe the structure and behaviour of the technology used in the enterprise. The **physical elements layer** is an extension of the technology layer and includes things like equipment, facilities, distribution networks and materials [Gro21b]. The technology and physical layer were combined into one layer, similar to what is in the European Interoperability Reference Architecture (EIRA) framework. The inputs for the building blocks in both the application layer and the physical and technology model layer are identified through the research shown in Section 3.2.

3 Related Works and Background

This section will discuss both the policy trends affecting digital government and the technical architecture of digital governments.

3.1 Policy Goals

Policies can be a course of action or principles used by organizations that provide a framework and guidance for decision making [Wik21]. For any new reference architecture to be successful, understanding the policy goals, motivations, and objectives is critical. Thus, as a starting point for this research, it was necessary to identify commonly occurring policy goals. There are numerous initiatives at the local, regional, or national levels related to digitalization. For this research, the supranational level was analyzed. This was because as it often deals with broader and more theoretical goals and values, these are normative attributes that can be attached to cross border digitalization initiatives. By understanding these policy goals better, it is possible to develop a stronger theoretical reference architecture. With this in mind, this paper started by analyzing three supranational digital government-related initiatives. These initiatives are presented below.

- The Organisation for Economic Co-operation and Development's (OECD's) Digital Government Policy Framework (DGPF). In 2020 the OECD identified six key dimensions (digital by design, data-driven, government as a platform, open by default, user-driven, proactiveness) that make up its Digital Government Policy Framework [OEC20].
- The Digital Nations is a group that currently consists of ten countries that have formed together as the most digitally advanced governments in the world and have

created a forum to improve digital services and share best practices [Nat21a]. In their charter, they outline several principles, such as user needs, open standards, open government, digital inclusion and accessibility, sustainability, that they are committed to fulfilling as they work towards advancing their digital development. [Nat21a].

- The Principles for Digital Development (PDD) are nine principles for digital development that are meant to help in applying digital technologies to development programs. They were created in consultation with a number of international organizations including the World Bank, the World Health Organization and agencies of the UN (among others) [fDD21].

The goals from each of these initiatives were compiled and then an internal workshop was held to explore each identified policy goal in detail. For each goal it was necessary to consider how it could impact the current and future design of a digital government interoperability platform reference architecture. After a thorough review, it was determined that the OECD's DGPF was best suited to guide and structure this research. It was deemed to be the most comprehensive framework for the purposes of this research and provided sufficient goals which could then be used as a motivation to support key building blocks.

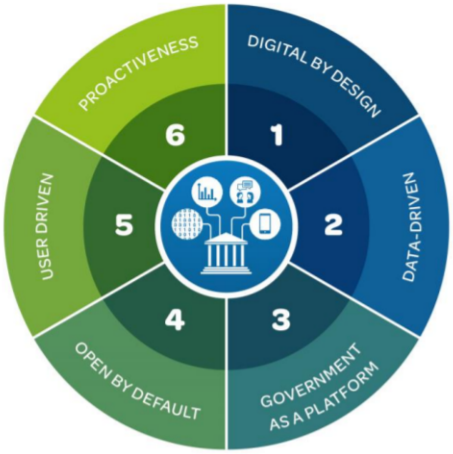

Figure 3: The OECD Digital Government Policy Framework, based on the OECD Recommendation of the Council on Digital Government Strategies from [OEC20]

Digital by Design

The first of six dimensions looked at from the OECD DGPF is the digital by design dimension.

When services work seamlessly across different channels, the public sector is able to continue investing in and benefiting from digitalisation, while simultaneously working *to ensure that no citizen is left behind due to uneven access or lack of skills necessary to use digital technologies.* [OEC20] p. 11.

This is the idea that digital is not just a technical topic, but it is more transformative and involves coordination amongst different areas [OEC20].

Data-Driven Public Sector

The second dimension looked at from the OECD DGPF is the idea of the data-driven public sector.

A data-driven public sector recognises and takes steps to govern data as a key strategic asset in generating public value through their application in the planning, delivering and monitoring of public policies, and adopts rules and ethical principles for their trustworthy and safe reuse. [OEC20] p. 14.

Both data access, and data sharing are important for a digital government and can improve service delivery. As use of newer technologies such as artificial intelligence and machine learning increase, the significance of this is only expected to grow [OEC21b].

Government as a platform

The third dimension from the OECD is that of government as a platform (GAAP).

A government acts as a platform for meeting the needs of users when it provides clear and transparent sources of guidelines, tools, data and software that equip teams to deliver user-driven, consistent, seamless, integrated, proactive and cross-sectoral service delivery. [OEC20] p. 20.

There are three models that the OECD DGPF identifies when looking at GAAP. The first is an ecosystem that supports service teams to meet needs, the second is a marketplace for public services, and the third is rethinking the relationship between the citizens and the state [OEC20]. These models are not mutually exclusive from one another and can build on progress from one area to another.

Open by Default

The fourth dimension in the OECD DGPF is open by default.

A government is open by default when it makes government data and policy-making processes (including algorithms) available for the public to engage with, within the limits of existing legislation and in balance with the national and public interest. [OEC20] p. 24.

This can be seen as a shift from more reactive and passive approaches by government to instead an approach that is more proactive. This includes the use of digital technologies and data in G2G, G2C and G2B to improve communications, consultations and engagements [OEC20].

User-Driven

The fifth dimension of the OECD DGPF is that of being user-driven.

Government becomes more user-driven by awarding a central role to people' needs and convenience in the shaping of processes, services and policies; and by adopting inclusive mechanisms for this to happen. [OEC20] p 28.

This reflects the idea of designing services with the end-user in mind and also including users in the design process [OEC20].

Proactiveness

This is the sixth dimension of the OECD.

Proactiveness represents the ability of governments and civil servants to anticipate people's needs and respond to them rapidly so that users do not have to engage with the cumbersome process of data and service delivery [OEC20] p. 33

Proactiveness is a dimension that can not exist on its own, as it builds on the other five dimensions within the OECD DGPF.

3.1.1 Policy Goals and ArchiMate Model

The importance of policy goals is seen in the motivation layer. Looking back to Figure 2, the motivation layer in ArchiMate is used to model the reasons that guide the changes of the architecture [Gro21b]. The OECD DGPF, therefore, is valuable in providing a theoretical foundation for the proposed reference architecture, particularly at the motivation layer. The policy goals relating to the digital government are seen as a big motivator for ongoing changes in interoperability platforms. As it is a forward-looking framework, identifying building blocks that support the achievement of these goals will lead to a reference architecture that is relevant to all governments interested in building a modern digital government platform.

3.2 Analysis of Government Data Exchange and Interoperability Solutions

The information in Section 3.2 is based on an internal report prepared for Cybernetica [McB21].

The initial review of the twenty countries' interoperability systems showed a wide range in terms of how advanced these systems were. For example, countries like Singapore, South Korea, and Belgium showed a high level of advancement, whereas countries like the USA, Australia, and New Zealand were on the opposite end of the spectrum. Across countries, a wide variety of approaches were used. In some, an API-first based approach was being pushed (UK, Australia, New Zealand). In others, older enterprise service bus systems were being utilized. Some countries (for example, Norway) have released state-of-the-art systems based in the cloud utilizing a microservices-based architecture, while in others (for example, Korea) a centralized method for hosting and exchanging data was used. The interoperability solutions implemented were clearly influenced by the context and governing structure of each country, for example, if it was a unitary or federal state or its public administration tradition (Confucian, Anglo-Saxon, continental Europe, etc.).

Reflecting back on how interoperability is structured within these countries, a matrix begins to emerge consisting of two dimensions: the method of data exchange, and the method of data storage. For each axis, the scale moves from centralized to decentralized. This matrix is shown as 4. Examples were seen in three of the four categories: South Korea provides an example of a country with both centralized data exchange and data storage, the Netherlands demonstrates a country that has both decentralized data exchange and decentralized data storage, and countries like Denmark and Greece demonstrate countries that have decentralized data storage, but a centralized data exchange. No examples were seen where there was a decentralized data exchange, but centralized data storage. Due to the nature of this configuration, it is also unlikely for it to appear. Most countries could be classified as having a centralized data exchange with decentralized data storage, but we may see a shift in the future from centralized to decentralized data exchange with the increasing movement towards API-based interoperability systems.

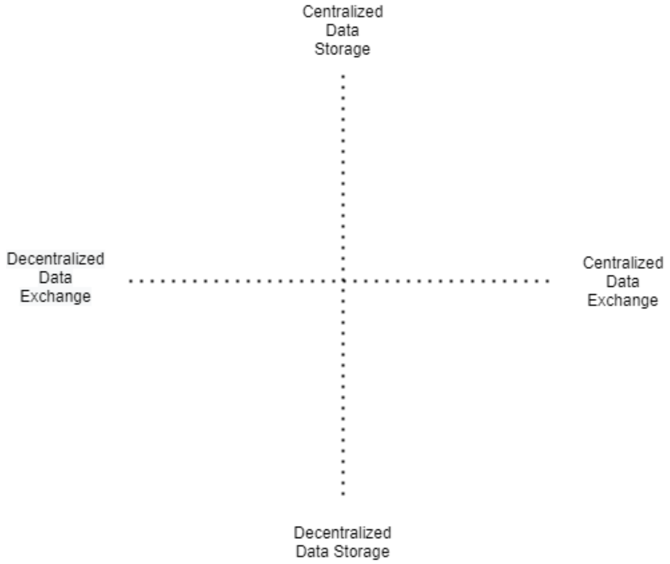

Figure 4: Data Exchange Matrix

Most interoperability systems studied still relied on SOAP-based web services for data exchange, but there was a clear interest in moving to support RESTful APIs as well, with some promising to move completely to an API based ecosystem in the future. Regarding hosting, most solutions were not yet cloud-based, though there was a clear interest to make a move in this direction. Norway provides the strongest example of a cloud-based interoperability solution.

Though the technical solutions differ quite substantively across the countries studied, there were some clearly identifiable building blocks. All platforms had mechanisms in place for security, monitoring, authorization, authentication, auditing, etc. In many countries, there was a clear desire to develop the once-only principle or the tell us once policy. This is a policy that requires the government to reuse data that is already held by another government agency. Belgium, Denmark, and the Netherlands provide the best examples for technical solutions related to this principle. Related to this is the idea of event-based notifications and business process execution. Related to this, and to ensure accurate exchange of data across contexts and organizations, was metadata or canonical data building block.

From a user perspective, two important building blocks identified were those related to MyData (a tool that gives citizens the ability to authorize a third party to query or use their data) and consent management. The MyData building block is primarily a C2B service (a citizen to business service) that encourages and enables the private sector to reuse and take advantage of existing government data with respect to citizens' right to privacy and data ownership. The consent management building block is rather a G2G component and is often found in countries where legal consent is required by a government agency to access or exchange citizens' data.

Finally, there were clear building blocks in more advanced interoperability platform solutions related to APIs. The first is a GUI for API management. These solutions enabled an easy way to manage APIs, approve access, conduct statistics, generate authorizations, and other such tasks. The other API related building block is also related to API management and is that of an API store. This API store or "catalogue" provides access to information about an API, such as its functionalities and endpoints.

3.3 Review of Government Data Exchange and Interoperability Solutions

The analysis of government data exchange and interoperability solutions was used to identify key building blocks. These building blocks are identified in the application layer of the ontology map that was created, as seen in Figure 2. The building blocks refer to the different pieces that are considered essential for the larger interoperability platform to function. The following building blocks were identified:

- APIs which include API platforms, interfaces for API management, API stores and gateways and data transformation including functionalities supported by Enterprise Service Buses;
- Governance building blocks which include organizational, data and API governance, as well as audit and monitoring;
- Catalogues which include organization, service and data catalogues;
- Communication Building Blocks for communication with citizens;
- Orchestration of Services;
- Payments for monetization of services;
- Privacy including consent management;
- Security including identity management and trust services;
- End-user authorization for services which can also include delegation;
- Event-based notifications, including business process execution; and
- Metadata including metadata management and metadata storage.

This review provided valuable input for the identification of building blocks for the digital government interoperability platform reference architecture.

4 High-level Digital Government Platform Reference Architecture

Based on the research conducted in Section 3, the digital government interoperability platform reference architecture was constructed. A quick review of how the policy and data exchange and interoperability solution analysis relates to the ontology map is seen in Figure 5. As can be seen, the scope of the reference architecture is focused on the physical and technological infrastructure, and the application building blocks and building block categories.

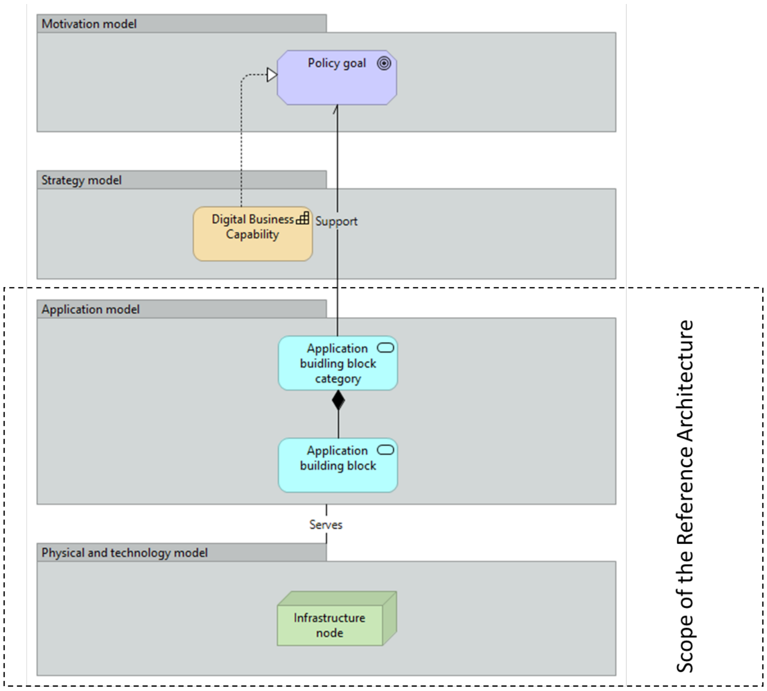
Motivation model
Policy goal
Strategy model
Digital Business Capability
Support
Application model
Application buidling block category
Application building block
Serves
Physical and technology model
Infrastructure node
Scope of the Reference Architecture

Figure 5: ArchiMate Ontology Map (high level model) with the scope of the reference architecture identified

4.1 Description of the Layers

High-level representation of the layers and categories of the building blocks in the reference architecture are shown in Figure 6. The layers are used to model the structure and behaviour. The categories indicated within the layers are a high-level way to group together related building blocks.

This section describes each of the layers in more detail.

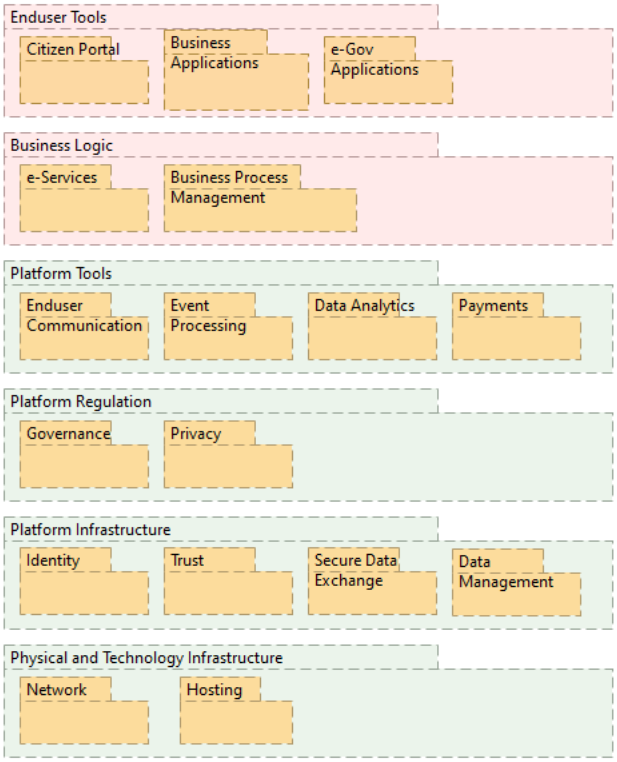

Figure 6: High-level view of interoperability platform layers and categories

- The **Physical and Technology layer** describes the categories of building blocks of Network and Hosting. This is a critical layer on which the rest of the model is based.
- The **Platform Infrastructure layer** includes several categories of building blocks and these building blocks are considered essential for building a digital society. This includes having a way to manage the data and having digitized databases, and also having an identity, trust services and secure data exchange to support interoperability and movement of data between organizations.
- The **Platform Regulation layer** focuses on the governance of the ecosystem and supports privacy.
- The **Platform Tools layer** focuses on encouraging proactive government and promotes two-way communication between all citizens, private businesses and public entities.
- The **Business Logic layer** defines the rules of how e-services function within

society, as well as the way that processes are built on top of the existing tools and infrastructure through business process management.

- The **End-User Tools layer** shows the different ways in which the stakeholders can interact with one another, share information and access services.

4.2 Digital Government Platform Layers and Applications Layers

The layers that are depicted in Figure 6 themselves fall into two groups: digital government platform layers and digital government application layers. The digital government platform layers are depicted in green and the digital government application layers in pink.

The digital government platform layers form the basis for a regulated and trusted digital society. They enable a digital economy for all stakeholders within the society including businesses, citizens and government. These layers enable society to benefit from the network effects by providing tools for interaction in the trusted environment. For example, government can include private businesses in its digital operations, or private businesses can transact with each other on the platform. The digital government platform consists of the following layers (in green) in the reference architecture:

- Platform Tools
- Platform Regulation
- Platform Infrastructure
- Physical and Technology Infrastructure

Then there are the digital government application layers. These implement the business logic of government services and have user interfaces for citizens, businesses and government clerks. The reference architecture depicts a special case of platform usage, where the platform is utilized by government applications.

The reference architecture has two application layers (in pink):

- End-User Tools
- Business Logic

In general, other organizations (such as private and third sector organizations) can operate on the platform. In this case, it can be referred to as a society level digital ecosystem.

5 Detailed View of Digital Government Platform Reference Architecture

While Figure 6 was a high-level depiction, a more detailed view is provided as well. In this section, the categories with the layers are broken down into building blocks as identified in Figure 7.

The building blocks depicted are based on what is currently found in both existing platforms and in platforms depicted via white-papers and are influenced by policy goals. Each building block is an important composition piece of the larger structure represented. A building block can be defined as a component that can be combined with others to deliver architectures or solutions and building blocks can be defined at various levels of detail [Gro21a].

5.1 Physical and Technology Infrastructure

This layer of the reference architecture includes categories of building blocks involved in networking and hosting. While the type of hosting may vary, the building blocks of the **network** and **hosting** form a critical layer on which the other categories are built.

Networking is defined as transmission systems or switching, routing or other equipment which allows signals to pass through [joi21].

Hosting can refer to the facility (equipment and components) or service and infrastructure as well. Building blocks can be hosted privately, on a **public cloud** (owned by a third party and shared between organizations) or through a **government cloud**.

5.2 Platform Infrastructure

This layer includes the categories of identity, data management, trust and secure data exchange. The platform infrastructure layer is key to supporting the tools in the layer above.

5.2.1 Identity

Identity can refer to identity management components or services and they essentially allow for user authentication [joi21]. A digital identity can apply to either a person, or an organization, and the use of a digital identity allows for authentication. It also enables systems to trace back to see who interacted with what in a system.

Identity Federation is another key building block and is defined as “the process of delegating an individual’s or entity’s authentication responsibility to a trusted external party” [Sen21] It has the benefits of allowing one ID to allow users to access multiple applications [Sen21].

5.2.2 Data Management

Metadata is essentially data about data that allows it to be managed and maintained. A metadata catalog therefore allows for the creation, storage, categorization and retrieval of metadata [joi21].

Base registries are under the control of a public administration, government or government-appointed agency and refer to a trusted and authentic source of information. They hold information about persons, companies, vehicles etc, and are seen as authentic,

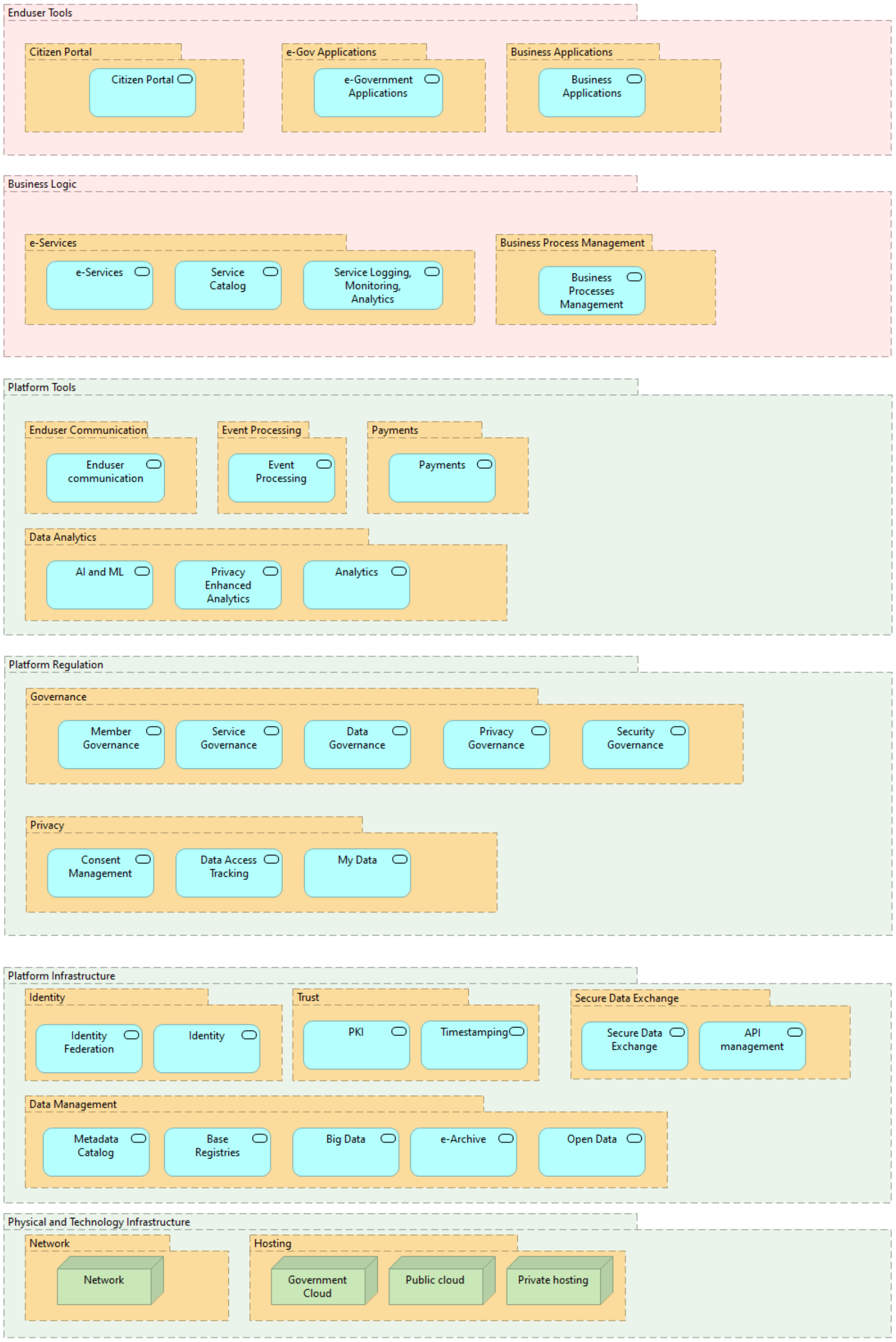

Figure 7: A detailed view of building blocks within digital government interoperability reference architecture identified via layers (green and pink), categories (yellow), and building blocks (blue)

reliable and a cornerstone for the delivery of public services. They are also sometimes referred to as basic data [Com21a]. It is important to protect the data in base registries as there is often sensitive personal data. The protection of this data is defined in legislation and regulations [Com21a]. It is also important that the quality of the data in these registries is maintained as they form the cornerstone of public services. Having base registries that are interoperable with one another also assist the implementation of the once-only principle. The once-only principle reduces administrative burden on citizens and businesses by allowing public entities to share information with each other so that if a public service is needed the information only has to be entered one time, reducing administrative burden and increasing efficiency [Dig21b].

Big data refers to large and complex data sets that come from many different sources (such as sensors, smart cars, GPS etc.) and that requires new technologies to be processed. The data is often collected in near real-time and is analyzed to gain new insights [Par21]. Key discussions and considerations around big data are privacy challenges. As the technological capabilities and the amount of data being collected increase it is also important that privacy-preserving features are considered with respect to big data.

e-Archive refers to ensuring that information is kept accessible and reusable and is preserved for long-term use [Dig21a]. Archiving is often managed under a document management policy or law which determines the length of time for storage and outlines rules around the preservation of files.

Open Data [dat21] refers to information collected, produced or paid for by the public sector which is then made available and accessible for reuse for any purpose. Openness is a key policy goal and it is a way to improve the performance of the public sector through improving the efficiency of public services and their quality, the economy through the development of innovative services and society through improved transparency and accountability [OEC20]. Governments promote business and the development of innovative, citizen-centric services by providing and encouraging the use and reuse of datasets [OEC21a].

5.2.3 Trust

Trust refers to electronic services that help parties make binding decisions and this category includes the building blocks of PKI and timestamping [iD21b].

PKI or Public Key Infrastructure refers to the creation, management, distribution, storage and revocation of digital certificates through a set of established policies and systems [eni21]. Digital certificates are used for secure communications and digital signatures, and the PKI is there to authenticate the certificate and make sure it can be trusted [eni21].

Timestamping refers to the use of an electronic timestamp which can be used for auditing purposes as well. Timestamping is used to prove that certain data existed at a certain moment [iD21a].

5.2.4 Secure Data Exchange

Secure Data Exchange refers to the ability to exchange data between different organizations in a way that maintains privacy and security (i.e. sending it over encrypted and authenticated channels) and also ensures that data integrity is maintained throughout the exchange. In the context of a large society level platform like digital government, scalability of the data exchange is an important consideration.

API Management enables the publishing, testing and executing of APIs on the platform and enforces usage policies and access control. It also allows the collection and analysis of statistics of API usage on the platform.

5.3 Platform Regulation

This layer represents some key principles and characteristics of the digital government platform and includes the categories of governance and privacy. It interacts with all the others layers as it is a central component of the platform. These categories govern the rules of the other building blocks and contribute to the establishment of trust and also enforcing regulations within the platform.

5.3.1 Governance

Governance refers to various types of governance including member, service, data, privacy and security. From an organizational perspective, this refers to shared legal frameworks. Security frameworks can refer to “agreed governance approach focusing on protection aspects on data, information and knowledge assets and organizational resources handling them” and the security policies refer to the rules and procedures for individuals accessing and using IT [joi21]. Privacy frameworks refer to an “agreed governance approach focusing on confidentiality aspects on data, information and knowledge assets and organizational resources handling them” and privacy policies refer to how parties gather, use disclose and manage data[joi21]. Data policies refer to “a set of broad, high level principles which form the guiding framework in which data management can operate" [joi21].

5.3.2 Privacy

Under the category of privacy there are three building blocks identified. The first is **consent management**. Consent management supports compliance with regulations and ensures that the user understands what their data is being used for and that their agreement to, or rejection of the use of their data for that purpose is managed [GDP21].

Data access tracking is the ability to check the use of personal data in databases and to see which organizations are querying the data and what kind of personal data is being shared.

My Data is an umbrella building block for the rest of citizen privacy features including personal data audit and delegation of citizen rights.

5.4 Platform Tools

The platform tools layer enables implementation of democratic values as the building blocks support data-based policy making, and encourage proactive government and promotes two-way communication between all citizens, private businesses and public entities.

5.4.1 Data Analytics

One of the building blocks within this category is **Artificial Intelligence and Machine Learning**. AI is defined as “systems that display intelligent behaviour by analysing their environment and taking actions — with some degree of autonomy — to achieve specific goals" [Com21b]. There is also the building block of **privacy enhanced analytics**. This is being able to protect personal data while still allowing data to be analyzed and used, but in a way that anonymizes data and prevents the data from being personally identifiable. One example of this is Sharemind [BLW08], which is a privacy enhancing technology that allows data-driven services while still providing end-to-end data protection.

5.4.2 Payments

Payment refers to an e-payment component. This allows the system to complete payment transactions and allows payments to be transacted through an e-payment service [joi21].

5.4.3 Event Processing

Event processing is a method of tracking and analyzing (processing) streams of information (data) about things that happen (events) [Wik22]. It simplifies the implementation of proactive life-event based e-services. In the Estonian context, this means that if the information is available and citizens have agreed to the use of the information for these purposes, then the state can proactively offer opportunities rather than waiting for the citizen to initiate the process [EE21a]. Examples of life-event based proactive services are the birth of a child or starting a business.

5.4.4 End-User Communication

The **end-user communication** building block is a catch-all and refers to communications with citizens, private businesses and government clerks which can now happen in a variety of different ways digitally such as chat, email and SMS. It allows for two-way communication between government agencies and citizens and other stakeholders, potentially in real-time, through the use of these tools.

5.5 Business Logic

The business logic layer encompasses the categories of e-services and business process management. It defines the rules of how e-services function within society.

5.5.1 E-Services

Public e-services are services provided via technology by government or public agencies to either businesses or citizens. E-services include the building blocks of service, service catalogue and service logging, monitoring and analytics. Stakeholders such as private businesses, public agencies and citizens should be able to access e-services.

5.5.2 Business Process Management

Business process management is understanding the business processes involved and the workflows which can then be automated, analyzed and improved. This is a key building block when considering how processes are designed, modelled, executed, monitored, optimized and also re-engineered as processes may be shifting from analogue to digital or as systems are made interoperable.

5.6 End-User Tools

This layer consists of the categories and building blocks of citizen portals, e-government applications and business applications.

Citizen portals provide a single point of access to services for citizens. There are many national portals, that vary in terms of the number and depth of services they provide.

E-government applications is also a broad building block that includes different services, including the ones that enable data-driven policymaking.

Lastly, there are **business applications** which allow private businesses to access applications on the digital government platform.

5.7 Policy Goals and Reference Architecture Model

This brief discussion builds on an understanding of the reference architecture that was presented and shows how the layers and building blocks can help support the achievement of the OECD DGPF.

The **data-driven government dimension** of the OECD includes data-driven services and analysis, and also consent and transparency of use of private data. Providing data-driven services within government includes the delivery of e-services. Data analysis to support a data-driven government is achieved through the category of data analytics, which includes building blocks like privacy-enhanced analytics and AI and ML. Consent and transparency over the data being used by the government is achieved through the building blocks within the privacy category (consent management, data access tracking).

The next dimension is **digital by design**, which also includes the ideas of legislative support, digital skills, technological capabilities and digitalized base registries. Within the reference architecture, it is assumed that digital capabilities are in place as they are integral to not just supporting a platform, but also supporting a digital government.

The dimension of **government as a platform** forms the platform layers and includes the GAAP infrastructure, which is being presented within this research. This includes the categories of identity, data management and trust as well as their related building blocks. It also includes looking at the scope of services (government, citizen, business), which influences the categories related to e-services and identity. It impacts the layer of end-user tools and designing the platform for scale. Further, it is important to consider both platform security and platform governance as part of GAAP which is reflected in the platform regulation layer.

The dimension of **openness** includes open data, transparency, open protocols and standards, open-source and open innovation. This is reflected in categories of governance, privacy and data management.

The dimension of **user-centricity** is about looking at the user-driven design, and digital inclusiveness. This is reflected in the layer of end-user tools. This is a shift from government-centred approaches to instead now focusing more on user-driven approaches. This in turn emphasizes two-way communication flows and services that are simple and less bureaucratic. This can be seen in the platform layers tool which includes the categories of end-user communication, payments and event processing. It also touches on the building blocks in the layers of business logic and end-user tools which all represent digital transformation changes from formerly analogue processes.

And lastly, the dimension of **proactiveness** includes anticipating citizen needs and proactive service execution. Achieving this policy goal relies on categories within the platform-tools and building blocks including technology such as AI and ML. Proactive service execution relies on other categories within the platform layers tool including event processing. This type of anticipatory government is built on building blocks associated with the other dimensions, such as having a data-driven government.

6 Conclusion

The goal of this paper was to understand how governments are currently building their interoperability platforms. The research looked at policies relating to digital government and also at the interoperability and data exchange systems, and reference architectures in different countries. This information was then used to identify the building blocks which would support a digital government interoperability platform reference architecture. This approach was unique because the building blocks we identified are also meant to support the achievement of the OECD DGPF, as a policy is also an important consideration for governments. During the research, we gained a solid understanding of governmental interoperability initiatives and identified the commonly occurring technical building blocks. This resulted in the creation of the reference architecture, which can be used as a basis for future discussions regarding government interoperability.

One of the main takeaways from the research is that a digital government interoperability platform reference architecture is a much wider concept than the digital government itself. It is a tool that enables regulated data exchange for the whole society. However, the scope of services within the platform can be used by more than just digital government. For example, it also has the potential to be used by private sector and third-party entities which allows for positive network effects and a potential increase in services and applications.

Additionally, it is important to consider the key building blocks. These are the foundational building blocks for building a digital society. Examples include trust, secure data exchange, identity and base registry building blocks. These are seen in Figure 7 within the platform infrastructure layer and they are a critical base for supporting the reference architecture.

Lastly, a distinguishing feature of a digital government interoperability platform is the importance of platform regulation. This includes consideration around trust, privacy and governance. The regulated exchange of data is a unique feature within the platform. It contributes to establishing trust and provides a way to enforce regulations within the platform. It is important as it is not just the public sector, but also non-government entities that can be a part of the platform.

Interoperability is an overarching term and this is reflected in the design of the reference architecture. It is not solely about a technical exchange of data. The building blocks show that it is also about supporting data exchange through various factors such as policy, regulation and data governance.

Governments around the world are continuing to invest in new technological solutions. For future conversations it is important to have both an understanding of what the common occurring technical building blocks are, and what policy goals could be supported through the implementation of these building blocks. This reference architecture is based on a theoretical foundation in policy, and a practical foundation in understanding what technical building blocks some governments are using. Therefore, it can be a useful tool for identifying the key building blocks needed for a digital government interoperability platform reference architecture.

6.1 Future Research

This reference architecture is our first attempt at identifying key building blocks and the policies that influence them. Future research could include a closer look at the existing technological infrastructure in more detail to understand how the current situation influences future development. One approach would be to do a detailed cross-country comparison of different data exchange technologies and systems. While this paper looked at different systems and compared them at a high-level, a more detailed look at the technological differences between the systems could provide valuable insight.

Another area for further analysis is a more detailed look at how each building block identified within the reference architecture is currently implemented in practice, or what needs to be done to implement the building block. One example of this could be a review of architecture of event-based services, and event processing on an interoperability platform. All digital governments are in a state of evolution and digitalization is a process that needs to be continually reviewed and updated. While the policy trends provide a theoretical foundation, we should also continue to understand changes in the technological landscape to see what impacts, if any, these new technologies may have on digital government interoperability platforms. On a final note, this reference architecture did not consider the business layer elements, or the organizational processes. A review of the business processes and workflows could be done to expand the reference architecture.

References

[BLS20] Baseer Ahmad Baheer, David Lamas, and Sónia Sousa. A systematic literature review on existing digital government architectures: State-of-the-art, challenges, and prospects. *Administrative Sciences*, 10(2), 2020.

[BLW08] Dan Bogdanov, Sven Laur, and Jan Willemson. Sharemind: A framework for fast privacy-preserving computations, 2008.

[Com21a] European Commission. Access to Base Registries. https://ec.europa.eu/isa2/sites/default/files/publications/access-to-base-registries-good-practices-on-building-successful-interconnections-of-base-registries.pdf, 2021. (accessed: 09.12.2021).

[Com21b] European Commission. Artificial Intelligence for Europe. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN, 2021. (accessed: 09.12.2021).

[dat21] data.europa.eu. What is open data. https://data.europa.eu/en/trening/what-open-data, 2021. (accessed: 09.12.2021).

[Dig21a] CEF Digital. eArchiving. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eArchiving, 2021. (accessed: 09.12.2021).

[Dig21b] CEF Digital. Once-Only Principle. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Principle, 2021. (accessed: 09.12.2021).

[EE21a] E-Estonia. Proactive government. https://e-estonia.com/wp-content/uploads/facts-a4-proactive-government.pdf, 2021. (accessed: 09.12.2021).

[eE21b] e Estonia. Why there's no digital transformation without interoperability. https://e-estonia.com/why-theres-no-digital-transformation-without-interoperability/, 2021. (accessed: 09.12.2021).

[eGS03] OECD e Government Studies. The e-Government Imperative. https://www.oecd-ilibrary.org/governance/the-e-government-imperative_9789264101197-en, 2003. (accessed: 09.12.2021).

[eni21] enisa. Public Key Infrastrcture (PKI). https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/public-key-infrastructure-pki, 2021. (accessed: 09.12.2021).

[fDD21] Principles for Digital Development. Principles for Digital Development. https://digitalprinciples.org/, 2021. (accessed: 14.10.2021).

[GDP21] GDPR.EU. What are the GDPR consent requirements? https://gdpr.eu/gdpr-consent-requirements/, 2021. (accessed: 09.12.2021).

[Gro21a] The Open Group. The TOGAF Standard, Definitions . https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap03.html#tag_03_23, 2021. (accessed: 09.12.2021).

[Gro21b] The Open Group. Welcome to the ArchiMate® 3.1 Specification, a Standard of The Open Group. https://pubs.opengroup.org/architecture/archimate3-doc/toc.html, 2021. (accessed: 09.12.2021).

[iD21a] iD. Trust services: timestamping service. https://www.id.ee/en/article/trust-services-timestamping-service/, 2021. (accessed: 09.12.2021).

[iD21b] iD. Trust Services: What are they? https://www.id.ee/en/article/trust-services-what-are-they/, 2021. (accessed: 09.12.2021).

[joi21] joinup. Chapter 4 EIRA Glossary . https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira/chapter-4-eira-glossary, 2021. (accessed: 09.12.2021).

[McB21] Keegan McBride. Technical Analysis of Governmental Data Exchange and Interoperability Solutions: A twenty country comparative study. Unpublished (Internal Report in Cybernetica), 2021. (prepared: 22.11.2021).

[Nat21a] Digital Nations. Digital Nations Member Countries. https://www.leadingdigitalgovs.org/organization, 2021. (accessed: 01.10.2021).

[Nat21b] United Nations. E-Government. https://publicadministration.un.org/egovkb/en-us/about/unegovdd-framework, 2021. (accessed: 09.12.2021).

[OEC14] OECD. Recommendation of the Council on Digital Government Strategies. https://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf, 2014. (accessed: 09.12.2021).

[OEC20] OECD. The oecd digital government policy framework. https://www.oecd.org/gov/the-oecd-digital-government-policy-framework-f64fed2a-en.htm, 2020.

[OEC21a] OECD. Open Governemnt Data. https://www.oecd.org/gov/digital-government/open-government-data.htm, 2021. (accessed: 09.12.2021).

[OEC21b] The OECD. Data governance: Enhancing access to and sharing of data. https://www.oecd.org/sti/ieconomy/enhanced-data-access.htm, 2021. (accessed: 17.01.2022).

[O'R] Tim O'Reilly. Chapter 2. Government As a Platform. https://www.oreilly.com/library/view/open-government/9781449381936/ch02.html. (accessed: 09.12.2021).

[Par21] European Parliament. Big data: definition, benefits, challenges (infographics). https://www.europarl.europa.eu/news/en/headlines/society/20210211STO97614/big-data-definition-benefits-challenges-infographics, 2021. (accessed: 09.12.2021).

[PNB12] Theresa A. Pardo, Taewoo Nam, and G. Brian Burke. E-government interoperability: Interaction of policy, management, and technology dimensions. *Social Science Computer Review*, 30(1):7–23, 2012.

[Pop19] Richard Pope. Playbook:Government as a Platform. https://ash.harvard.edu/files/ash/files/293091_hvd_ash_gvmnt_as_platform_v2.pdf, 2019. (accessed: 09.12.2021).

[Pro08] United Nations Development Programme. e-Government Interoperability. https://www.unapcict.org/sites/default/files/2019-01/e-Government%20Interoperability.pdf, 2008. (accessed: 09.12.2021).

[pro17] ISA² programme. The new european interoperability framework. https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf, 2017. (accessed: 04.10.2021).

[Sen21] Dinika Senarath. Identity Federation – a brief introduction. https://dinika-15.medium.com/identity-federation-a-brief-introduction-f2f823f8795a, 2021. (accessed: 09.12.2021).

[SSO11] Khairul Anwar Sedek, Shahida Sulaiman, and Mohd Adib Omar. A systematic literature review of interoperable architecture for e-government portals, 2011.

[Uni20] United Nations. UN e-government survey 2020. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020UNE-GovernmentSurvey(FullReport).pdf, 2020. (accessed: 01.10.2021).

[Wik21] Wikipedia. Policy. https://en.wikipedia.org/wiki/Policy, 2021. (accessed: 09.12.2021).

[Wik22] Wikipedia. Complex Event Processing. https://en.wikipedia.org/wiki/Complex_event_processing, 2022. (accessed: 11.01.2022).