Master's Thesis of Public Administration

A Comparative Study of Digital Identity Scheme in Korea and Peru focuses on the identification and authentication of natural persons

- Digital Identity Scheme -

한국-페루 디지털 정체성 제도에 대한 비교연구: 인간의 증명과 인증을 중심으로

February 2023

Graduate School of Public Administration
Seoul National University
Global Public Administration Major

Yuri Aldoradin Carbajal

A Comparative Study of Digital Identity Scheme in Korea and Peru focuses on the identification and authentication of natural persons

– Digital Identity Scheme –

Academic Advisor Kim, Junki

Submitting a master's thesis of Public Administration

October 2022

Graduate School of Public Administration
Seoul National University
Global Public Administration Major

Yuri Aldoradin Carbajal

Confirming the master's thesis written by
Yuri Aldoradin Carbajal

December 2022

Chair	Ko, Kilkon
Vice Chair	Choi, Taehyon
Examiner	Kim, Junki

A Comparative Study of Digital Identity Scheme in Korea and Peru focuses on the identification and authentication of natural persons

ABSTRACT

A Comparative Study of Digital Identity Scheme in Korea and Peru focuses on the identification and authentication of natural persons

– Digital Identity Scheme –

Yuri Aldoradin Carbajal
Global Public Administration Major
The Graduate School of Public Administration
Seoul National University

Digital identity is the collection of attributes that uniquely differentiates a person in his interaction with digital services. The literature and previous research suggest that it is an essential component to the digital transformation and a vital element for strengthening the digital trust. Currently, due to worldwide spread of COVID-19, which has accelerated the digital transition in the public and private sector, the non-face-to-face transactions have been increased, coupled with cybercrimes such as identity theft, private data leakage, fraud, among other cybercrimes. In this sense, governments should become aware of the importance of digital identity management, because it is increasingly embedded in everything we do in our digital and offline life (WEF, Identity in the Digital World a new chapter in the social contract, 2018, p. 9). To deal with those issues and leverage all the potential of digital identity at national level, many countries implement a Digital Identity Scheme, which is a well-designed and articulated collection of policies, business rules, technologies, organizations, and processes in charge of governing the digital identity lifecycle to promote a digital society. Hence, countries such as The Republic of Korea (hereinafter, Korea) and The Republic of Peru (hereinafter, Peru) have been developed and implemented different kind of policies, legal instruments, initiatives, and digital technologies to enhance accessibility,

efficiency and security of the identification and authentication process, for instance, Korea has issued the Electronic Government Law and implemented cross-platforms such as Government24 (정부 24) as official electronic government portal, Digital ONEPASS (디지털원패스) as a digital authentication platform to enable a convenient no-face-to-face authentication of the citizens, Resident Registration System (RRS), as a fundamental national information system which manages and stores relevant personal information of Koreans, and Sharing Information System (행정정보공동이용시스템), as a interoperability platform to exchange information with governmental agencies. Moreover, Korea has a PKI Scheme which is divided into a National Public Key Infrastructure (NPKI), and a Government Public Key Infrastructure (GPKI). All these regulations, technologies and platforms are vital elements of the Korean Digital Identity Scheme.

In the case of Peru, based on Law N° 26497 enacted in 1995, the government has been managing and maintaining the National Identification Registry of Peruvian. Moreover, since issuance of Digital Government Law in 2018, Peru has been implemented different kind of cross-platforms such as the Single Digital Platform for Citizen Orientation (GOB.PE), to offer one point of contact between government and citizens, National Interoperability Platform, to promote information exchange among public entities, the National Digital Government Platform, to provide cloud services to the public entities, and National Platform for Identification and Authentication of Digital Identity (ID.GOB.PE), to verify a person's identity.

Although there are similarities, the outcomes are different, in the Electronic Government Development Index 2022, Korea is ranked 3rd in the world, while Peru is ranked 59th, from another side, in terms of digital identity, Korea has a digital identity ecosystem operating, for instance Government24 accepts several authentication methods which are easily and conveniently for the citizens such as ONEPASS, KAKAO, Samsung PASS, among others (MOIS, Status of Government 24, 2022). To 2021, almost 132,025,035 petitions were filed online through Government24 (MOIS, Status of Government 24, 2022). In the case of Peru, the digital identity scheme is an ongoing project, which is leading basically by the government, based on the Digital Government Law and its enforcement decree. In that vein, this research aims at understanding the

components for governing and managing a Digital Identity Scheme in Korea and Peru and identifying the gap between them. Therefore, in this study we are going to focus on how the Digital Identity Scheme of Korea is performing to strengthen accuracy, inclusiveness, security, and usability of digital identity of persons. We are going to establish the similarities and differences by using a comparison framework which is an adaptation of the frameworks used by the United Nations (UN), International Telecommunication Union (UIT) and Organization for Economic Cooperation and Development (OECD). Additionally, in this moment, undertaking a comparison study between Korea and Peru is a relevant work, because Peru is implementing transversal digital government platforms based on the Digital Government Law, and based on that we are dealing with cybercrimes and digital threats, that is why we can learn of the best practices and good lessons of the Digital Identity Scheme in Korea and design better policies and decisions for Peruvian implementation.

This research was carried out by using a qualitative research method which involved online interviews with ICT specialists from Korea and Peru to generate an in-depth understanding of the digital identity scheme of both countries. A total of ten specialists were interviewed. Interviews provide an overview of the digital identity evolution in Korea and allow me to identify challenges and policy recommendations in the implementation process of Digital Identity Scheme in Peru. Based on the results the big differences are integrated in three factors: strong and continuous digital leadership, timely legal framework, and modern ICT technology to support development and public services rendering.

However, the results also suggest that it is possible to get big achievements on the Digital Identity Scheme in Peru, making institutional arrangements, enhancing digital regulation and optimizing the budget with the purpose to create a sustainable digital identity ecosystem.

Keyword: Peru, Korea, Digital Identity, Digital Government, Digital Transformation, Digital Identity Scheme, PKI.

Student Number: 2021-20119

Content

LIST OF ABBREVIATIONS

DGI: Digital Government Index
EGDI: Electronic Government Development Index
GPKI: Government Public Key Infrastructure
eIDAS: The Regulation on electronic identification and trust services for electronic transactions in the internal market
IADB: InterAmerican Development Bank
ICT: Information and Communication Technology
ITU: International Telecommunications Union
IOFE: National Electronic Signature Infrastructure
MOIS: Ministry of the Interior and Safety
MSIT: Ministry of Science and ICT.
NIA: National Information Society Agency
NIST: National Institute of Standards and Technology
NPKI: National Public Key Infrastructure
OECD: Organization for Economic Cooperation and Development
OECD DAC: Organization for Economic Cooperation and Development Assistance Committee
OAUTH: Open Authorization Framework
PKI: Public Key Infrastructure
KISA: Korea Internet and Security Agency
RENIEC: Registro Nacional de Identificación y Estado Civil
RRA: Resident Registration Act
RRS: Resident Registration System
RRN: Resident Registration Number
R&D: Research and Development
RFC: Request for Comments
SDG: Sustainable Development Goals
TLS: Transport Layer Security.
UK: United Kingdom
UN: United Nations
US: United States
UNDESA: Department of Economic and Social Affairs of United Nations
WEF: World Economic Forum

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

1.1 STUDY BACKGROUND

A ubiquitous society, smart nation or digital society are just some kind of names given for this radical change in the whole society based on the integration and adoption of digital technologies and data in our day-to-day economic-social life.

In this regard, it is an unavoidable fact that more and more social and economic activities depend on digital technologies and data (WEF, The Global Risk Report 2022, 2022, p. 9), that is why, some scholars and researchers assert that digital technologies and data are catalyst for prompt transformation of the society (Kim S. , The Evolution of Korean e-Government, 2015, p. 1), others point out that we do not have another way, the integration of government innovation and digital technologies, what we called electronic government or digital government is a mandatory initiative for being efficient and enhancing productivity.

In that sense, electronic government is not only the most recent paradigm in the ongoing process of modernizing public administration; it has also become a strategic policy intervention to boost efficiency and productivity in economic and social activities (Eifter, 2004, p. 2).

In that vein, the broad deployment of digital technologies and data in the public administration is the beginning of a new era of governance (Sadigova, 2014, p. 1) , which implies the overall transformation of the government (goals, functions, structures, rules and civil servants' awareness) (Chong-sik, 2020, p. 176) .

Governments can no longer remain the bureaucratic inertia, low efficiency, cumbersome processes, and negative image that people have about

it, they must embrace the innovation, citizen-centered approach, and digital government as a heart of the new public administration.

In this regard, along with the digital advances, new strategic approaches emergence; nowadays, developed countries such as United Kingdom, Korea, United States and international organizations such as OECD, ITU, UN, and global consulting firms such as Gartner Group, Deloitte Research and Accenture have ceased to use the term electronic government (e-government) and have begun to promote digital government or digital transformation as a key component of government modernization strategies (Chong-sik, 2020, pp. 5-13).

In this context, by seeking not to be left behind or to be digitally excluded, many countries have established the digital transformation as a national objective of their society, which stretches from public sector and private sector to academia, industry, and citizens.

Moreover, to reach that goal, some countries have issued national policies, strategies, plans or laws, with the aim to boost digital inclusion, promote digital innovation, enhance interoperability, improve transparency, protect privacy, strengthen digital trust and promote digital technologies adoption in your society.

Likewise, crosscutting digital platforms such as public information sharing systems, digital authentication platforms, official electronic government portals, (single point of contacts with citizens) aim at providing convenient, secure and trustworthy digital services to the citizens.

Table 1. Some key Digital Government Initiatives over the time

Digital government initiatives	Country	Year
Electronic ID Card for citizens	Finland	1999
National Public Key Infrastructure (NPKI)	Korea	2000
Electronic Government Act	Korea	2001
Electronic Government Act	United States	2002
Government for Citizens (G4C)	Korea	2002

Public information sharing systems	Korea	2005
National Information Resources Service (NIRS)	Korea	2005
National platform of interoperability	Peru	2011
Digital Government Strategy	United States	2012
Single point of contact (GOV.UK)	United Kingdom	2012
Digital Government Law	Peru	2018
Single point of contact (Government24)	Korea	2018
Single point of contact (GOB.PE)	Peru	2018

Source: Own development, 2022

As a result, the number of digital services, applications and digital platforms which are trying to meet citizen's needs, and demands are exponentially increasing and being able to differentiate between digital and offline life becomes more and more diffuse.

At the same time, scholars and researchers became aware of issues related to digital trust, privacy, national security, and digital security (cybersecurity). They emerge as pain points in a digital society, the reason why they become either items in our digital agenda or political opportunities for policymakers.

Consequently, it must be recognized that now developed and developing countries are in the middle of an ongoing digital transformation process (UN, E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development, 2020, pp. 33-34), which, irrespective of whether we like it or not, will change the way public sector, private sector, academy, and citizens have been performing their activities.

As you can be seen, the traditionally face-to-face dealings with the government and private sector have been replaced by non-face-to-face interactions, therefore, every day citizens must prove their identity using different kind of credentials such as account logins (user and passwords), biometrics (eye scan or fingerprints) or identity cards (Sullivan, 2018, p. 2).

Drawing on the above, it is important to mention that on June 18, 2008, as part of the Seoul Declaration for the future of the internet economy, ministers

declared that, "*for contributing to the development of the internet economy, they will strengthen confidence and security, through policies that ensure the protection of digital identities and personal data as well as the privacy of individuals online*" (OECD, Seoul Declaration on the Future of the Internet Economy, 2008). Consequently, it can be inferred that if a person has many credentials, there is a high-risk level of increasing information security issues such as identity theft or fraud.

In this regard, the challenge for the governments is to envisage a vision, strategy, policies, plans, and institutional arrangements to leverage the benefits and potential of a safe, inclusive, trustworthy, and affordable digital identity for the citizens.

According to the OECD a proper digital identity management can bring the following benefits: a) allow people identify yourself online, b) promote information security, c) enable a trusted relationship between parties, d) set a proportional and rationale level of assurance of the identity of the remote parties, and e) protect privacy and personal information (OECD, The Role of Digital Identity Management in the Internet Economy: a Primer for Policy Makers, 2009).

Thereby, over the last decade, the Europe Union developed a series of guidelines and standards to lead the digital identity management implementation at national level and allow the cross-border digital authentication at European level, for instance, in 2014 the European Parliament enacted the Regulation N° 910/2014 Electronic Identification and Trust Services for Electronic Transactions in the internal market, often called eIDAS, as a result, Europe has a specific framework to promote a cross-border digital identity ecosystem between its members, countries like Estonia, Australia,

Spain, Finland, Italy, Croatia, Finland, among others have designed and deployment a National Digital Identity Scheme.

Table 2. National Identity Scheme Portals

Country	Portals
Estonia	https://www.id.ee/en/
Australia	https://www.digitalidentity.gov.au/
Spain	https://www.dnielectronico.es/
Germany	https://www.ausweisapp.bund.de/home/
Italia	https://www.spid.gov.it/en/
Croatia	https://nias.gov.hr/en
United Kingdom (UK)	https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify
France	https://franceconnect.gouv.fr/cgu
Denmark	https://www.nemid.nu/dk-en/get_started/request_nemid/

Source: Own development, 2022

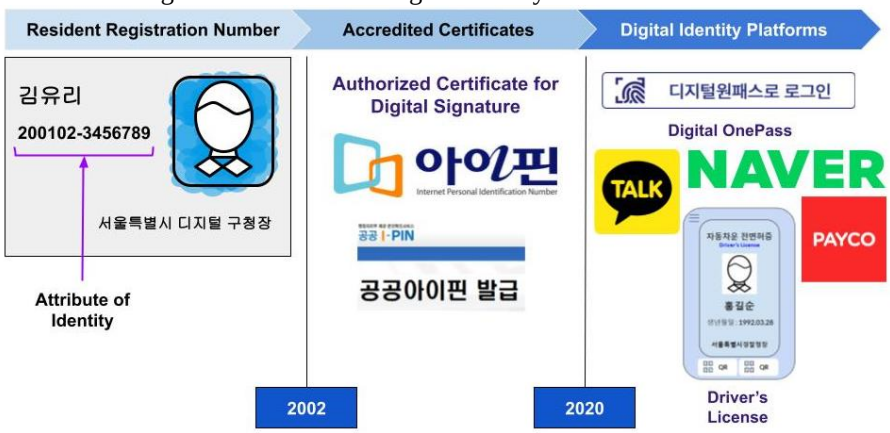
To deal with identification and authentication issues, at the beginning, Korean Government promoted the use of resident registration card, as a credential based on that Koreans can proof their identity, time later, with the adoption of digital technologies, the government promotes internet personal identification numbers (i-Pin), after that Koreans used to use accredited or authorized certificate until 2020, afterwards, and based on the revision of the Digital Signature Act, the use of exclusive accredited certificates was abolished. Nowadays, the Korean digital identity and signature market is more dynamic and competitive.

Moreover, taking advantage of best practices on digital identity management, in 2020 Korea launched a national digital authentication platform, which is called Digital ONEPASS (디지털원패스), aimed to facilitate interactions with the public administration.

Additionally, according to the revision and updating of Promotion of Information and Communications Network Utilization and Information Protection Act, State Public Officials Service Regulations, Road Traffic Act, Electronic Government Act, Korea has prepared of ground to include “social

networks" and "financial applications" as "Identification Providers", and it has undertaken pilot digital identity solutions like mobile public officials ID and mobile driver's licenses. At a first glance, all this would seem to suggest that the Digital Identity Scheme in Korea is being transformed through the application of digital technologies such as mobile devices, public key infrastructure, face recognition and artificial intelligence.

<Figure 1. Overview of Digital Identity evolution in Korea>



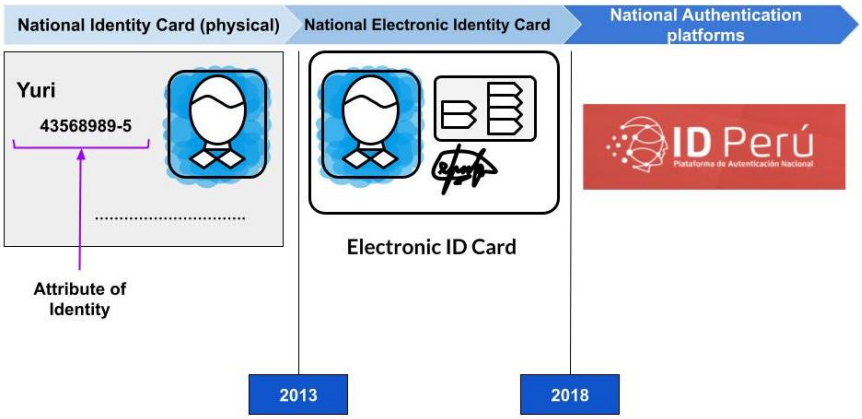
Source: Own development, 2022

In the case of Peru, the identification of the citizens is clearly developed in both the Political Constitution, which was enacted in 1993, and the Law N° 26497, Law of the National Registry of Identification and Civil Status. Under this legal framework, time later, in 1997, official identity documents began to be issued by using computers, which served to process and record citizen information. We started to store Peruvian's information such as names, gender, date of birth, legal physical address, civil status, among others.

From 1997 to 2005, the standard used for cards was the ISO ID-02 format, but from 2005 the format was ISO ID-01 (RENIEC, History of Identity Documents, 2022).

In 2013, with the adoption of cutting-edge technology, the issuance of the National Electronic Identity Card began, it contained a chip with digital certificates for digital authentication and digital signature. Moreover, the chip stores biometric information to perform a Match-on-Card comparison.

<Figure 2. Overview of Digital Identity evolution in Peru>



Source: Own developed, 2022

Moreover, the digital identity and its utilization on dealings with the public sector was promoted by the Governmental Digital Identity Framework set out on the Digital Government Law enacted in 2018, the big challenge now is the implementation of its fundamental components such as digital identity guidelines, digital authentication platform, digital identification services, among others. Summing up, the implementation of a Digital Identity Scheme in Peru is being created through the application of a Governmental Digital Identity Framework and implementation of crosscutting digital platforms. However, one striking point in both countries is that they do not have a full-fledged policy dedicated to digital identity which extends beyond the public sector to include the private sector.

Drawing on the above, this study presents a systematic literature review to explain the digital government and digital identity scheme in Korea and Peru.

To do this, the study applied a study case with Korea, which is one of the most notable cases of successful electronic government implementation worldwide.

This study is anchored academically in two terms "digital identity" and "digital identity scheme", understanding them as “collection of attributes that uniquely differentiate a person in his interaction with digital services”, and “a well-designed and articulated collection of policies, technologies, organizations, and processes in charge of governing the digital identity lifecycle to promote a digital society”, respectively.

This study involved interviews with ICT specialists from Korea and Peru, a total of ten specialists were interviewed. At the first time, the interviews with the specialist provide an overview of the digital identity evolution in Korea and Peru, later, considering the feedback getting from the answers, an in-depth understanding of the digital identity scheme of both countries was generated.

Previous research proves that globally speaking there are different ways to compare the electronic government development amongst countries, nevertheless, there is not much evidence about Digital Identity Schemes comparisons studies, that is why a theoretical comparison is constructed based on the literature review, international organization’s studies, and interviews with ICT specialists.

Moreover, the current research could be added to the pool of research both on digital identity and digital transformation, it can also be helpful for researchers and practitioners alike in Latin American.

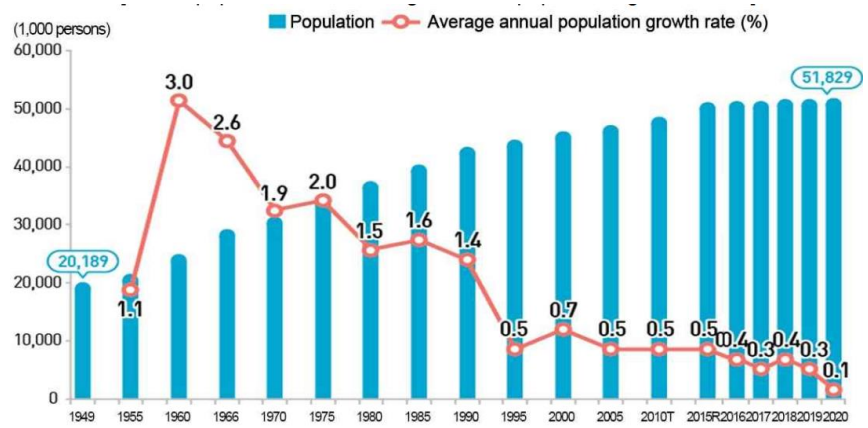
1.2 BACKGROUND OF THE COUNTRIES

This section attempts to outline and explain some overarching features of Korea and Peru from a social and economic perspective. As a matter of fact, for the thesis it is so useful to bear in mind social and economic aspects in Korea and Peru, because they are part of the environment and context in which one country is going to implement digital solutions.

a) Korea

The Republic of South Korea, commonly known as South Korea, Korea or ROK, is a country in Eastern Asia. According to Korean Official Statistics, the population of Korea is about 51.82 million persons and by 2020 the average annual population growth is 0.1% from 2019 (KOSTAT, 2021).

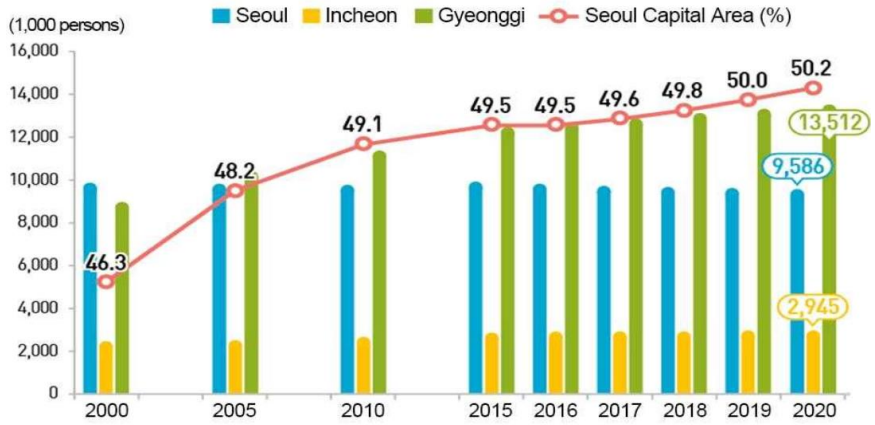
<Figure 3. Total population and average annual population growth>



Source: Korean Statistics (KOSTAT), 2020

Additionally, the population of Seoul Capital area, it means Seoul, Incheon and Gyeonggi, amounted to 26.04 million persons in 2020 (KOSTAT, 2021), accordance with that almost 50.2% of the total population live in the Seoul Capital Area and one-fifth of the Korea's total population lives in Seoul, the capital city (Ko, 2021, p. 113).

<Figure 4. Population in the Seoul Capital Area>



Source: Korean Statistics (KOSTAT), 2020

Generally speaking, in Korea the basic administrative structure is the district "Si (city)", which is part of one province "Do". To date, Korea has eight provinces (Gyeonggi-do, Gangwon-do, Chungcheongnam(south)-do, Chungcheongbuk(north)-do, Jeollanam-do, Jeollabuk-do, Gyeongsangnam-do, Gyeongsangbuk-do), one autonomous province (Jeju-do) and one special city, Seoul (Greater Seoul Metropolitan Area – GSMA) (Im, 2019, p. 22). Seoul in practical terms, it is functioning as the center of administration, politics, and economy.

According to article 3 of the Constitution of Korea, its territory consists of the Korean peninsula and its adjacent islands. Korea is surrounded by so-called big countries such as Japan, China, and Russia and three seas, the West Sea, also known as the Yellow Sea, the East Sea, and the South Sea. Because of its location in the global map, Korea plays a strategic geopolitics role in the global world, the reason why, Korea has been dealing with conflicts and different interests of its neighboring countries (Ko, 2021, pp. 10-11). With shortage of natural resources, and a lot of mountains, and small valleys

(NATGEO, 2022), its economic development doesn't stay related to agriculture and extractive activities.

From a social perspective, Korean society has unique features for instance, it is governed as a one nation with one ethnic group (it is ethnically homogeneous) and it has a single language (Im, 2019, p. 69), however, based on migrant workers and multicultural families, Korea is in the process of moving on to a multicultural society (Ko, 2021, p. 105).

From an economical point of view, the development of Korea is noteworthy, because after Japanese colonialism between 1910-1945 and followed by the Korean War between 1950-1953, the economy of Korea was in dire conditions, Korea was a collapsed country. In that vein, Korean public finances were dependent on government loans and foreign aid, mainly from the United States and other developed countries. Moreover, at the end of the war and after the division of Korea, most of the heavy industrial facilities like chemical plants were in North Korea, as a result the economic recovery was a real challenge by Korea (Dongsung Kong, 2015, pp. 15-19).

As a result, and bearing in mind this context, since 1960 until 1980 the principal objective of the government was creating a sustaining economy as soon as possible, however surrounded by powerful enemies, to survival required becoming economically strong (Kenneth L. Judd, 2000, p. 500), many scholars pointed that in this period of time the idea was follow an export-driven policy and implement an export-oriented economy (export-oriented industrialization), it meant the economic growth was the priority of the government over all the national agenda (Ko, 2021, p. 20), therefore, the economy was prioritized in all policy areas (Im, 2019, p. 69).

The government focused on creating and maintaining a good relationship between public finance and the market-economy, the latter was

achieved by empowering the private companies' autonomy (Dongsung Kong, 2015, pp. 20,24).

Additionally, Korea made an intensive investment on Information and Communications Technology (ITC), enhanced transparency of corporate governance and joined the Free Trade Agreement (FTA).

These were also important decisions for fostering the economic development of Korea (Ko, 2021, p. 22).

Nowadays, Korea maintains its competitiveness in ICT and heavy industries such as shipbuilding, petrochemicals, steel, machinery, non-ferrous metals, and semiconductors, among others, as a result in 1996, Korea joined the OECD, and in 2008 it became part of the Group of Twenty (G-20) Leadership (Dongsung Kong, 2015, p. 13). Without any doubt from an economic perspective Korea is a worldwide striking case of study.

Recently Korea, bearing in mind the challenges of the Four Industrial Revolution (4IR) and recognizing the catalytic role played by the government in support the economy, is attempting new trade tactics to cope with the new future, reason why, in 2020 Korea released the Korea New Deal, its national strategy for the great transformation, it sets out a long term vision to build a vibrant digital, green and safe country, it also establishes an estimated budget, goals, milestones, and projects needed to improve noncontact infrastructure, build smart logistics systems, train digital and green experts, and set the foundation for carbon neutrality in order to overcome the economic crisis caused by COVID-19 and adapt to changes in technology, economic and social structures.

To have a better idea about the economic structure of Korea we see the Table 3 Korean export's structure. As we notice the main economic activities in Korea are related to ICT and thereon.

Table 3. Korean export's structure (%)

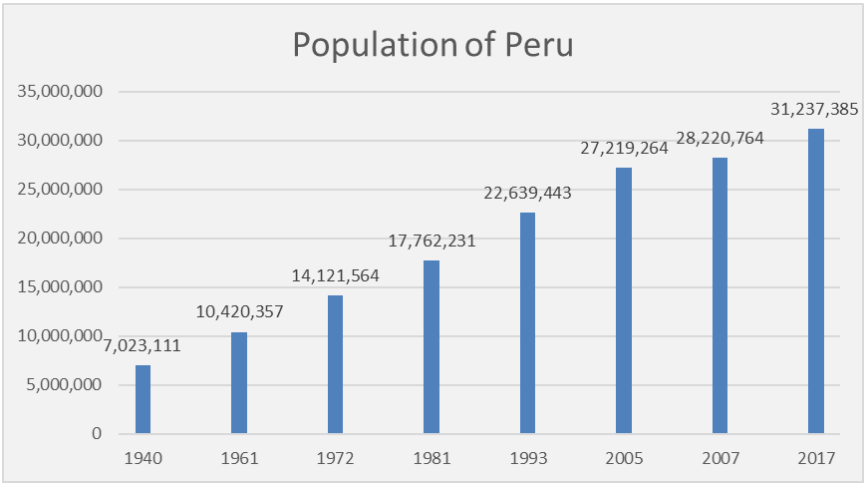
Sector	2018 ($618 Billons)	2019 ($556 Billons)	2020 ($531 Billons)
Integrated circuits	18.7%	15.3%	16.8%
Cars and vehicle parts	9.4%	10.89%	9.95%
Telephones	1.18%	2.12%	2.42%
Refined petroleum	7.22%	7.05%	4.38%
Passenger and cargo ships	2.58%	3.11%	3.26%
Others	60.92%	61.53%	63.19%

<Source: https://oec.world/en/profile/country/kor?deltaTimeSelector1=deltaTime3&subnationalDepthSelector=productHS6&yearSelector1=exportGrowthYear25&yearlyTradeFlowSelector=flow0>

b) Peru

Peru is a country in the center of South America, according to the National Institute of Statistics and Informatics (INEI in Spanish), its current population is about 33 million people, 30% of whom live in the capital, Lima.

<Figure 5. Total population of Peru>



Source: National Institute of Statistics and Informatics, 2017

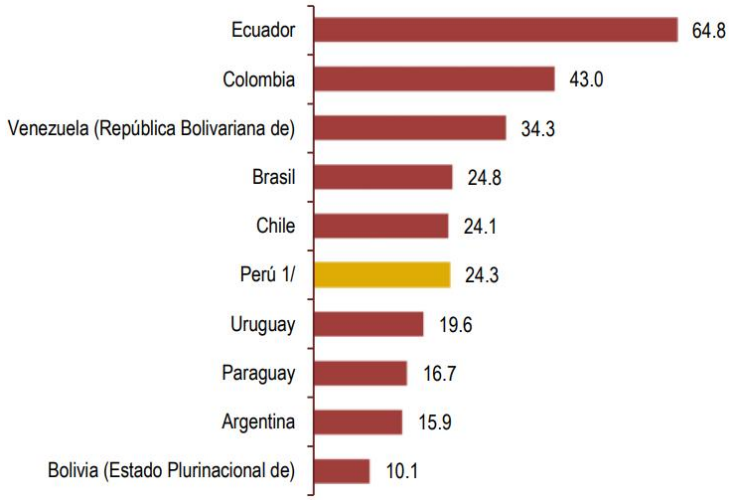
Peru borders to the South with Chile and Bolivia, to the North with Ecuador and Colombia, to the East with Brazil and to the West with the Pacific Ocean. In addition, according to article 189 of the Constitution, the territory is

composed of regions, provinces, and districts. Peru has 25 Regions, also called Regional Governments, and about 195 provinces and 1, 600 districts. A district is part of a province and the basic administrative structure of the State.

Peru has one autonomous province, Constitutional Province of Callao, and one special city, Metropolitan Area Lima. Lima in practical terms, it is functioning as the center of administration, politics, and economy, even when Peru claims that they are in an ongoing decentralization process.

In South America, Peru is the country with the third largest land area (1,285,215.6 km^2) after Brazil and Argentina; however, in terms of density, it ranks sixth (24.3 persons/km^2), with Ecuador and Colombia being the most densely populated countries, with 64.8 persons/km^2 and 43 persons/km^2, respectively (INEI, 2017).

<Figure 6. Population density in South America, 2017>



Source: National Institute of Statistics and Informatics, 2017
< https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1539/libro.pdf>

From an economic standpoint, the cornerstone was the assumption of the presidency of Alberto Fujimori Fujimori in 1990, because a new Constitution was enacted, which implies in economic terms a new economic model following the Washington Consensus, and the spread of a neoliberal

ideology (Lust, 2019). As such, according to its article 58 the private initiative is free, it is exercised on a social market economy, in this context, the role of the state is to guide the development of the country, and acts in the areas of employment promotion, health, education, security, public services, and infrastructure.

The State plays a subsidiary role and intervenes when there are market failures. Thirty-two years have passed, and Peru is an emerging economy, its economic growth depends on export its mineral resources (gold, copper, zinc, silver, iron, among others), basically, Peru provides raw materials for economic development in the advanced capitalist countries such as the global north and China (Lust, 2019).

Other industries are relating to textiles (clothes, garments, yarns, among others) and agribusiness (blueberries, mangoes, cocoa, avocado, and olives) (Malca, 2021, p. 1), however, the contribution of them to the gross domestic product (GDP) is limited.

In this sense, scholars agree that extractive development models do not guarantee lasting and structural progress and make the country vulnerable to recessions. Fundamentally, the Peruvian economy is divided into an economy of private corporations (transnational corporations) and micro-enterprises (Lust, 2019). To have a better idea about the structure of our economy we see the Table 4 Peruvian export's structure in 2020. As we notice the main economic activity is Mining.

Table 4. Peruvian export's structure, 2020 (Million US$)

Sector	2018	2019	2020
Agriculture	5907 (12%)	6333 (13%)	6858 (16%)
Commercial Fishing	3296 (6%)	3542 (7%)	2867 (6%)
Mining	29814 (60%)	29039 (60%)	26372 (62%)

Hydrocarbons	4039 (8%)	2979 (6%)	1352 (3%)
Manufacturing	5822 (11%)	5647 (11%)	4842 (11%)
Others	189 (3%)	154 (3%)	121 (2%)

Source: Central Reserve Bank of Peru, 2020
< https://www.bcrp.gob.pe/eng-docs/Publications/Annual-Reports/2020/annual-report-2020.pdf>

1.3 THEORETICAL BACKGROUND

a) Electronic Government Survey

The UN evaluates and compares the level of progress on electronic government around the world; almost 193 UN member states have been evaluated since 2002. The Department of Economic and Social Affair of the United Nations (UNDESA) had produced the Electronic Government Survey per year until 2005, since 2008, the survey has been done every two years (Kim S. , The Evolution of Korean E-Government in the perspective of Actor-Network Theory, 2014, p. 46).

Table 5. Evolution of EGDI among Peru and Korea

EDGI	**2020**	**2018**	**2016**	**2014**	**2012**	**2010**	**2008**	**2005**	**2004**	**2003**
PER	71	77	81	72	82	63	55	56	53	53
ROK	2	3	3	1	1	1	6	5	5	13

Source: UN, 2020

The Electronic Government Survey aims at providing a base of knowledge and experiences about electronic government policies and initiatives among member states. In other words, decision-makers will be able to learn from successful approaches and pitfalls in other states and guide electronic government policies and strategies in their countries (Kim S. , The

Evolution of Korean E-Government in the perspective of Actor-Network Theory, 2014, p. 46).

To undertake the comparison of different economies, the UN created an e-government development evaluation method based on two (02) indexes: the Electronic Government Development Index (hereinafter EGDI) and the Electronic Participation Index (Chong-sik, 2020, pp. 86-87). In the context of this research, the most relevant index is EGDI, because it assesses and compares the electronic government performance of economies based on three (03) dimensions: a) Online service index, b) Telecommunication infrastructure index and c) Human capital index.

Table 6. Dimensions of Electronic Government Development Index (EGDI)

Dimensions	Components
Online Service Index (OSI)	The topics listed below are just some of the total topics evaluated by UN. • Links to Sustainable Development Goals (SDGs) • Information about gender equity policy • Information about social protection policy • Links and information about e-government strategy • Links and information about electronic participation • Links and information about open data portal • Links and information about e-procurement • Links and information about digital security or cybersecurity • Links and information about digital identity • Others
Telecommunication Infrastructure index (TII)	• Estimated internet users per 100 inhabitants • Number of mobile subscribers per 100 inhabitants • Active mobile-broadband subscription • Number of fixed broadband subscription per 100 inhabitants
Human Capital Index (HCI)	• Adult literacy • Combined primary, secondary and tertiary gross enrolment ratio • Expected years of Schooling • Average years of Schooling

Source: Own development, 2022

Considering the analysis of the three dimensions of EDGI, we identify that there are core elements used to compare the digital government

development among UN members, they are a) institutional arrangements, b) leadership and policy, c) ICT infrastructure, and d) legal framework.

b) Digital Government Index (DGI)

The Digital Government Index (hereinafter DGI), made by OECD, measures the maturity level of digital government in OECD members and partner countries. DGI becomes a tool to support policy decisions that could be used for benchmarking progress of digital government across OECD members. As a result, a striking base of knowledge of best practices, common challenges, and technological trends can be shared and maintained.

In this regard, DGI is based on six (06) dimensions, which derive from OECD Recommendations on Digital Government Strategies and the Digital Government Policy Framework issued in 2020 (both are briefly explained in item 4.2 of Conceptual Framework). The dimensions of DGI are a) digital by design, b) data-driven public sector, c) government as a platform, d) open by default, e) user-driven and f) proactiveness. As we see in the <Table 7. Aspects evaluated by Digital Government Index (DGI)>, DGI evaluates aspects related to institutional arrangements, leadership, ICT infrastructure and legal framework (OECD, Digital Government Index, 2019)

Table 7. Aspects evaluated by Digital Government Index (DGI)

Aspects evaluated	Components
Institutional arrangements	• Governmental body in charge of leading and coordinating decisions on digital government, governing ICT projects and coordinating the public sector data policy,
Leadership and Policy	• National digital government policy • Public data policy (public sector data policy) • Information security policy • Action plan for open government
ICT Infrastructure	• Enterprise architecture for the government • Interoperability platform • Digital identity system or Digital Identity Platform • Data center for the government • Public Information Sharing Systems • Open data portal
Legal framework	• Principles, standards, framework, guidelines, or rules developed or adopted for ethical use of data, personal data protection,

	design of digital services, data management, digital identity, interoperability, • Digital Signature Act, Digital Identity Act, Cybersecurity Act, Digital Inclusion Act, Interoperability Act, e-procurement Act, Digital Inclusion, Explicit requirements for public sector to share data with other public organizations, exert a ethical use of data,

Source: Own development based on DGI

Considering the analysis of the six (06) dimensions of DGI we identify core components used to compare the digital government development in OECD members are a) institutional arrangements, b) leadership and policy, c) ICT infrastructure, and d) legal framework.

c) Key factors of Korean Electronic Government Success

Definitely the electronic government development in Korea is a striking and remarkable case of study, in that sense, some researchers assert that the key factors in implementing Korean electronic government are fundamentally law, standards, and rely systems (Kim S. , The Evolution of Korean E-Government in the perspective of Actor-Network Theory, 2014, p. 50). Others point out that we need to consider aspects like the high rate of the internet and the degree of coverage of broadband population (Sadigova, 2014, p. 3).

Some assert that the success factors of Korea e-government are a) strong leadership, b) vision and strategy, c) strong management, c) stable budget and resource allocation, d) improvement and alignment of legislation and e) national information infrastructure. Other researchers point out that aspects like a) politics, leadership and ICT governance, b) technical and institutional, and c) cooperation and technical assistance are essential components of successful deployment of electronic government in Korea (Chong-sik, 2020, pp. 175-224).

In the same line, MOIS and NIA highlight that digital government policy, leadership, legal framework, digital government infrastructure are the essential elements of the notable digital transformation of Korea.

Table 8. Key factors of Korean Electronic Government Succeed

Key factor of success	Description
Leadership	Ministry of Interior and Safety (MOIS)
Institutional arrangements	Ministry of Interior and Safety (MOIS) Ministry of Science and ICT (MSIT) National Information Society Agency (NIA) Korea Local Information Research & Development Institute (KLID) Korea Internet & Security Agency (KISA) Korea International Cooperation Agency (KOICA)
Legal framework (Law, policy, Enforcement Decrees)	Resident Registration Act (RRA) Electronic Government Act (E-government Act)
ICT Infrastructure	Public Information Sharing System (하나로민원) Resident Registration System (RRS) Government24 (정부 24) Digital One Pass (디지털원패스) Open Cloud Platform (PAAS-TA)
Budget	ICT Promotion Fund ($ 1 billion per year) • Information Communication Infrastructure • Information and communication research and development • E-government projects

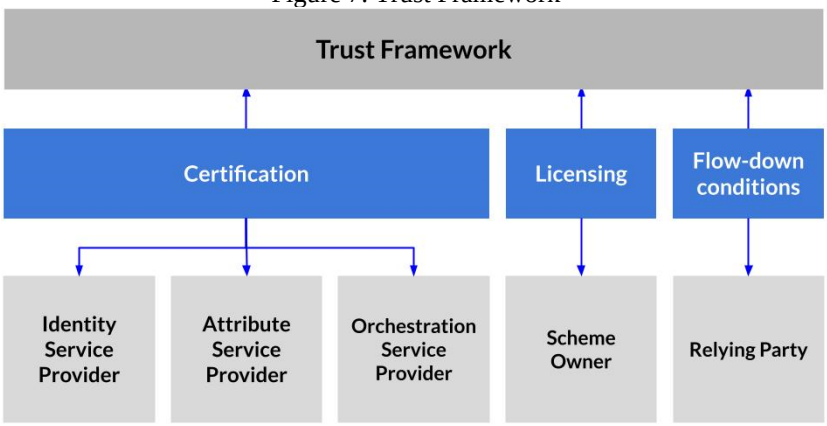
Source: Own development, 2022

d) United Kingdom Digital Identity and attributes trust framework

UK digital identity and attributes trust framework is a set of business rules, open technical standards, and guidelines for creating and maintaining a Digital Identity Scheme. Consequently, under this framework any organization that wants to be a secure and trustworthy identity service provider or attribute service provider needs to prove that they comply with a set of rules and technical standards, if they meet and follow them, they will get a certificate as a trust service provider.

As a result, other members or participants can trust or feel more confident about accuracy and integrity of the services provided by them, because they proved that they are able to safely manage digital identity's attributes and follow technical standards (DCMS, 2022). Under this framework any organization needs to perform one of the following roles a) identity service provider, b) attribute service provider, c) orchestration service provider, d) relying party and e) scheme owner.

<Figure 7. Trust Framework>



Source: <https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/uk-digital-identity-and-attributes-trust-framework-alpha-version-2 >

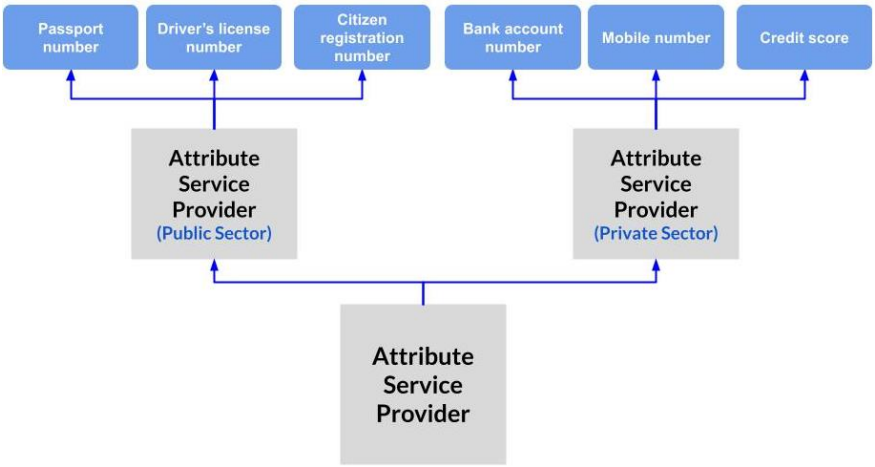
To understand the roles in the Digital Identity Framework, it is preferable to mention a briefly abstract of them:

a) Identity Service Providers (ISP), they are responsible for verifying user's identities. An identity service provider can be a public entity or private organization. They need the authorization of users (user's agreement) to share their digital identity with relying parties. In some OECD studies an identity provider is responsible for carrying out the registration of individuals, for establishing their identity and for issuing

credentials (OECD, Digital Identity Management, Enabling Innovation and Trust in the Internet Economy, 2011, p. 12).

b) Attribute Service Providers (ASP), their main activities are collecting, assessing, and sharing pieces of information that characterized one user. An attribute service provider can share their attributes with Identity Service Providers or relying parties.

<Figure 8. Attribute Service Provider>



Source: <https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/uk-digital-identity-and-attributes-trust-framework-alpha-version-2 >

c) Orchestration Service Providers (OSP), they are accountable for ensuring a safe exchange of information across ISP, ASP, and RP.

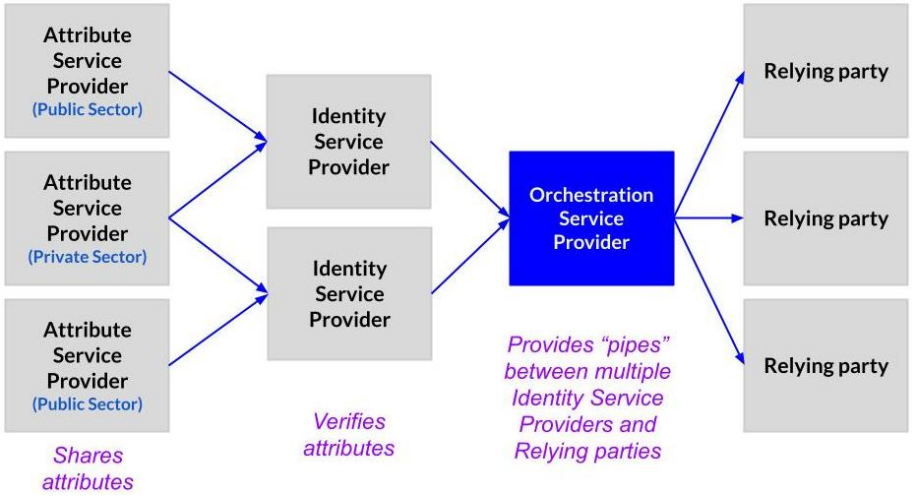
d) Relying parties (RP), fundamentally they are consumers of services provided by ISP, ASP or OSP.

e) Scheme owner (SO), whose functions are creating, leading, and overseeing a digital identity scheme, a digital identity scheme includes roles, specifications, and processes to participants' enrollment in the scheme and dispute resolution.

The specifications for creating and assessing identity and attribute service providers requires to meet rules to either strengthen information

security (confidentiality, integrity, and availability), prevent privacy leakage, fight against fraud, manage risks and information security incidents, improve data management, promote accessibility and inclusiveness, enhance record management and interoperability, and promote transparency of the services.

<Figure 9. Coordination among ASP, ISP, OSP and RP>



Source: <https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/uk-digital-identity-and-attributes-trust-framework-alpha-version-2 >

As such, UK Digital Identity and attributes trust framework provides a clear overview about the components of a digital identity scheme.

e) The Digital Identity Management and its impact on the digital economy

The Digital Identity Management and its impact on the digital economy, it is a study made by Inter-American Development Bank (hereinafter IADB), which analyzes the Digital Identity Schemes in Spain and Estonia with the purpose of identifying advantages, best practices and learned lessons of both implementations. It should be noted that, according to the Electronic Government Survey, which evaluates the development of electronic government worldwide, Estonia is ranked 3rd worldwide, while Spain is in

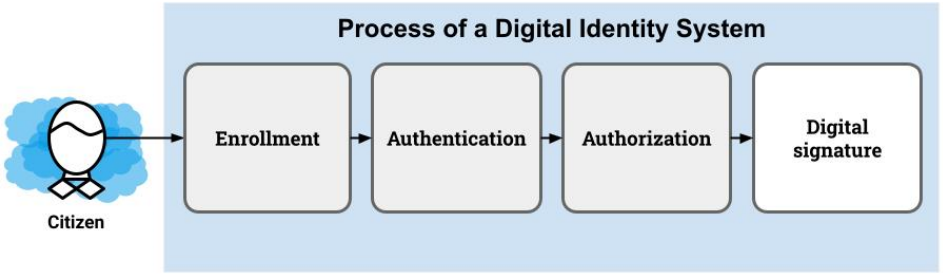
position 17th (UN, E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development, 2020, p. 318), so we are talking about ones of the most digital government advanced countries worldwide.

First, the study posits that digital identity is a cornerstone for generating trust in the digital environment, however the development and implementation of a Digital Identity Scheme must take into account the national context, including history, culture, political style, demographics, and digital government development of the country. In this line, for the public and private sector, the main triggers for its implementation have definitely been the increasing number of digital transactions and regulatory requirements, especially those related to risk management, fraud management and information security (IDB, Identidad Digital y su Impacto en la Economía Digital, 2017, pp. 3-12).

Whether we like it or not our digital identity is increasingly embedded in everything we do in our lives (WEF, Identity in the Digital World a new chapter in the social contract, 2018, p. 9).

Drawing on the above, we can understand a Digital Identity Scheme as a set of articulated organizations, processes, technology, and regulation with the aim of managing the lifecycle of the attributes of a person's identity. In this vein, the main processes of a Digital Identity Scheme are a) Registration in a Digital Identity System (Enrollment), b) Authentication, c) Authorization and d) Digital Signature.

<Figure 10. Main processes of a Digital Identity Scheme>



Source: Own developed, 2022

To have a better understanding about these processes, each of them are briefly summarized below:

1. Enrollment or registration, basically it is the creation of the user in the identification registry (information system or digital platform) and the corresponding assignment of an authentication credential (digital identity credential).
2. Authentication, group of activities with the purpose of verifying if the person is who they say they are. Fundamentally, the authentication process is based on three (03) factors, they are:
    a. Something the person knows, for example, a password.
    b. Something the person is, for example face, iris, or voice biometrics.
    c. Something the person has, for example, a credit card or digital certificate
3. Authorization, a process that consists of verifying whether you have the privileges to access certain resources.
4. Digital Signature, a mechanism that ensures the integrity of a document and the authorship of the signature. The digital signature is done through digital certificates.

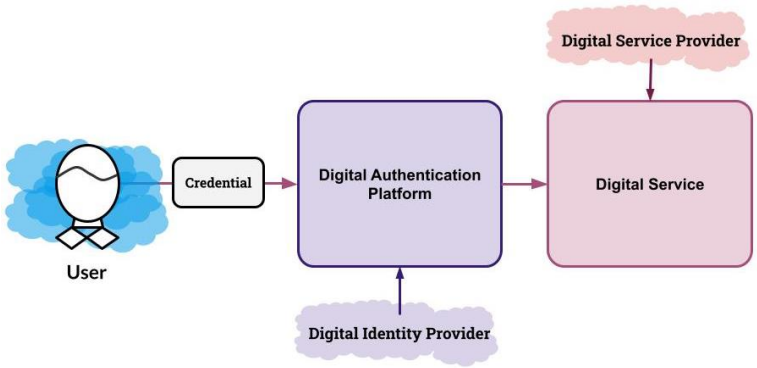
In the light of the above mentioned, the main roles of the Digital Identity Scheme are a) users, b) digital identity providers and c) digital services providers, each of them is summarized below:

a) Users, natural persons that need an identity, aim at performing transactions with the public and private sector.
b) Digital identity providers collect, store and preserve digital identity attributes of users. They are accountable for maintaining

the security, accuracy, and trustworthiness of digital identity attributes.

c) Digital service providers, basically public and private organizations, who are supported by digital identity providers to design, develop and render digital services aim at meeting user's needs.

<Figure 11. Roles of the Digital Identity Scheme>



Source: Own developed, 2022

Moreover, by analyzing the study, we observe that the comparison between Estonia and Spain was undertaken based on essential elements such as governance, institutional arrangements, legal framework, and technology.

Table 9. Elements evaluated on the comparison between Estonia and Spain

Elements evaluated
General Overview
1 What are the main triggers for the implementation of a Digital Identity Scheme?
a) To enhance the cybersecurity (digital security) of digital services
b) To strengthen user's trust and confident on digital environment
c) To promote the electronic commerce
d) To comply with digital regulation
2 When you carry out online transactions with the public sector, what kind of credentials can you use to proof your identity?
a) Electronic Identity Card (ID Card), Personal Identity Card or Resident Registration Card
b) Digital Certificates
c) User and Password
3 What are the essential components of the Digital Identity Scheme?
a) Digital Identity Regulation
b) Safety, interoperable and scalable ICT Infrastructure

	c) Collaboration between public and private sector
	d) Campaigns or programs to strengthen digital skills of the citizens and stakeholders
Governance	
4	Who governmental entity is accountable for issuing digital identity credential such as personal identity cards, digital certificates?
5	Who governmental entity is accountable for promoting and coordinating the deployment of digital identity scheme at national level, it means in public and private sector at national level?
6	Who is accountable for maintaining the digital identity information system or registry?
7	What is the role of the private sector in the Digital Identity Scheme?
	a) Manufacture and customization of an either national identity card, personal identity card or electronic identity card
	b) Provide software to use either a national identity card, electronic identity card or digital certificates
	c) Provide technical support and training to users and business that use either national identity card or electronic identity card
Technology or digital platforms	
8	Is there a national platform to carry out a digital signature?
9	Is there a national identity information system or registry?
10	Is there a national digital authentication platform?
11	What kind of Digital Identity Scheme have your country implemented?
	a) Account-oriented interactions
	b) PKI-oriented interactions
	c) Blockchain-oriented interactions
12	Does your national identity card include biometric information?
13	Is there a one single point of contact (national e-services portal) with the citizens?
14	What can I do with my National Identity Card?
	a) Face-to-face authentication (offline)
	b) Digital authentication (online)
	c) Digitally sign documents
Regulation (Legal framework)	
15	Is there a Personal Information Code?
16	Is there a Data Privacy Law?
17	Is there an Electronic Administration Law?
18	Is there a Digital Government Law?
19	Is there a Digital Signature Law?
20	From what age is it mandatory to have a national identity card or electronic identity card?

Source: Own development, 2022

Drawing on the above, the learning lessons from Digital Identity Scheme implementation of Estonia and Spain are:

a) A clear understanding about the different objectives of digital signature and digital identity allows leveraging of their potential, one is related to the manifestation of will, and the other one is related to the identification and authentication of persons.
b) To have a legal framework to prepare the ground for supporting the validity of digital identity cards or mobile ID will enhance electronic transactions and enable the implementation of digital government projects or initiatives and reduce resistance to change.
c) To promote the adoption of technical standards such as OpenID Connect, ISO/IEC 29115, SAML 2.0, OAUTH 2.0, among others, ensure interoperability and a common language among stakeholders.
d) To find a balance between security and usability allows to improve the user experience.
e) To establish a financial model to make a sustainable solution.
f) To become aware of the importance of cross-border digital identity, because in a global economy the human and goods mobility requires a new framework to verify the identity of persons and things.

1.4 PURPOSE OF THE RESEARCH

a) Purpose of Research

Along with the rise of digital services, we see that fraud, data misuse, data leakage and identity theft are not restricted to the physical world, they exist on digital environment either, most of these problems in the digital world are due to proofs of digital identity are simple account-oriented interactions (user and passwords), that is how internet growing up, nonetheless, we need to find cutting-edge solutions to harness the potential of digital identity as part of

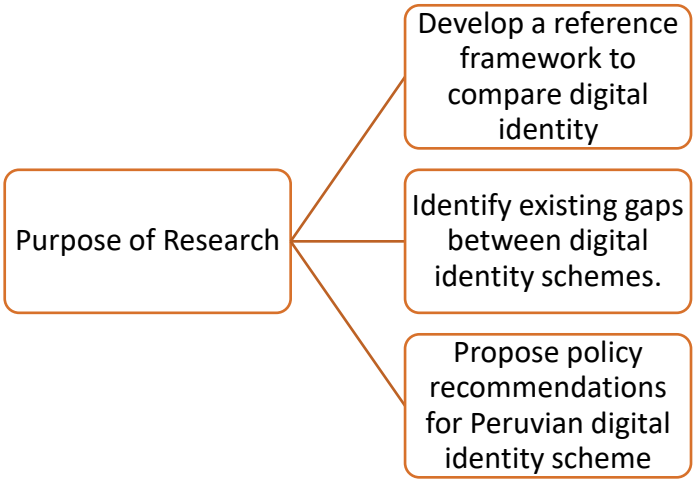
recovery strategies from COVID-19 pandemic, strengthen digital trust and gradually migrate to a human-oriented digital transformation approach.

As we have seen, a good Digital Identity Scheme brings benefits like saving money and time of the citizens, increasing resilience to cope with new shocks, reducing significant risks of identity fraud and misuse of personal data, encouraging digital innovation, and creating digital services by allowing to re-use digital authentication components, improving user experience, and complying with regulation (GOV.UK, 2022). That is why, Korea and Peru have been implementing a Digital Identity Scheme, trying to leverage those benefits.

In that vein, this research, firstly, seeks to fill the lack of a reference framework to compare Digital Identity Schemes, to achieve that we are going to consider international standards, best practices, and previous studies on Digital Identity Schemes worldwide.

Secondly, being aware that the level of digitization in Korea is higher than Peru, the comparison strategy will focus on identifying the existing gaps between both schemes from a comprehensive perspective, it means, as a researcher, the Digital Identity Scheme will be addressed as a system, a set of actors, processes, rules, and components interacting among them, sharing data and information to both improve digital identify management of individuals and strengthen citizen's trust in the digital environment.

<Figure 12. Purpose of research>



Source: Own developed, 2022

Finally, I will propose public policy recommendations aimed at improving Peruvian Digital Identity Scheme development based on the results of the comparison. The recommendations need to consider the effects on the interaction between market and government, likewise, attending the major risks on digital identity such as unconscious bias, privacy breaches and discrimination (Ayed, 2011, pp. 4-5)

b) Research questions

In this line, recognizing the remarkable economic-social development of Korea, and its striking digital government progress, the research question will focus on identifying How Korea is governing its Digital Identity Scheme to strengthen sustainability, accuracy, inclusiveness, security, and usability of a person's digital identity?

Therefore, considering the properties of a convenient, safety and trustworthy Digital Identity Scheme and their different components, this research is going to focus on the comparison of the following areas: digital identity legal framework, digital identity technology (cross-border platforms)

ICT budget and ICT market. Consequently, the questions that are answered at the end of the thesis are:

1. How does the digital identity legal framework provide sustainability, inclusiveness, security, and usability of digital identity of persons?
2. How does the digital identity technology provide sustainability, accuracy, inclusiveness, security, and usability of digital identity of persons?
3. How does digital identity governance provide sustainability, accuracy, inclusiveness, security, and usability of digital identity of persons?
4. How to explain the different levels of performance of Digital Identity Scheme in Korea and Peru?
5. How can I improve the Digital Identity Scheme in Peru according to Korean experience?

The comparison will be made from the policy perspective considering accuracy, inclusiveness, security, and usability as main criteria.

c) Research objectives

Based on the research purpose and research questions, the follow research objectives were set up:

- Establish and validate a framework to compare digital identity schemes.
- Identify gaps between digital identity regulation, technology and governance between Korea and Peru from the policy perspective considering accuracy, inclusiveness, security, and usability as main criteria.
- Determine policy recommendations for Peruvian digital identity scheme

CHAPTER 2. KEY CONCEPTS AND FRAMEWORK

This section aims to have a comprehensive point of view about the literature and concepts about digital government and digital identity, to have a deeper understanding of the essential role of digital identity scheme for developing a digital society while enhancing security, privacy, and digital trust on cyberspace (digital environment).

Various academic thoughts are presented to compare differences in academia and the evolution of the concept. In addition, it introduces the theoretical framework that will be used for making a comparison between the digital identity scheme in Korea and Peru.

Therefore, before explaining what a digital identity scheme is and why it is a fundamental element for the further development of the digital society, we are going to attempt to clarify the main concepts and definitions related to digital government and digital identity that guide us during the comparison study.

Additionally, I have to say that surfing among different points of view, technical documents, notes, and literature was an enriching personal experience to have a deeper understanding of the huge potential of digital identity to transform our societies.

2.1 Identity

To understand what we mean by digital identity, first we need to define identity. In the physical world the identity is not created by us, it is given to us, our parents will initiate the identity life cycle, when they give us our names, then hospital and government verify you are alive and then they issue an

identity certificate, most of the time called birth certificate, then during the time and based on different events of life (finish studies, get job, get married, retired and died) more and more credentials are issued (national identity card, driver license, passport, among others) by institutions and organizations and added to our initial trustable credential (DID Alliance Korea, 2020).

As we can see, from this perspective, in the physical world, our identity, at the beginning, is something provided to us by a group of trustable actors coming together (parents, hospital, and government).

As we can see, in the physical world the identity authentication is based on physical credentials such as passport, driver license, national identity card, among others (IDB, Identidad Digital y su Impacto en la Economía Digital, 2017, p. 7).

Others pointed out that identity, in a general point of view, entails that a person can be identified and recognized during all its life, its features and characteristics used by the identification can change over the time or can be changed by the person (IDB, Identidad Digital y su Impacto en la Economía Digital, 2017, p. 6).

Some others assert that digital identity is seen as an intersection of identity and technology in the digital age (Ayed, 2011, p. 1). Now, from a linguistic point of view, according to the dictionary of Cambridge University, identity is "who someone is" or "the things that make one person or group of people different from others". Likewise, the dictionary of the Royal Spanish Academy (RAE) asserts that identity is a collection of features of an individual or a community that characterize them compared to others.

Complementing those definitions, from a philosophical perspective our identity is molded and affected by our context, experiences, social relationships, culture, habits, practices, among others (Springer, 2008). Historically, the

identification of natural persons has always been a task carried out by states for a host of reasons to do with control of the population, taxation, movement (human migration), voting, providing convenient public services, dealing with administrative affairs, and other functions (Springer, 2008).

From a politic and global governance perspective, under the Sustainable Development Goals (SDG), in specific, according to its objective 16, by 2030, our governments will endeavor to provide legal identity for all their citizens, including birth registration, so it entails that identity is a global issue and our governments must strengthen their effort to implement a solution in order to provide a reliable credential to all their citizens such as national identification card, birth certificate, ID Card, or resident registration card and so on, without any doubt in a digital era this solution requires a digital identity system to storage, process and distribute the huge amount of data and information that will be generated.

In the same line, the Inter-American Development Bank (IDB) pointed out that the identity of a person, organization, thing, or process is everything that characterizes it. In an individual, identity ranges from physical characteristics, gender, biometric information, or experiences, to belongings, diplomas, or properties (IDB, Identidad Digital Autogestionada, 2020, p. 8). Similarly, for the World Economic Forum (WEF) our identity is literally who we are, that is, a combination of history, innate aspects, beliefs, and things we learn, identity is the result of our cultural, family, national, gender identity, etc. (WEF, Identity in the Digital World a new chapter in the social contract, 2018, p. 9).

From a legal standpoint, identity is the right to be recognized as a human being and citizen of one community or country, in this respect, most of the countries have enacted a comprehensive regulatory framework, which

encompass different kind of legal instruments such as specific articles in the Constitution, specific laws, enforcement decrees (Presidential Decrees or Supreme Decrees), or enforcement rules or regulations (Ministerial Decrees).

From a technological point of view, an identity can be defined as a collection of personal attributes, which can be used to define an identity, for instance forename, surname, date of birth (Bouzefane, 2015, p. 47). In this line, the International Telecommunications Union (ITU) refers to identity as the representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context (ITU, Digital Identity Road Map, 2018, p. 16).

Some ICT specialists from the DID Alliance, open industry association established for Decentralized Identity, claim that identity is the way to express the unique characteristics whether it is a human being or an object (DID Alliance Korea, 2020). In the case of The Department for Digital, Culture, Media & Sport from the UK, we can consider the identity as a digital representation of a person acting as an individual or as a representative of an organization (DCMS, 2022).

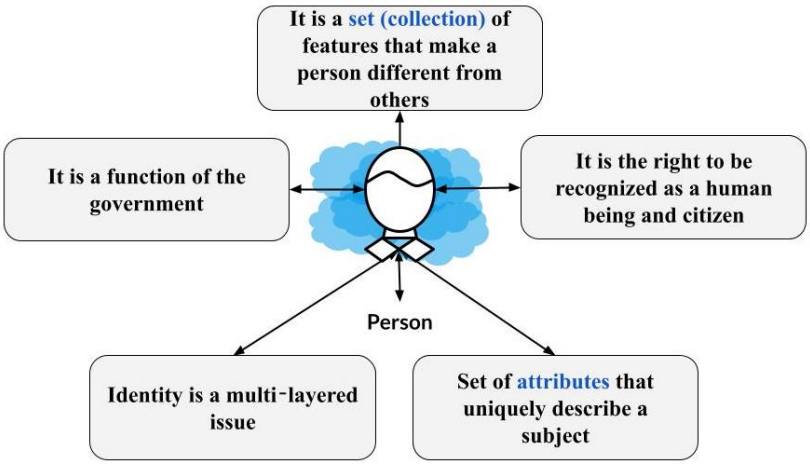
In line with the above, the standard ISO/IEC 24760-1 refers to identity as "*the set of attributes related to an entity*" (ISO, 2019). Under the ISO, when they refer to an entity, it is not necessarily a person, this can be a group of people (organization) or any device that can carry out a transaction. In this sense, it is important to mention the work made by the National Institute of Standards and Technology (NIST) in its Special Publication 800-63-3 Digital Identity Guidelines, which pointed out that "*identity is an attribute or set of attributes that uniquely describe a subject within a given context*".

As we can see, the scholarly work about identity is vast, there are many definitions of what identity is, based on them we can infer that identity is a

multi-layered field which encompass political, human, social and technological aspects.

Additionally, drawing on the above, under this research we can understand the identity as a set of attributes of one person that uniquely describe it within a particular domain. <Figure 13> shows us a brief overview about the main concepts of identity and gives us an idea about the different fields involved in its development.

<Figure 13. Identity concepts>



Source: Own development, 2022

2.2 Digital Government

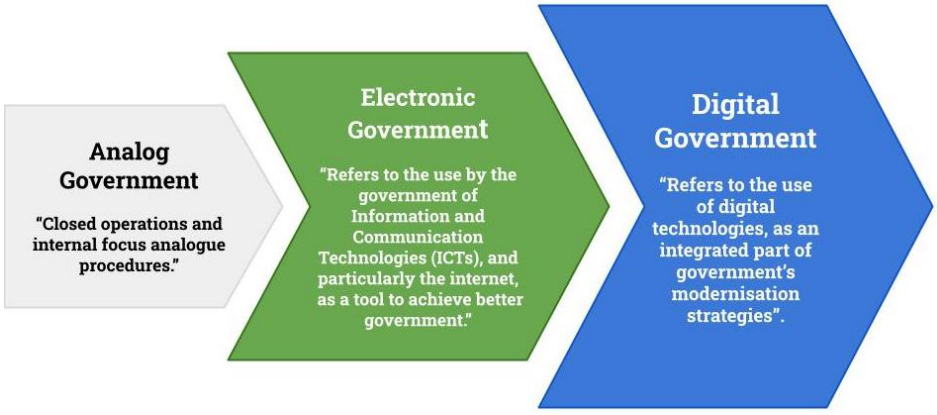
Due to the globalization, and changes in government ideology, public administration, technology, and citizen's needs and preferences, the traditional concept of electronic government (e-gov), which was popular during the 90's around the world, had evolved to digital government, seeking a renovate approach to meet citizen's needs (agility, security, privacy) through the provision of digital services based on strategic use of digital technologies and data.

To achieve that nationwide we need an ecosystem integrated by the public sector, enterprises, technology community and academia working and

interacting among them to create value and cutting-edge solutions. This new ecosystem, namely the digital ecosystem, could be led by the government through Digital Transformation Agency, Digital Government Secretariat, Ministry of Information and Technology, among others, in close coordination with different stakeholders or could be led by another kind of mechanism such as multi stakeholder committee (public and private sector).

Additionally, when we refer to digital government, we must highlight its unrelenting focus on a radical and disruptive transformation of the business model of the government, its policies, and public services based on the capabilities of digital technologies and data to promote the development of the society. In this context, the Organization for Economic Cooperation and Development (OECD) points out that digital government is the use of digital technologies, as an integrated part of government´s modernization strategies, to create public value. It relies on a digital government ecosystem comprised of government actors, non-governmental organizations, businesses, citizen's associations, and individual which supports the production of and access to data, services, and content through interactions with the government (OECD, Recommendation of the Council on Digital Government Strategies, 2014, p. 6).

<Figure 14. Evolution of Electronic Government to Digital Government>



Source: OECD adapted, 2022

Furthermore, the OECD, as part of its mission, has published different kinds of surveys and recommendations for the development and implementation of digital government strategies for its member economies. As shown in <Table 10>, the recommendations are focused on two (02) areas, one of them is the developing a digital government strategy, while the other one is related to implementing it.

Table 10. Recommendation on digital government strategies

1. Recommendations in developing and implementing digital government strategy	
1.1	Ensure greater transparency, openness and inclusiveness of government processes and operations.
1.2	Encourage engagement and participation of public, private, and civil society stakeholders in policy making and public services design and delivery.
1.3	Create a data-driven culture in the public sector.
1.4	Reflect a risk management approach to addressing digital security and privacy issues and include the adoption of effective and appropriate security measures.
2. Recommendations in developing digital government strategy	
2.1	Secure leadership and political commitment to the strategy.
2.2	Ensure coherent use of digital technologies across policy areas and levels of government.
2.3	Establish effective organizational and governance frameworks to coordinate the implementation of the digital strategy within and across levels of government.
2.4	Strengthen international co-operation with other governments.
3. **Recommendations in implementing digital government strategy**	
3.1	Develop clear business cases to sustain the funding and focused implementation of digital technologies projects
3.2	Reinforce institutional capacities to manage and monitor project's implementation.
3.3	Procure digital technologies based on assessment of existing assets.
3.4	Ensure that general and sector-specific legal and regulatory framework allow digital opportunities to be seized.

Source: Adapted from OECD, 2022

Drawing on the above, for developing a digital government strategy, the leadership, political commitment and having a governance framework to organize the participation of public, private, academy, and civil society are essential elements of its success. On the other hand, for implementing a digital government strategy, the proper funding of the initiative, project management and the regulation play a key role in its achievement. Additionally, based on adoption of the recommendations, the OECD has identified a series of essential features in the successful deployment of digital government, which have been integrated as a part of the Reference Framework for Digital Government Policy.

As shown in <Table 11> the Digital Government Policy Framework includes six foundational (06) dimensions 1) Digital by design, 2) Data-driven public sector, 3) Government as a platform, 4) Open by default, 5) User-driven and 6) Proactiveness. It demonstrates that the deployment of digital government is not a technical issue (technology), it is a domain that requires political intervention and, necessarily, articulation with the various actors of the digital ecosystem (public sector, private sector, academy, and citizens) aiming to establish a comprehensive and systemic vision of the services, processes, regulation, and institutions that can meet citizen needs in agile, responsive, and proactive way.

Table 11. OECD Digital Government Policy Framework

1. Digital by design
Digital by default implies to design services to be provided through digital channels since the beginning taking advantage of the potentialities of data and digital technologies, As a result, the business model of the government and its structure, process, channels (face-to-face service center, mobile, or web page), roles (Chief Information Officer – CIO and Chief Data Office - CDO) and business rules must be transformed seeking to enhance its efficiency and performance of doing so. Therefore, beyond a technical topic, digital by default is a strategic and cutting-edge approach to create and provide public services via digital channels. This dimension can be evaluated as follows: • Is there a National Digital Government Strategy or similar policy document? • Is there a governmental agency in charge of leading and coordinating decisions on digital government? What is its level of coordination and taking decisions on ICT projects? Is there a specific regulation on digital government? Is there a technological architecture? Is there an interoperability framework? Is there a digital identity system? • Are there measures of financial benefits of ICT projects? Do the ICT projects consider digital divide issues, for instance digital connectivity or digital skills?
2. Data-driven public sector
The data is recognized as a strategic asset for designing and maintaining high level of public services, because of that governments are implementing strategies, plans, digital platforms, and roles (Chief Data Officer) to promote the interoperability, data analytic and open data initiatives, but at the same time ensure an ethical and reasonable use of it. This dimension can be evaluated as follows: • Are there rules or ethical principles for trustworthy and safe reuse of data. • Does the government manage the data as a strategic asset? • Does the government use the data to shape policies and services? • Is there a public data policy? • Is there a governmental agency in charge of coordinating the implementation of the public data policy? Are there dedicated leadership roles for data policies (Chief Data Officers)?Is there a data inventory? Is there a risk management framework or policy? • Is there an information security policy?
3. Government as a platform
Government plays the role of a platform for meeting the needs of users and creating new digital services or business opportunities by exchanging data and information to private sector and entrepreneurs. The government envisions the data and information as key elements of digitalization of burden activities on any value chain in every sector. The

government implement platforms focusing on the accurate, availability, interoperability, quality, and security of the data and information. The centralization and availability of resources for the whole-of-government eases access and facilitates understanding and the coherence of digital and data solutions across public agencies. Currently, one way that governments are dealing with that is providing application programming interfaces (API), which helps to enhance the interoperability and collaboration among public and private sector. As a result, we create an ecosystem when different stakeholders can collaborate, share knowledge, create digital services, and leverage of the digital technologies potential. This dimension can be evaluated as follows:

- Is there an interoperability platform?
- Is there a data center or cloud services for the government?
- Is there guidelines and standards to ensure the interoperability?
- Do the government use a centralized approach to provide infrastructure, platform, and software to the whole government?

4. Open by default

A government is open by default when it makes government data and policy-making available to the public, within the limits of existing legislation and in balance with the national and public interest. This dimension can be evaluated as follows:

- Is there an open government data action plan, policy, or guidelines?
- Is there an open government portal? Is the data provided over the open data portal understandable by persona and readable by machine?
- Does the provision of open data use any kind of open license?

5. User-driven

The digital services are designed around real user needs rather than business needs, in doing so, the government undertakes new ways to understand the wider user needs, its requirements and context (environment). As a result, the government have a better notion about the user experience, and can design processes, services, and policies to meet the citizens demands. User-driven is challenging to the governments in designing and implementing services around user experience, and, at the same time, be ensured to provide seamless experience over the different type of user's devices. In addition, user-driven design is based on research but not often practiced in government (World Bank, 2016). This dimension can be evaluated as follows:

- Does the government use a digital platform to oversee and foresee the people's needs and demands?
- Is there an action plan to reduce the digital divide or plans to increase the digital skills?
- Is there a process of monitoring and evaluating the digital policies?
- Is there guidelines or indicators to measure the user satisfaction with digital government services?
- Designing and implementing of services is based on research or user experience?
- Are the functions and experience of digital services same in different type of devices?

6. Proactiveness

The government based on the previous dimensions design, implement, and provide services around citizen needs, preferences, circumstances, and location. The government has the tools to anticipate and address citizen's issues a proactive approach. Coordinating across agencies at national, regional, and local (municipal) level exchange information and knowledge to find what they need to perform their duties. This dimension can be evaluated as follows:

- Is it possible to communicate policies, strategies, and initiatives across multiple channels to inform citizens?
- Is there training on the use of digital tools to communicate with the people?

Source: Adapted from Reference Framework for Digital Government Policy and Digital Government Index 2019

Another important reference in the field of digital government is Gartner's report, who defines digital government as a government designed and operated to leverage digital data and thus optimize, transform, and create public services (World Bank, 2016, p. 7). Consistent with this, Gartner set a digital maturity model which has five (05) levels, seeking to guide and provide a tool that allows organizations to evaluate and make strategic decisions to improve their level of digitization according to their objectives and capabilities.

As shown in <Table 12>, Gartner asserts that deployment of digital government can be approached as a process that begins with the enablement of online services (e-government), but as we take advantage of managing the data and incorporate collaborative work practices amongst entities and various stakeholders of the ecosystem, we will improve our levels of digital maturity and, above all, we will develop the ability to create cutting-edge (innovative), agile and proactive solutions to meet the needs of citizens, what Gartner calls smart government.

Table 12. Five (05) levels of digital government maturity

Initial (E-government)	**Developing (Open)**	**Defined (Data centric)**	**Managed (Fully digital)**	**Optimizing (Smart)**
The focus is on moving services online for user convenience and cost savings.	The focus is on promoting transparency and citizen engagement and data economy. E-government and Open initiatives often coexist.	The focus shifts from simply listening to citizen or user needs to exploring the new possibilities collecting and leveraging data.	The public organizations and governmental agencies have fully committed to a data centric approach to improving government. The data flows regularly across organizational boundaries.	The digital innovation process uses open data and is embedded throughout the entire government. Innovation is a predictable and repeatable process.

Source: Adapted from Gartner, 2022

2.3 Digital Identity

Some of the early movers in digital identity considered it as a central element in fostering the internet economy (OECD, Digital Identity Management, Enabling Innovation and Trust in the Internet Economy, 2011, p. 13), because thanks to its use we can interact online and have the chance to being recognized by the other part. In other words, digital identity enables non-face-to-face interactions between persons and organizations.

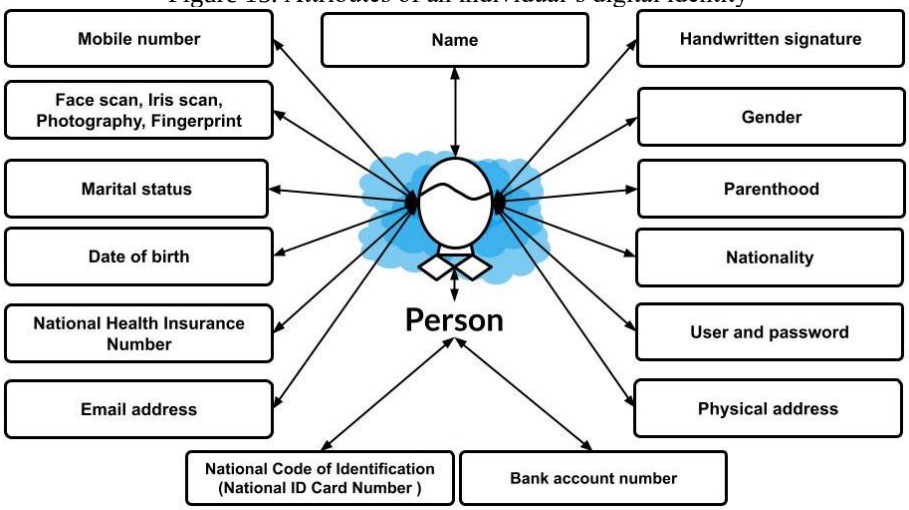
Along the same lines, the United Nations in its "2020 Electronic Government Survey" indicates that digital identity plays a central role in the development of digital government and the use of data; likewise, it points out that digital identity lays the foundations for the safe sharing of data and information between public entities (UN, E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development, 2020, p. 171). In the same line, we can refer to digital identity as a collection of traces that we leave behind us (digital identifier, users, IP address, email address, avatars, links, etc.) as well as the analysis of these information (Bouzefane, 2015, p. 9).

Likewise, we can say that the digital identity is a set of digital data which represents an entity in the digital virtual world (internet, information system, etc.), some can say that it is a computer representation. In this context, when we mention an entity, it can be a person, group of people, organization, or devices, even, we can consider that a person can also create different digital identities.

In addition, digital identity can be understood as a set of attributes (digital data) that represents an entity (person, organization, object) in the digital environment. For instance, in the case of an individual (natural person)

their attributes can be its name, username and password, date of birth, postal address, age, gender, profession, email, comments, photos, videos, etc. <Figure 15> shows the basic attributes of an individual's digital identity.

< Figure 15. Attributes of an individual's digital identity>



Source: Own development, 2022

Additionally, the World Economic Forum (WEF) indicates that our identity is increasingly digital, distributed and plays the role of a decision maker of what products, services, or information we can access or receive. In terms of the WEF, our digital identity is not a simple access web page, it is the integration of the immense amount of information that exists about us, our profiles, and the history of our activities online (WEF, Identity in the Digital World a new chapter in the social contract, 2018, p. 9).

Most of the time, the integration of data and information implies interoperability between information systems or digital platforms, in the context of this research, interoperability is the ability to exchange data and to make use of these data within the receiving system (Tolk, 2013, p. 1).

Another point of reference is the work made by in the National Institute of Standards and Technology (NIST) in its Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management, which asserts

that digital identity is the unique representation of a subject engaged in an online transaction (NIST, 2017, p. 12), it means that a digital identity is always unique in the context of a digital service. In the same line, a digital identity can be understood as a digital representation of a person acting as an individual or as a representative of an organization.

It enables them to prove who they are during interactions and transactions. They can use it online or in person. Services and organizations that let users use secure digital identities can better trust that those users are who they say they are (GOV.UK, 2022). In the same line, the Inter-American Development Bank (IDB), in its study Identity Management and its impact on the digital economy, points out that digital identity is the cornerstone of the digital transformation of Latin America and the Caribbean (LAC), its value underlies on the quality of civil registries.

That is the reason because during the enrollment or registration process, gathering of data for registering the digital identity attributes such as name, photography, age, gender must be deemed an essential activity to build a robust digital identity scheme. Additionally, IDB refers that digital identity is an essential element for the inclusion and reduction of transaction costs throughout the economy, thus helping to improve the quality of services in both the public and private sectors (IDB, Identidad Digital y su Impacto en la Economía Digital, 2017, p. 3).

Another good point of reference is the Australian Government, who claims that digital identity is a safe, secure, and convenient way to prove who you are online every time you access government services (Australian Government , 2022).

2.4 Attributes

We can understand attributes like a piece of information that describe aspects or characteristics about a person or organization (DCMS, 2022). Another way to understand them is like the characteristics or properties of an entity that can be used to describe its state, appearance, or other aspects. It is a particular well-defined aspect of the description of an entity in an identity management system (ISO, ISO/IEC 24760-1, 2011, p. 2).

We can use a combination of attributes to create a digital identity. Note that the values of the attributes in an entity together describe the entity in a specific domain.

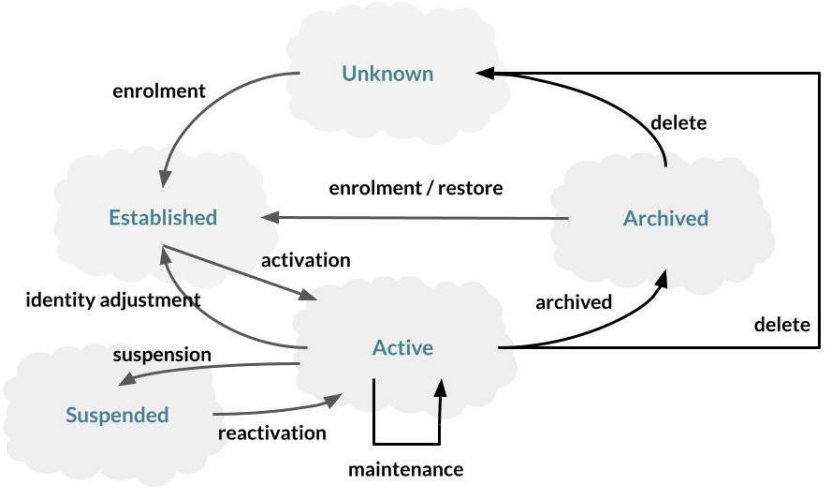
2.5 Identity Management

Identity management can be understood as the process of managing user identities by providing access rights and privileges within a company or organization by employing emerging technologies (Srinivasan Madham Kumar, 2010, p. 1). In the same way, the ISO/IEC 24760-1, identity management refers to the processes and policies involved in managing the lifecycle and value, type, and optional metadata of attributes in identities known in a particular domain (ISO, ISO/IEC 24760-1, 2011, p. 5).

Now, when it refers to attributes, it means characteristics or properties of an entity that can be used to describe its state, appearance, or other aspects. In addition, when the ISO mentions “lifecycle” it is because the attributes and their metadata can take different values during their existence.

Furthermore, it suggested that some states such as unknown, established, archived, active and suspended, all of them can be affected during the time by an individual’s activities.

<Figure 16. Identity lifecycle>



Source: Adapted from ISO, 2022

One additional thing is that under this definition the identity management can be applied to different entities such as human beings, organization (government agencies), business entities, devices (SIM card, computers, among others), systems, subsystems, or software applications. In fact, the definition is neutral in this regard. To name one example, on September 1, 2006, the Uruguayan government enacted the Law N° 17997, with the purpose to identify and maintain a national register of every calf born in national territory (Uruguay), at the beginning the identification was voluntary but with the entry into force of the Law N° 17997, the identification was mandatory.

<Figure 17. Identification of every calf born>

Source: https://parlamento.gub.uy/noticiasyeventos/noticias/node/85404
https://www.inac.uy/innovaportal/file/5219/1/libro_trazabilidad_ingles.pdf

In this respect, I must highlight that this thesis focuses on natural persons (human beings, persons, individuals) interacting with digital services provided by public entities or private organizations through the cyberspace (digital environment). Drawing on the above, the notion of Identity Management cannot be completely understood if we do not mention its main processes, according to the ISO/IEC 24760-1 there are at least three (03) processes: Identification, Authentication and Maintenance. In the same way, the OECD, accomplishing its mission, put forward five (05) processes for the digital identity management Registration, Authorization, Authentication, Access Control and Revocation. As shown in <Table 13>, the common and fundamental processes in Digital Identity are Identification and Authentication.

Table 13. Digital Identity Management Processes

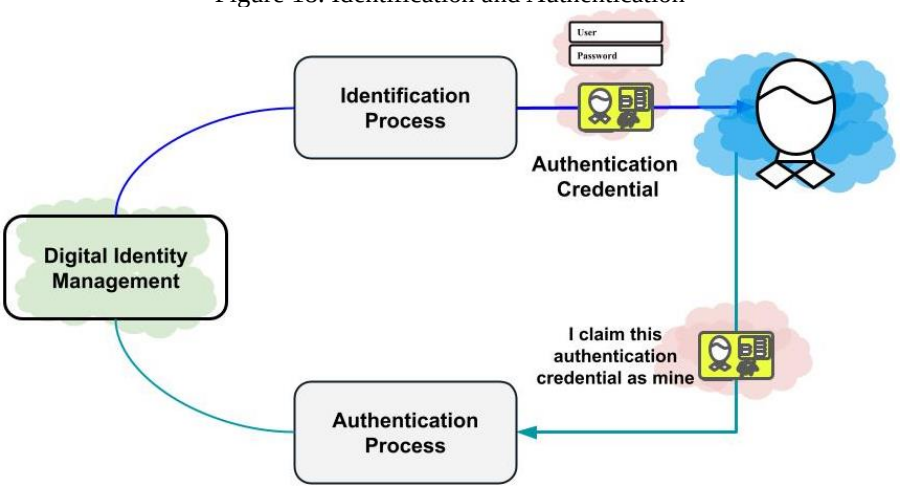
ISO/IEC 24760-1		**Digital Identity Management OECD**	
Process	**Subprocess**	**Process**	
Identification	Verification	Registration or Enrollment	
	Enrolment		
	Registration	Authorization	Give privileges Who is he allowed to do?
Authentication	-	Authentication	Who is the subject?
Maintenance	-	Control Access	What privileges / resources / actions (Read, Write, Execute, Delegate) the subject is allowed to do based on its identity
	-	Revocation	

Source: Own development

In this regard, WEF proposes that we must differentiate with special care identification and authentication terms, because they are usually confused, but have different meanings and purposes. On the one hand, identification is the process to univocally identify who is one within a context or population, often involves performing identity tests that allow us to verify and validate

attributes (name, date of birth, fingerprints, iris scan, etc.) that the person or entity claims (present). On the other hand, authentication is the process of determining if the authentication credentials (user and password, fingerprint, token, etc.) used to indicate and claim a certain digital identity is valid, it belongs to the person or entity previously identified. Considering all the above, digital identity management has become a crucial component of controlling who has access to information, and under what conditions (Brubaker, 2009).

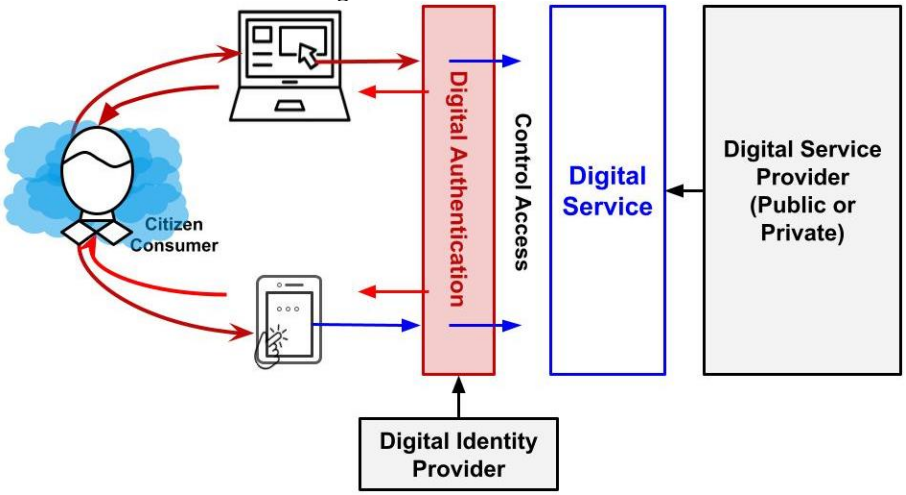
<Figure 18. Identification and Authentication>



Source: Own development, 2022

Drawing on the above, the authentication can be defined as "*the process of verifying that people are who they say they are, is an essential first step in the provision of electronic services*" (UN, E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development, 2020, p. 171). In the same line, we can understand the authentication like a performing a check of access credentials input during the access phase to the digital service (ITU, Digital Identity Road Map, 2018, p. 50). The latter definition clarifies more the difference between authentication and control access, with the first one you only validate the identity of a persona, while the second one, you can validate the privileges that it has.

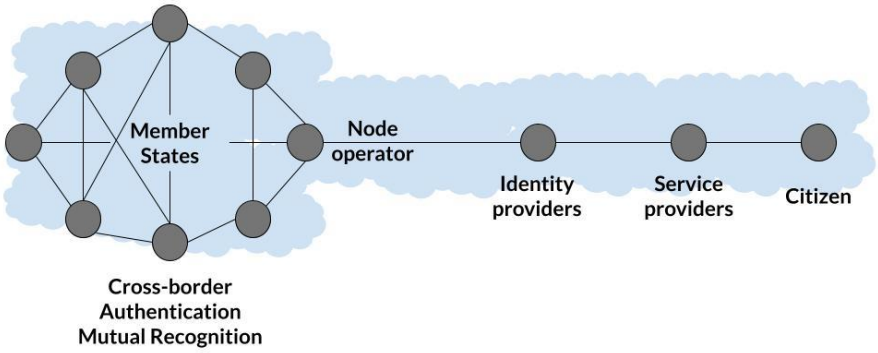
<Figure 19. Authentication>



Source: Own development, 2022

In the same line, the Regulation N° 910/2014 of the European Parliament and the Council on "Electronic identification and trust services for electronic transactions in the internal market and repealing", pointed that electronic identification means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person. In the same way the European Regulation indicates that authentication is an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.

<Figure 20. Cross-border Authentication Scheme (eIDAS)



Source: Own development

Traditionally, the authentication has been done by three (03) factors of authentication (mechanism), they are: a) Something that you know, for example your password to log in, b) Something that you are, for instance handwriting, biometric (fingerprint, iris scan, voice recognition, hand recognition) and c) Something that you have, for instance security token based on cryptography (Lee, 2013). As shown in <Table 14>, the different kinds of factors of authentication.

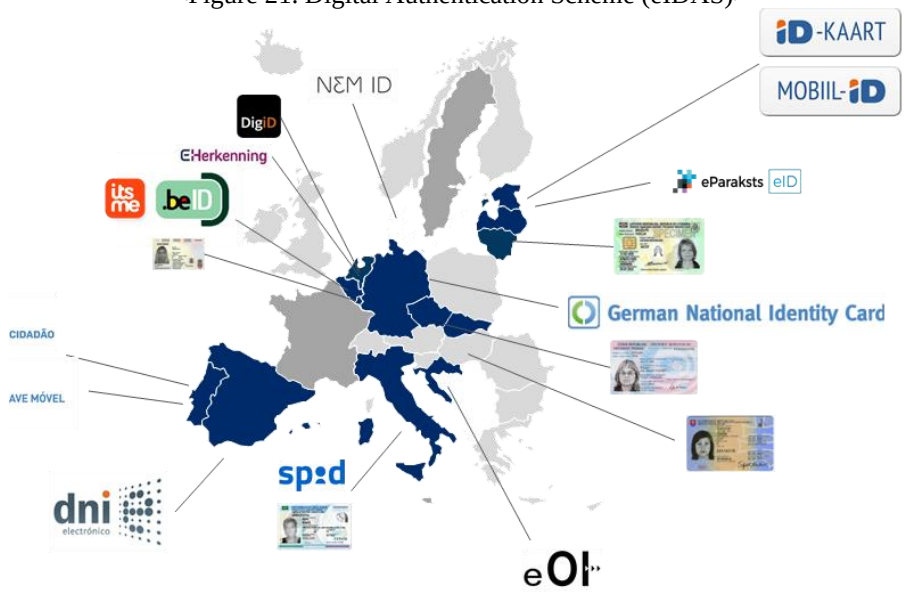
Table 14. Factor of authentication

Factor of authentication	**Examples**
Something that you know	Password
Something that you are	Biometric (fingerprinting, iris scan, etc.)
Something that you have	Security token base on cryptography

Source: Adapted from NIST

The Challenge is how to escalate the Digital Identity Management at a National Level, in this regard, one remarkable step was made by European Union when they enacted the "Electronic Identification and trust services for electronic transactions in the internal market (eIDAS)", which proposes a framework to a cross-border digital identity recognition in the European Union (EU), with the aim of providing a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. eIDAs introduces a mutual recognition of nationally issued Electronic Identification Schemes (eID schemes), which is mandatory to access public services, and voluntary to access private services.

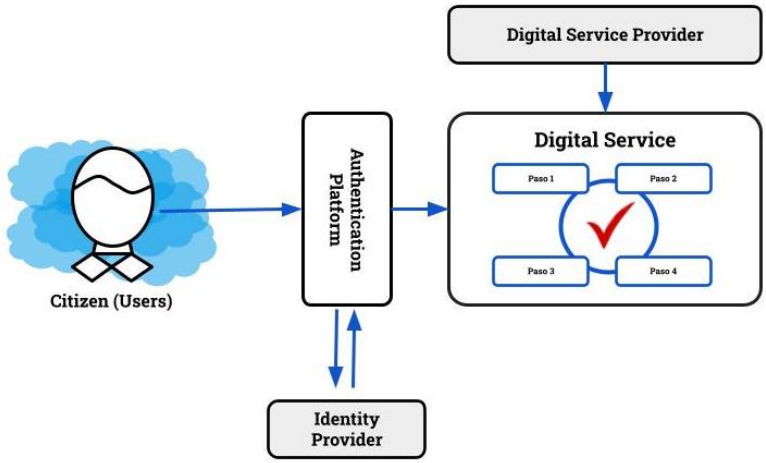
<Figure 21. Digital Authentication Scheme (eIDAS)>



Source: Adapted from EIDAS, 2022

As noted above, it is important to bear in mind that every Digital Identity Scheme has at least three (03) elementary components (Deloitte, 2016): a) service users, b) identity providers, who capture and store attributes of the identity of the users, they make sure that they are true, and they come to complete transactions on their behalf, and c) the service providers, who provide the digital service to the users (citizen, clients, customers, etc.)

<Figure 22. Basic elements of Digital Identity Scheme>



Source: Own development, 2022

2.6 Cyberspace

Before turning our attention to the structural components of the digital identity scheme and how it is essential to strengthen the security and trust in cyberspace, it is helpful to analyze some of the definitions of the term cyberspace. The first one is provided by the United States Department of Defense (US DoD), while the second one is provided by The International Organization for Standardization (ISO). According to the US Department of Defense the cyberspace is "…many different and often overlapping networks as well as the nodes (any device or logical location with an internet protocol address or other analogous identifier) on those networks, and the system data (such as routing tables) that support them. Cyberspace can be described in terms of three layers: physical network, logical network, and cyber-persona.

The physical network layer of cyberspace consists of the geographic component and the physical network components. It is a medium where the data travels. The logical network layer consists of those elements of the network that are related to another in a way that is abstracted from the physical network, i.e., the form of relationships is not tied to an individual, specific path, or node. A simple example is any website that is hosted on servers in multiple physical locations where all the content can be accessed through a single uniform resource locator. The cyber-persona layer represents yet a higher level of attraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. The cyber-persona layer consists of the people on the network".

On the other hand, The International Organization for Standardization (ISO) refers to cyberspace as a "Complex environment resulting from the interaction of people, software, and services on the internet by means of

technology devices and networks connected to it, which does not exist in any physical form". Both definitions have in common that the person is a key component of cyberspace; but we must emphasize that is the person (individual) interacting with other entities (government, business, individuals, etc.) using its digital identity through the networks to perform its social and economic activities.

Finally, considering the definitions above mentioned when we refer to a cyberspace, we understand a complex and synergistic environment of three overarching layers: physical, logical and persona interacting among them.

2.7 Cybersecurity

Along with our increased dependence on digital technologies and rise of cyber attackers it is imperative to design safeguards and measures to improve the digital security of our information systems, process, and information (Lee, 2013, p. 1). The International Organization for Standardization (ISO) refers that cybersecurity is understood as the preservation of confidentiality, integrity, and availability of information in cyberspace (ISO, 2012), these three properties confidentiality, integrity, and availability are the cornerstone of the information security standards (Lee, 2013, p. 1).

Confidentiality means "*the information is not available or disclosed to unauthorized entities; integrity is prevention of unauthorized modification of protected information, the information is accuracy and completeness, availability means the information is accessible and usable on demand by unauthorized entities*" (ISO, ISO 27000, 2018).

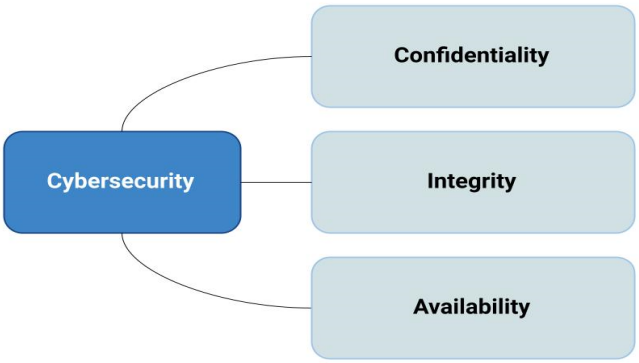
However, many times this concept is understood only from a technological perspective, that is why the ITU points out at Global

Cybersecurity Index 2020 that cybersecurity is "(...) a multidisciplinary field, and its application involves all sectors, industries, and interests, (...). To increase the development of national capacities, efforts must be developed from a political, economic, and social perspective.

This can be developed by law enforcement agencies, justice departments, educational institutions, ministries, private sector operators, technology developers, public-private partnerships, and cooperation between States" (ITU, 2020).

Drawing on the above we can conclude that security in the digital environment (cybersecurity) requires a comprehensive approach, it is not a merely technical aspect, but rather includes aspects of national security, international cooperation, regulation, coordination between companies, the public sector, organized civil society and citizens. <Figure 23> shows the principles of cybersecurity.

<Figure 23. The principles of Cybersecurity>



Source: Adapted of Security Basics for Computer Architects, 2022

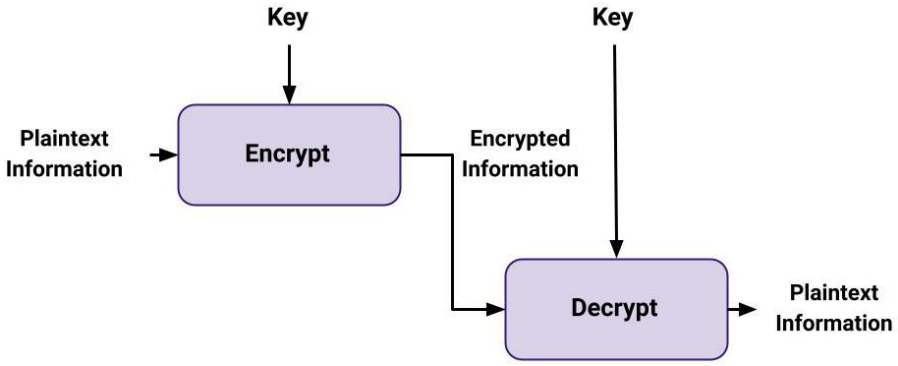
2.8 Cryptography

It is a mechanism to enhance the confidentiality and integrity of information during transmission, computing, and storage (Lee, 2013, p. 29). It can be understood as the discipline which embodies principles, means, and

methods for the transformation of data to hide its information content, prevent its undetected modification and/or prevent its unauthorized use (ISO, ISO 7498-2, 1989). There are three cryptography methods: symmetric-key, Cryptography hash functions and asymmetric-key.

- Symmetric-key cryptography means that an original message is encrypted by the sender and decrypted by the recipient using the same key. It is used to protect confidentiality.

<Figure 24. Symmetric-key cryptography>



Source: Adapted of Security Basics for Computer Architects

- Cryptography hash functions means that an original message is compressed into a short, which is called hash value. Any change in the original message, the resulting hash will change. It is used to protect integrity.

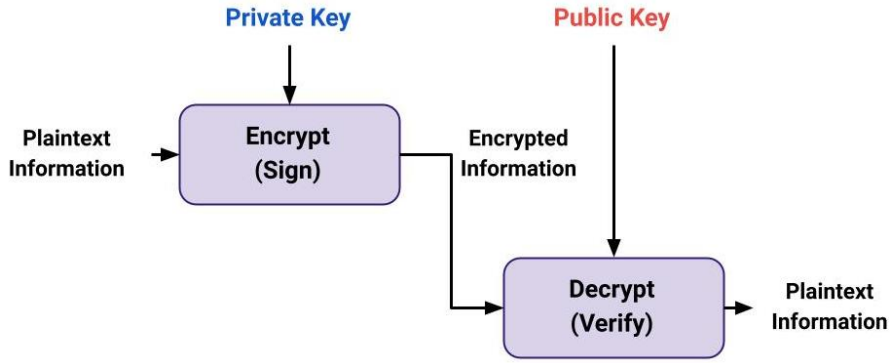
<Figure 25. Hash>

Source: Adapted of Security Basics for Computer Architects

- Asymmetric-key cryptography, also called Public-key cryptography uses two keys, one for encryption and other one for decryption. The private key can be used for encryption messages and documents, it is

like signing documents, and the private key is also used like your digital identity, it means we can identify a piece of software, a chip, hardware, system, and persons. It is used for authentication.

<Figure 26. Asymmetric-key cryptography>



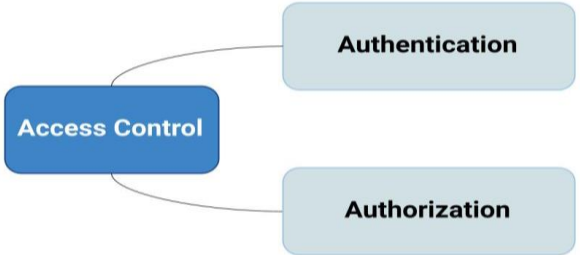
Source: Adapted of Security Basics for Computer Architects

2.9 Access control

Access control refers to ensuring or restricting access to those allowed to access the information or assets based on business and security requirements (ISO, ISO 27000, 2018). It comprises of Authentication and Authorization. Authentication aims at dealing with the issue Who is he/she? The authorization answers the question Who is he/she allowed to do? (Lee, 2013, pp. 2-3).

Both Authentication and Authorization are the fundamental processes to control legitimate access to protected assets such as data, information, code, software among other resources. Access control can be applied to electronic devices, humans, organizations, etc.

<Figure 27. Access control>



Source: Adapted of Security Basics for Computer Architects

2.10 Digital divide and digital inclusion

According to the National Digital Identity Plan 2020-2025 made by RENIEC, digital divide is a set of barriers that prevent universal, ubiquitous, equitable and affordable access to information and public services or procedures available by secure electronic means. In that vein, there are two factors that generate the digital divide, they are a) Digital divide due to connectivity and b) Digital divide due to digital illiteracy.

The first one is related to the possibility or difficulty of having a computer or electronic device connected to internet, while the second one refers to the human capacity to know how to use the electronic device or software (RENIEC, National Digital Identity Plan, 2020).

In the same line, the National Digital Identity Plan 2020-2025 pointed out that digital inclusion is the process of incorporation of variety of actors to use electronic means to access digital services (RENIEC, National Digital Identity Plan, 2020).

2.11 Transport Layer Security (TLS)

The Transport Layer Security (TSL) protocol or as it is sometimes referred to Secure Sockets Layer (SSL) protocol, it is a connection-oriented protocol, client-server protocol, probably it is the most widely deployed communications security protocol used on internet (Turner, 2014), it provides authentication, integrity, and confidentiality for two parties.

It enables establishment of a secure channel between two parties over the public internet (Lee, 2013, pp. 74-75).

2.12 OAuth 2.0 and OpenID Connect

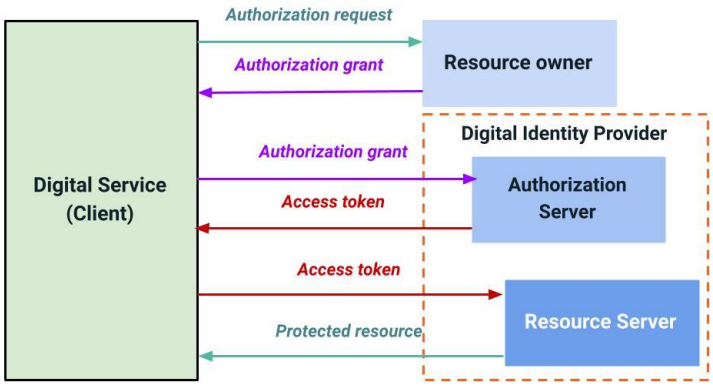
a) Open authorization framework 2.0 (OAuth 2.0)

The open authorization framework 2.0 (Oauth 2.0) is an emerging identity management standard, enabling an end-user to grant an application-controlled access to personal information stored at a third party (Al-Sinani, 2011).

It is a protocol based on RFC 6749, it was published at the end of 2012, its purpose is to define a standardized process to allow a third-party application to access a protected resource on the web (typically personal information).

The presence of a human being is not mandatory in the process (N. Hossain, 2018). OAuth 2.0 is popular amongst social networks like Facebook, Google, and Twitter, all of them are making their APIs based on the OAuth protocol to increase user experience (Kim S. O., 2019).

<Figure 28. Open authorization workflow>



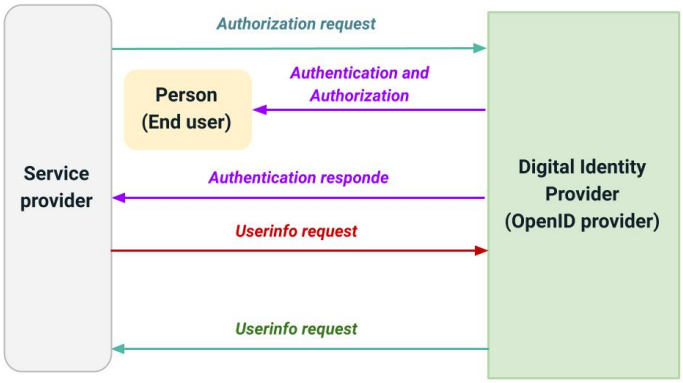
Source: Interoperable OAuth 2.0 Framework, 2022

b) OpenID Connect

OpenID Connect protocol is an open, decentralized, free framework for user authentication. It was developed based on OAuth 2.0 protocol (Batista, 2022). Technically, OpenID Connect has two main components: Relying party

(RP) and OpenID Provider (OP). RP is a service provider (digital service provider); it means an entity that relies on the Identity Provider to verify and assert the identity of users. An OpenID provider is an identity provider capable of authenticating a user (Jorstad, 2009). In addition, OpenID can Exchange data and information using REST and JSON messages, and to deal with security issues it uses TLS.

<Figure 29. OpenID workflow>



Source: Interoperable OAuth 2.0 Framework. 2022

2.13 Public Key Infrastructure (PKI)

Overall, a Public Key Infrastructure (PKI) is a technology that was introduced for establishing trust over an insecure electronic environment, it is an enabler for digital trust. To do this, PKI has a centralized and hierarchical model for enabling trust (Rajendran, 2017, p. 1). PKI represents the underlying for digital signatures (Vatra, 2022, p. 1).

PKI is a general-purpose security infrastructure that is enabled by public key cryptography technology, and it is functioned to provide network security services. It offers a full set of security assurance infrastructure for sectors like e-commerce, e-government, e-baking and among others (Zhang, 2010, p. 1). PKI gives each user a pair of keys, a private key and public key, used in every signed transaction, the private key is used only by the signer, the

public key is available and used by those that need to validate the signer's digital signature (Vatra, 2022, p. 1).

For some scholars, adopting a general point of view, the components of a PKI framework are technology, standards, policy, and implementation (Rajendran, 2017, p. 1).

Others from a more technical perspective assert that the components of a PKI are Certifying authority, registration authorities, repository, archives, and end users. The PKI's services are confidentiality, integrity, authenticity, and non-repudiation (Vatra, 2022, pp. 1-2).

2.14 Digital Signature

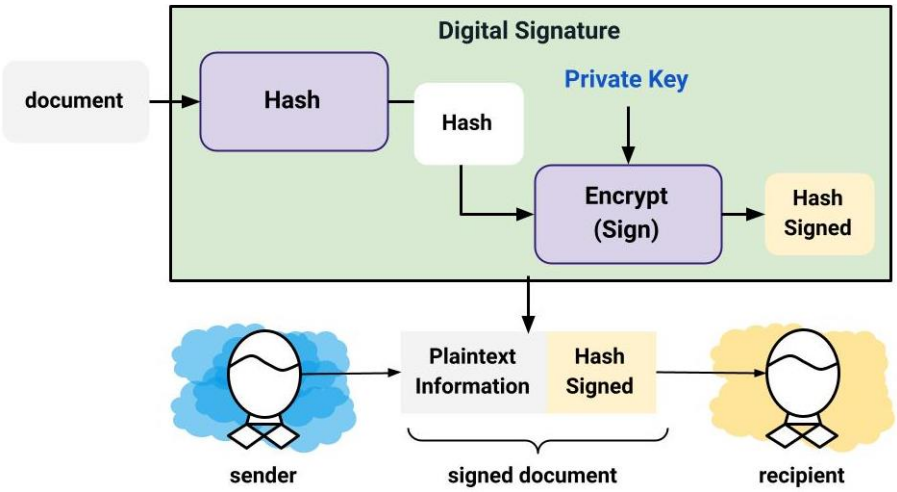
Rapid development of the Internet makes electronic government and electronic commerce a new model for business activities, however at the same time, it generates a greater security risk, in this regard, digital signatures technology is an effective solution to ensure data exchange integrity and non-repudiation of sending messages.

A digital signature is used to bind the signer with a document, to ensure the integrity of the document that was signed (Lee, 2013, p. 54).

According to IS0 7498-2 standard, digital signature is defined as data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove source and integrity of the data unit and protect against forgery.

From a technical perspective, digital signature makes use of asymmetric cryptography, it means a private key to generate signature from document hash, and public key to verify signature (Husni, 2015, p. 1).

<Figure 30. Digital signature>



Source: Adapted of Security Basics for Computer Architects, 2022

2.15 Framework to comparison

For conducting the comparative analysis between the Digital Identity Schemes of Korea and Peru, we need to deal with two (02) issues a) What is the framework for undertaking a comparison between Digital Identity Schemes? and b) What techniques and tools will be used to perform the comparative analysis?

To deal with the first question, by recognizing that there are different ways to compare the electronic government development amongst countries, but there are not much evidence about how to compare digital identity schemes between countries, a theoretical comparison is constructed based on the experience of Electronic Government Development Index (EDGI), Digital Government Index (DGI), Key factors of Korean Electronic Government Succeed, literature review, international organization's studies, and interviews with ICT specialist.

By combining of the concepts and theories, the researcher devised a Comparison Framework consisting of five (05) dimensions: 1. Governance, 2.

Legal framework, 3) Technology, 4) Investment on Research and Development (R&D) and 5). Market, that will be describe below.

Governance, we are going to evaluate if there is a Digital leadership it means a public engagement of the President, Minister, or competent executive role in to carry out the Digital Agenda, it can be proved if there is a National Policy, Plan or Strategy which orientates the planning and decisions of the governmental agencies under a top-down approach. Likewise, we can analyze if there is a stand-alone independent or not, which is accountable for maintaining and overseeing the deployment of digital government and digital identity at national level (Ministry, Agency, Secretary). To evaluate the governance, we are going to use the table below:

Table 15. Governance Evaluation Criteria

Governance		
Component	Level	
1.1 Institutional arrangements	Strong (5p)	There is an autonomous (independent) governmental body, such as Ministry or Agency responsible for the digital transformation in public and private sector.
	High (3p)	Autonomous (independent) governmental body responsible for the digital transformation in public sector. In most of the cases, it is part of the executive branch of power.
	Medium (2p)	There is an Office, Secretariat or Department under a Ministry or governmental body responsible for the digital transformation in public, with an organizational structure and annual independent budget.
	Weak (1p)	There is an Office, Secretariat or Department under a Ministry or governmental body, without an organizational structure or control of annual budget.
1.2 Digital Leadership	Strong (3p)	There is a High-Level Commission or Specific role such as President, Premier, Prime Minister, Minister in charge of digital government, Chief Information Officer or Chief Digital Officer who led the digital agenda at national level and overseeing its implementation. Periodical meetings, long-term engagement, and the discussion of the digital issues as a part of the political agenda or national goals are features of the strong leadership. The executive's proficient is showed based on the timely issuance of Digital Master Plans, Digital Strategies, Digital Programs, etc.
	Medium (2p)	There is a High-Level Commission, or specific role such as President, Premier, Prime Minister or Minister in charge of digital government, Chief Information

		Officer or Chief Digital Officer who led the digital agenda at national level and overseeing its implementation. However, in the practice there are not periodical meetings, not long-term engagement, and discussion of the digital issues rarely are part of the political agenda. Political discussions delay and distract digital agenda. The executive's proficient is showed based on the emission of regulation, policies, and plans, however and unfortunately not always at the right time.
	Weak (1p)	There is not a specific role who led the digital agenda at national level and overseeing its implementation.
1.3 Collaboration and coordination	Strong (3p)	During the Digital Government Planning, the governmental body in charge of digital government has a close and effective collaboration with the governmental body responsible for the national budget such as Ministry of Economy and Finance, Ministry of Planning and Finance. Likewise, there is a flexible and dynamic distributions of responsibilities and activities in the deployment of digital government.
	Medium (2p)	Digital Government Planning it is an input for the national budget, and it is discussed with the Ministry of the Economy or Finance only when there is a political engagement, or the project or initiatives are included in the government plan or political pledge. There is the intention and technical will to make a proper distribution and coordination of the projects or activities, to avoid overlapping objectives, scopes, or duplicate investment.
	Weak (1p)	Digital Government Planning it is an input for the national budget, however, is not prioritized and not discussed with Ministry of the Economy or Finance. There is not a proper distribution and coordination of the projects or activities, some of them overlapping scopes and objectives.

Source: Own development, 2022

Legal framework, we are going to evaluate if there is regulation (Law, Presidential Decree, Supreme Decree, Enforcement Decree, among others) related to digital government and digital identity such as a) Digital Government Law, b) Regulation that assigns the responsibility of maintaining an identification system to an entity, c) Digital Identity Providers, d) Data Personal Protection Law or Data Privacy Act, among others. We are going to manage two options:

a) Have (1p): There is a law or regulation related to this field
b) Don't have (0p): There is no law or regulation related to this field

Technology, in the implementation of digital identity solutions we need to have a basic infrastructure to deploy the solutions, especially if we want to create digital services in an agile and flexible way. We are going to evaluate if there is a) Government Enterprise Architecture (Digital Architecture or Enterprise Architecture of the Government), b) Data Center, c) Identity Information System or National Identity Registry and d) Authentication Platform (Public Sector). We are going to manage two options:

a) Have (1p): This kind of solution, technology or facility is implemented.
b) Don't have (0p): This kind of solution, technology or facility is not implemented.

Investment on R&D, we are going to evaluate how much is the investment of the government on research and development. According to the World Bank (WB) (World Bank, 2022), the world average fluctuates between 1.97% to 2.2% of GDP, considering that information we are going to manage three (03) options:

Low (1p)	Medium (2p)	Strong (3p)
R&D <1% of GDP	**R&D** = [1.9%, 2.2%]	2.2% of GDP < **R&D**

Concentration of the market, are there digital identification providers in the market? is there a fierce competition among them or there is a high level of concentration in the market? We are going to manage three (03) options:

No market (0p)	Low concentration (3p)	High concentration (1p)
No companies	4 or more	2-3

Drawing on the above, to undertake the comparison, we are going to use a matrix, trying to sum the main points, issues, and findings, after that we can analyze them.

Table 16. Evaluation Criteria

Components					
1. Governance					
1.1	Institutional arrangements	Strong	High	Medium	Weak
1.2	Digital Leadership	Strong		Medium	Weak
1.3	Collaboration and coordination	Strong		Medium	Weak
2. Legal framework					
2.1	Electronic Government Law or Digital Government Law			Have	Don't have
2.2	Legal framework which assigned the responsible to maintain the basic identification system of citizen. (Registration of citizens). For example, a Resident Registration Act.			Have	Don't have
2.3	Regulation for Digital Identification Providers			Have	Don't have
2.4	Regulation for information security (cybersecurity), for instance National Cybersecurity Strategy			Have	Don't have
2.5	Regulation for interoperability			Have	Don't have
2.6	Regulation to protect the personal information and privacy of the persons, for instance Personal Information Protection Act, Personal Data Protection Law			Have	Don't have
2.7	Regulation to promote digital signature, for instance Digital Signature Act.			Have	Don't have
3. Technology					
3.1	Government Enterprise Architecture (GEA)			Have	Don't have
3.2	One Stop Service Portal, for instance Government24, GOB.PE			Have	Don't have
3.3	National Data Center			Have	Don't have
3.4	Open Cloud Platform (PaaS-TA and National Digital Government Platform)			Have	Don't have
3.5	Open Data Portal			Have	Don't have
3.6	Electronic Government Framework			Have	Don't have
3.7	Public Key Infrastructure (NPKI and GPKI)			Have	Don't have
3.8	Digital Authentication Platform (Public Sector)			Have	Don't have
3.9	Interoperability platform, for instance Public Information Sharing System or National Interoperability Platform.			Have	Don't have
4. Investment on R&D					
4.1	Investment on research and development (R&D)	Low	Medium		Strong
5. Concentration of the market					
5.1	Concentration of the market	No market	Low concentration		High Concentration

Source: Own development, 2022

CHAPTER 3: LITERATURE REVIEW

In this section, the researcher attempts to highlight the most important studies about digital identity and digital identity scheme available, to have a comprehensive understanding of the objective, approaches, constraints and concerns of previous studies in this field.

The noteworthy studies exerted by OECD, WEF and ITU gave us a clear understanding about digital identity and their components at national level, that is why we are going to describe all of them in a brief but understandable way.

1.1 Digital identity management, enabling innovation and trust in the internet economy

This study is the result of almost four years of analytical work developed by OECD between 2007 and 2011 with the purpose to share a common understanding about digital identity, explore the main policy issues surrounding digital identity and provide OECD policymakers the guidance to develop digital management policies, strategies, or plans.

First, the authors claim that digital identity management is an issue which emerges at the intersection of information security and privacy fields, it can be applied to natural persons (individuals), business entities, devices, software, among others. Second, the study focused on natural personas interacting with information systems of public and private organizations. In fact, having the possibility to be recognized by an information system is one of the main steps in the digital transformation process.

Third, according to the study the digital identity management process is enrollment or registration, authorization, authentication, and revocation. All

of them support the strategy of migrating social and economic activities to the digital environment.

In that sense, by offering security and privacy, digital identity management enables trusted relationships between remote parties. However, some digital identity practices create limitations to its development, for instance a) increasing number of credentials (user and passwords), b) high cost of registration or enrollment process because manual process and c) digital identity credential are not internationally recognized.

On the other hand, the challenges of the government are a) increase number of digital services, b) strengthen digital skills of citizens and people, c) promote flexible policies and creating a favorable condition to create a digital identity market attractive to investors, d) promote practices to enhance individual's privacy and e) create a national strategy for digital identity management, f) determine a balance between unique and multiple digital identity credentials and g) work with governments to enable cross-border digital identity management.

Drawing on the above, the research analyzes the digital identity strategies and policies of 18 countries, the study focuses on two aspects: vision and policies. Vision means the country has objectives and strategies to enhance the digital identity and policies refers to laws, plans, actions, among others.

Table 17. Digital Identity Management Evaluation Criteria

Vision	• Country have developed, are developing, or are considering the development of a national digital identity strategy.
	  • We are considering the development of a strategy.
	  • We have started to develop a strategy.
	  • We have finished to develop a strategy.
	  • We are starting implementation.
	  • We are quite advanced in the implementation.
	  • We are operating a digital identity scheme (fully developed).
	• Digital Identity Strategy considers as a fundamental objective:
	  • To realize electronic government.
	  • To create an advanced digital society.

	• To foster innovation in the internet economy for public and private sector. • To improve cybersecurity. • To reduce the requirement for users to log-in multiple times • To promote the use of a limited number of digital credentials or to facilitate the management of digital identity credentials • Digital Identity Strategy is led by: • High level of the government. • Specialized ministry or agency. • Digital Identity Strategy considers as a fundamental initiative: • Implement an electronic national identity card. • To modify the authentication market status quo. • To implement a Single Sign On (SSO) • Digital Identity Strategy scope encompasses: • Public sector • Public and private sector
Registration policy	• Citizen registration policy (centralized or decentralized) o Centralized, based on population register and unique identifier assigned to all citizens o Decentralized or federated, several registration systems coexist and interoperate. Each organization is autonomous regarding its registration mechanism. • Adoption of digital credentials voluntary or mandatory
Security policy	• Digital signature legislative framework to promote a PKI market. • Standards for security • Cybersecurity strategy
Interoperability policy	• To ensure exchange data and information in a federated registration policy we need to subscribe federation agreements. • Technical infrastructure to promote interoperability • Technical framework to promote interoperability • Standards for interoperability • Digital Identity Management is part of the basic technical infrastructure.
Privacy policy	• Legal privacy protection framework. o Privacy Impact Assessment PIA o Data protection Agency • Privacy by design • Channels to data breach notification

Source: Own development

As noted above, there are five dimensions to design a digital identity scheme comparison amongst countries, they are vision, registration policy, interoperability policy, security policy and privacy policy. Additionally, this study shows us that Digital Identity Schemes implementation should respect national context, style of government, culture, traditions, existing population

registers, political system, and history of the country. We must not establish a completely new scheme regardless of these aspects.

1.2 Digital Identity from a legal concept to a new reality

Digital identity has gone from an emergent legal concept to something that it is still not fully understood by citizens and society (Sullivan, 2018, p. 1), however as users and policy makers we can notice the implications of the digital identity in strengthening accuracy, inclusiveness, security, and usability of digital services on public and private sector.

In the case of the government the principal driver to implement a digital identity scheme is to increase efficiency in service delivery and reduce fraud (Sullivan, 2018, p. 4). In this regard, the implementation of a digital identity scheme is a strategic initiative to improve effectiveness and efficiency of the government and customer service in the private sector.

A digital identity scheme has two fundamental process a) Identification, it includes the registration of identifying information such as full name, date of birth, usually gender, signature, photograph, unique number, biometrics (scan iris, fingerprint, voice) among others which are used to link an individual to a digital identity. b) Authentication, it means verification of the identity at the time of a transaction when someone claims it. Digital identity is like a key to allow access to the system.

The study reveals that there is much to be done by policymakers to leverage the potential of digital technologies and digital identity, for instance Estonia is working on Estonia e-Resident program, the first international digital identity program, the main aim of the program is expansion of Estonia's economic base, the revenues of that implementation are about €14 million, the return of its investment was estimated as €100 for each €1 (Sullivan, 2018, p. 6).

Drawing on the above, all this development leads us to recognize that digital identity as an individual right, which in a digital environment has the potential to dismantle geographical boundaries and concepts of migration, residence, and citizenship (Sullivan, 2018, p. 6).

1.3 Identity in a Digital World a new chapter in the social contract

WEF undertook research about the state of art of digital identity to understand the reasons to implement it, types of digital identity scheme and elements of a good digital identity scheme.

From a business perspective, the reasons are a) creation of new markets, b) know your customers to retain their trust and ensure a good customer experience and c) manage the growing cyber risk such as identity theft, data leak, intrusions into customer's privacy, among others, d) manage the end-to-end value chain of the products. On the other hand, from the perspective of the government, the aims of its implementation are a) improving public service delivery, b) enhancing interoperability across the governmental agencies, c) strengthening privacy and information security, d) inclusion to avoid digital divide among others.

According to WEF there are five elements that a good entity must comply with, they are: a) fit to purpose, b) inclusive, c) useful, d) offers choice and e) secure. A brief explanation of these elements is relevant because they provide criteria for comparing digital identity schemes.

Table 18. Elements of a good digital identity scheme

Fit to purpose means that the digital identity scheme provides accuracy (digital identity is precise, as a result reduce the potential of identity fraud), uniqueness (username, identifiers, biometrics, among others), sustainability (business model such as free of charge, fees, among others are evaluated, public-private partnership to share financial burdens), and scalability (to grow as demand). Aspects like accuracy and uniqueness are associated with the digital trust of the system. Sustainability and scalability are related to the access and experience of the user.

Inclusive means that the digital identity scheme provides equal opportunity, safeguards against discrimination and mechanism to manage unintended consequences. The features evaluated are enrolment process (multiple entry points to access services, multiple identity systems based on their needs, concerns, and rights), multiple access point, accessible design (for people with differences on abilities, age, digital literacy, among others) and usage of standards.
Useful means that the digital identity scheme provides utility, convenience, ease of use, and interoperability and portability. The features evaluated are the adoption of digital identity system by individuals and organizations, mutual recognition of digital identity credentials (credentials issued by one system are accepted by another to authenticate and access services), the proofing process must be according to its context, level of risk and use-case and standards to proof authentication.
Offer choice means that the digital identity scheme provides transparency, privacy, data protection and user control. The features evaluated are data protection or privacy regulation, data commissioners or data protection authority (independent of the government or under a branch of the government), privacy by design and human capacity development.
Secure means that the digital identity scheme provides protection, data integrity and liability. The features evaluated are cybersecurity practices and human capacity development, ability to recover against an incident.

Source: Own development

Additionally, the study asserts that there are three archetypes of the digital identity scheme of today and tomorrow: centralized, federated and decentralized.

a) Centralized, a single organization manages, captures, stores, and uses attributes and data about an individual's identity. For instance, the government or bank. One single organization manages the digital identity scheme.

b) Federated, two or more centralized digital identity systems establish mutual trust. To accomplish that parties involved usually establish an agreement or technical standard.

c) Decentralized, there is not a single government or organization in charge of managing a digital identity system. Transparency and control are the main benefits offered to the users. This archetype is new, and it has been developed in the ICT market.

In sum, WEF provides a relevant framework which is useful, first, to categorize the type of digital identity schemes (centralized, federated and decentralized) and second, evaluate a digital identity scheme based on five criteria fit to purpose, inclusive, useful, offers choice and secure.

1.4 Digital Identity Roadmap guide

Digital Identity Roadmap guide is a publication of ITU, whose purpose is to provide guidance to policymakers in developing a National Digital Identity Framework and general understanding of the basic concepts of digital identity and how to apply them in a national context.

As we mentioned in the Conceptual Framework, ITU refers to identity as the representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. Drawing on this concept, the study asserts that digital identity is the digital representation of an entity detailed enough to make the individual distinguishable within a digital context. As the study mention, at national level the implementation of a national digital identity scheme brings benefits for citizens, government, and society, for example by a) improving convenience and user experience, b) reducing cost of access services, c) improving citizen inclusion, d) improving service delivery, e) reducing cost of service delivery, e) improving security, f)

In this vein, ITU provides some fundamental components to consider when we implement a digital identity scheme. They are a) Governance Model, b) Approaches for fostering adoption, c) Architecture Model, d) Sustainability Model. In the table below we resume the elements of every fundamental component:

Table 19. Components of a good digital identity scheme

Governance Model	Government is an Identity Provider
	Government is only a Regulator, the government has the role of issuing laws, specific regulation, criteria, conditions, among others.

	Government is a Regulator and Identity Provider
Approach for fostering adoption	• "*Government should be capable of offering secure, easy, and convenient access to a series of public services*". • How convenient the enrollment process is, it means what is the level of identity proofing, for instance identity proofing in person or remote identification. • Usability • Issuing of digital identity: Voluntary vs mandatory • Security and privacy, security by design approach, all the identity providers and service providers must meet government and international standards for security and data protection • "Identity broker, there is an intermediary that connect identity providers and service providers".
Architecture Model	There is one unique identity provider or multiple identity providers, or an identity broker with multiple identity providers.
Sustainability Model	Financing by the public sector Financing by the public and private sector Financing by the private sector

Source: Own development, 2022

Additionally, ITU pointed out that there are critical success factors to overall success in the digital identity scheme implementation. They are organization structure, project management, quality and standardization and Regulatory framework. To evaluate how the National Digital Identity Schemes has been implemented, the study analyzes some countries (Canada, India, Estonia, Tanzania, United Kingdom, etc.) the aspects evaluated are:

- Roles: Identity Broker, Identity Provider (Government), Digital Service Provider
- Process: Enrollment and Authentication
- Regulation
- Credentials: User and passwords, PIN, banking credentials, Digital Signature, ID Number, fingerprint, iris, OTP, among others.
- Level of adoption.
- Issuing of digital identity: Voluntary vs mandatory.

In sum, ITU provides a relevant framework to implement a Digital Identity Scheme and overall criteria to make a comparison amongst countries.

1.5 Limitations of study

As we have seen, there are various studies related to digital identity systems or digital identity schemes, most of them focused on understanding their types, components, and its interactions. The research carried out by the OECD and the WEF is relevant in that sense.

Notwithstanding the above, first, there are not many works comparing digital identity schemes at a country level, even less, those that try to compare a developed country like Korea with a developing country like Peru.

Finally, there are no developed digital identity comparison schemes, such as exists in the field of electronic government, competitiveness, or digital government.

CHAPTER 4: DIGITAL IDENTITY IN KOREA AND PERU

In this section, the researcher, first, attempts to describe every component of the Comparison Framework based on documental analysis and interviews with ICT specialists, second, to address the research questions and highlight the most important findings in the Digital Identity Schemes.

4.1 LEGAL FRAMEWORK

The rapid changes of modern societies entail an increasing pressure for ongoing adjustments of the legal and administrative framework (Eifter, 2004, p. 3).

In this regard, seeking to understand the differences in the development of Digital Identity Scheme in Korea and Peru, we are going to review the legal framework issued thereon. In the case of Korea, we are going to make a brief abstract about the Government Organization Act, Resident Registration Act, Electronic Government Act, Promotion of Information and Communication Network Utilization and Information Protection Act, Personal Information Protection Act, Digital Signature Act, and National Cybersecurity Strategy.

On the other hand, in the case of Peru we are going to focus on the Political Constitution, Digital Government Law, the Law of the National Registry of Identification and Civil Status (Law N° 26497), Ministerial Resolution N° 156-2021-PCM, Legislative Decree N° 1412, Signatures and digital certificates law, the Supreme Decree N° 029-2021-PCM, Enforcement Regulation of the Digital Government Law, Personal Data Protection Law, Digital Security and Trust Framework.

4.1.1 Korean digital identity legal framework

a) Government Organization Act

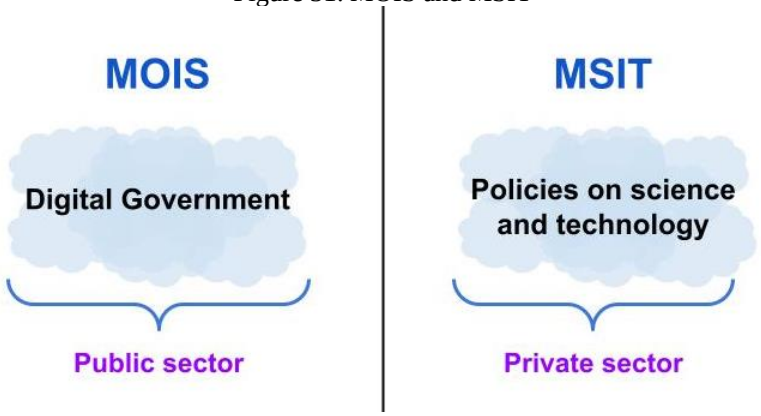
In March 2004, the Government Organization Act (Act N° 14839) was enacted, according to its article 34, MOIS was given electronic government jurisdiction, it means MOIS is in charge of coordinating and overseeing the affairs concerning electronic government.

This institutional arrangement made a well-organized structure to advance the e-Government services (Kim S. , The Evolution of Korean E-Government in the perspective of Actor-Network Theory, 2014, p. 38). In other words, MOIS takes the leading role in leveraging new technologies for the public sector (UN, Member State Questionary Korea , 2020).

MOIS oversees the development and implementation of plans related to electronic government and collaborates with the Ministry of Strategy and Finance to ensure budget to carry out the electronic government activities (MOIS, Digital Government Policy and Best Practices of Korea, 2020, p. 63).

In addition, its article 29 stipulate that the MSIT manages affairs concerning the formulation, oversees, coordination, and evaluation of policies on science and technology, and scientific and technological advancements, for instance, MSIT is accountable of establishing the technology development strategy for The Four Industrial Revolution (UN, Member State Questionary Korea , 2020).

<Figure 31. MOIS and MSIT>



Source: MOIS, 2022

Drawing on the above, currently, there are no ministries or organizations in charge of digital transformation in Korea. MOIS and MSIT work only in their own area, they do not collaborate with each other (Chong-sik, 2020, p. 291).

b) Resident Registration Act

Under the Resident Registration Act (hereinafter RRA) enacted in 1962 and in operation until now, every Korean has a unique identification number, Resident Registration Number (hereinafter RRN), granted to all citizens at the time of birth. In other words, every Korean has a personal identification number (Chong-sik, 2020, p. 211). Moreover, according to the article 6 of the RRA, all residents in Korea are subject to a resident registration, within the jurisdiction of Korea, except for aliens (Yoon, 2015, p. 78). Korea has been using RRN for the past 60 years, RRN used to be managed in paper form, however based on the digitization process of the Resident Registration which started in 1977, all the information is managed in digital form through the Resident Registration System (hereinafter RRS) (MOIS, 2022). The RRN aims to provide proper administrative services (public services), know about resident situation and

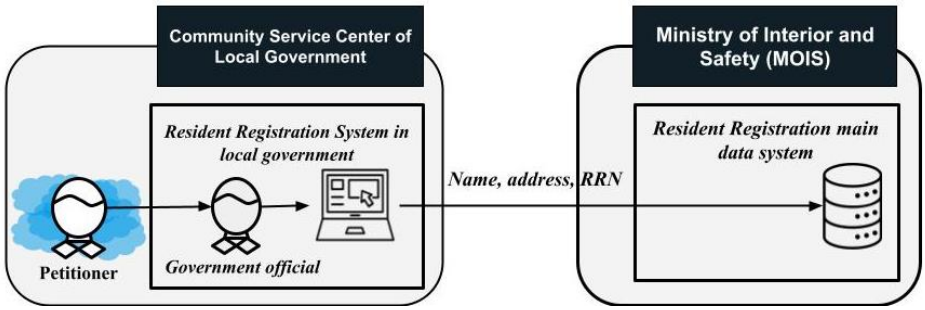
control movement of the population, it is composed of a thirteen-digit system (XXXXXX-XXXXXXX). The first six digits represent date of birth, the next ones represent birth year, gender, issuer agency, birth region's area code, and error correct check digit (Chong-sik, 2020, p. 210). Of course, there are differences in each country, some countries have a numeric identification system and others alphanumeric.

<Figure 32. Resident Registration Number (RRN)>

Source: DID Alliance <https://www.youtube.com/watch?v=4JaS_fONj3U>

Drawing on the above, every Korean already has a digital identity expressed by a number, the RRN is digital by default, and it is the primary key associated with personal information registered in RRS. According to article 28 of RRA the RRS is implemented and maintained by MOIS. Additionally, MOIS is responsible for sharing the resident registration information to other governmental agencies using the interoperability.

<Figure 33. Resident Registration System>



Source: Adapted from Resident Registration Act

Furthermore, according to the article 46 of Enforcement Decree of the Resident Registration Act, MOIS is responsible for authenticating names and resident registration numbers and issuing and delivering resident registration certificates at the request of the head of a district office. However, based on digital security incidents, cybersecurity threats, and cyberattacks, now the gathering or collection of the RRN is only possible when a specific law demanded for digital services, digital transactions, medical treatment, among others.

c) Electronic Government Act

The first electronic government law established in the world, The Korean Electronic Government Act was enacted in 2001 with the purpose to facilitate the realization of electronic government, enhance productivity, transparency, and democracy in the public administration, and improve the quality of life of citizens. It has been the strong legal basis for implementing electronic government projects and developing Korean electronic government, even though most developed countries do not have an Electronic Government Law (Kim S. , The Evolution of Korean E-Government in the perspective of Actor-Network Theory, 2014, pp. 3,28,215).

In that vein, its importance lies in establishing legal dispositions related to enterprise architecture, interoperability, digital signature, digital identity, among others. In terms of digital identity, it is important in article 10 which establishes that to provide an electronic government service, to verify the identity of the applicant is an essential activity.

In addition, according to its article 20, MOIS is accountable for integrating, establishing, managing, and facilitating internet-based integrated information systems to efficiently deliver digital services. In this vein, according to its article 37, MOIS may establish an Administrative Information-

Sharing Center to ensure an effective sharing of administrative information across governmental agencies.

Drawing on the above, based on the Electronic Government Act, the role of MOIS in implementing digital government in the public sector has been clarified and has brought and provided greater order in the digital ecosystem.

d) Personal Information Protection Act

The legal umbrella of this law covers the public and private sector, its purpose is to protect the freedom and rights of individuals by prescribing the processing and protection of personal information. According to its article 3, every provider of information and communications services shall contribute to protection of rights and interests of users and enhancement of users' abilities to use information by protecting personal information of users and providing information and communications services in a sounder and safer way. The authority in charge of overseeing and coordinating the implementation of the law is the Protection Commission.

e) Digital Signature Act

The Digital Signature Act was enacted in 1999, it aims at providing a legal framework for electronic signatures to ensure the safety and reliability of electronic documents. According to its article 2 electronic signature means data in electronic form which are attached to or logically associated with an electronic document for the following purposes (a) To identify the signatory and (b) To verify the fact that the electronic document has been signed by the signatory.

In this line, according to article 8 a certification-service provider may obtain accreditation whether it can comply with established operational standards. A certification-service provider could be a national agency, local

government, or legal person, Basically, with this article the government is opening a new market for private digital certificates providers.

Additionally, according to its article 6, the law establishes that the State shall endeavor to facilitate the use of various electronic-signature-creation devices, such as biometric authentication and blockchain. Nonetheless, the state shall not restrict it to the use of a specific electronic-signature-creation device in the statutes.

Finally, article 14 posits that a certification-service provider shall "verify the identity" of every person who intends to sign up for electronic-signature certification services. Finally, drawing on the above, based on the Digital Signature Act, Korea implemented a Digital Signature Ecosystem, it means there are a set of coordinated organizations, rules, and technology (PKI, Digital Certificates, Applications) operating and maintaining integrity, safety, and reliability of electronic documents, which can be used to promote a digital identity using digital certificates for high risk level of transactions.

f) National Cybersecurity Strategy

The digital environment is playing a protagonist role in social and economic development of Korea, nonetheless, the number of cyberthreats are increasing day by day.

Moreover, disputes among states are escalating and migrating to cyberspace and cybercrime damage to people continues to grow. In that context, the Korean government enacted the National Cybersecurity Strategy in 2019 with the vision to create a free and safe cyberspace to support national security, promote economic prosperity, and contribute to international peace.

From digital identity standpoint, the goal 1 related to ensure stable operations of the state, the principle 1 balance individual rights with

cybersecurity and the strategy 1 Increase the Safety of the National Core Infrastructure are the most associated with the deployment of Digital Identity Scheme, because the Government is encouraged to implement security measures to ensure national information and communication networks and systems, it entails that national platforms like Digital ONEPASS (디지털 원패스) and Government 24 (정부 24) are going to be protected against cyberthreats.

g) Promotion of Information and Communication Network Utilization and Information Protection Act

The Promotion of Information and Communications Network Utilization and Information Protection Act, it is an special law with the purpose of contributing to improving citizens' lives and enhancing public welfare by facilitating utilization of information and communications networks, protecting personal information of people using information and communications services, and developing an environment in which people can utilize information and communications networks in a healthier and safer way. This law establishes in its articles 23-3 and 23-4 the possibility to designate an identification service agency "identification service"; if they comply with designated standards, they can be part of the ecosystem. In other words, in the case of Korea there is a screening process, through which the companies interested in being a digital identification provider need to apply and meet the criteria. All these regulations create a Digital Identity Scheme or Digital Identity Ecosystem with the goal to promote the confidence and security of the users when they interact with digital services.

In sum, drawing on the above, Korea shows a developed digital legal framework, based on what, assigned entities play a key role (MOIS and KCC)

in the digital identity ecosystem, each of them carried out specific activities to ensure gain benefits from the digital technologies (new digital services, new identification services, designed new regulation, among others).

4.1.2 Peruvian digital identity legal framework

a) Political Constitution (The identity is a fundamental right)

The Peruvian Political Constitution issued in 1993, established in its article 2 that every person has the right to his identity, in fact the identity right is the second fundamental right established by the Constitution (RENIEC, National Digital Identity Plan, 2020); additionally, in accordance with its article 183 the National Registry of Identification and Civil Status (RENIEC in Spanish) is the autonomous entity, it means independent of any branch of power, and constitutional body of state in charge of registering births, marriages, divorces, deaths, and other acts that modify civil status, and also is its function to maintain the citizen identification register and issues the documents that prove their identity, the National Identity Card (Documento Nacional de Identidad - DNI in Spanish).

With the issuance of the Political Constitution, Peru ensured the right of every Peruvian to have an identity, it means every person has the right to be recognized as unique and different from others (RENIEC, National Digital Identity Plan, 2020).

Consequently, in a span of years later it made it possible to enact the Organic Law of the National Registry of Identification and Civil Status (Law N° 26497), with the purpose to regulate the functions and structure of the governmental entity in charge of the identification of Peruvian people.

b) Law N° 26497, Organic Law of the National Registry of Identification and Civil Status (RENIEC)

Under the Constitution and its legal umbrella on June 28, 1995, was enacted the Law N° 26497, Organic Law of the National Registry of Identification and Civil Status, which establishes in its article 2 that RENIEC is the entity in charge of organizing and maintaining the "National Identification Registry of Peruvian" and registering the facts and acts relating to their capacity and marital status. For that purpose, it will develop automated techniques and procedures that allow an integrated and effective management of identity information of Peruvians.

Additionally, according to the article 31 of Law N° 26497, RENIEC is in charge of maintaining the essential information's records about all Peruvians (name, civil status, date of birth, photography, gender, identification unique code, address, among others). Based on this information, RENIEC issues the National Identity Card (DNI), which according to the article 26 is public, personal, and not transferable.

It is the only personal identity card for all civil, commercial, administrative, judicial acts and, in general, for all those cases in which, by legal mandate, it must be presented. It also constitutes the only title of right to vote of the person in whose favor it has been granted.

Drawing on the above, by 2020, according to RENIEC's annual report, 98.9% of the Peruvian population is part of the register and all of them have a National Identity Card (RENIEC, Memoria Institucional 2020, 2020).

c) Digital Government Authority

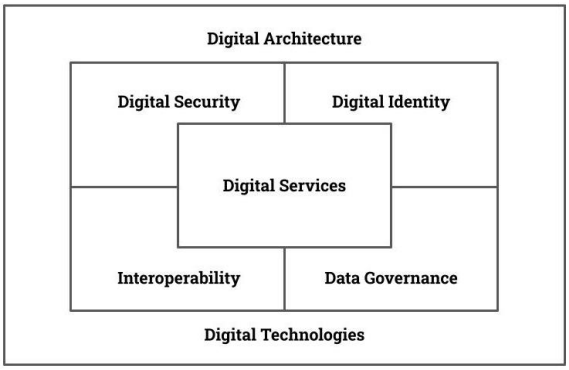
Based on Ministerial Resolution N° 156-2021-PCM, the Government and Digital Transformation Secretariat is the body of the Peruvian State responsible for the government, supervision, and control of the deployment of

government and digital transformation in the country. Having among its responsibilities the conduction and deployment of digital identity at the national level. Additionally, according to article 8 of the Digital Government Law, The Presidency of the Council of Ministers, through the Secretariat of Digital Government, is the governing body in matters of digital government that includes technologies digital, digital identity, interoperability, service digital, data, digital security, and digital architecture. Dictate rules and establishes procedures in matters of digital government and is responsible for its correct operation.

d) Legislative Decree N° 1412, Digital Government Law

On September 13, 2018, the Digital Government Law, Legislative Decree N° 1412, was enacted with the purpose of establishing a framework for the proper management of digital identity, digital services, digital architecture, interoperability, digital security and data, as well as establishing the legal regime applicable to the transversal use of digital technologies in the digitization of processes and provision of digital services by Public Administration entities at the three levels of government (national, regional and local).

<Figure 34. Digital Government Law>



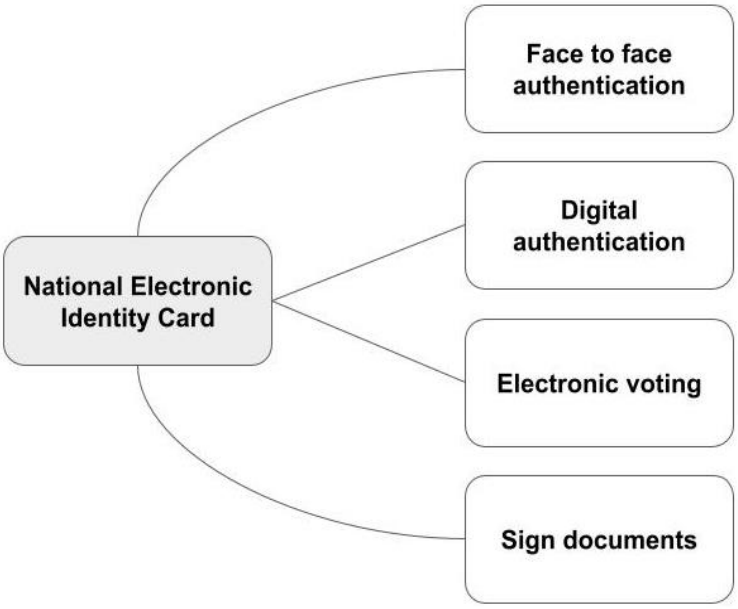
Source: Legislative Decree N° 1412, Digital Government Law

The law establishes in its article 10 that digital identity is a set of attributes that individualizes and allows to identify a person in digital environments.

Additionally, it refers that the attributes of the digital identity are granted by different entities of the Public Administration that, taken together, characterize the individual. Another aspect to highlight of the Digital Government Law is that it enables the possibility that public officials and servants can use the National Identity Card for the exercise of their duties and public functions, that is, to sign documents and reports in the processes and services provided to the citizen.

It is relevant to mention that Peruvian citizens can use the National Identity Card for authentication process in face-to-face and non-face-to-face environments and electronic voting.

<Figure 35. National Electronic Identity Card benefits>



Source: Legislative Decree N° 1412, Digital Government Law, 2022

e) Signatures and digital certificates law

The Signatures and digital certificates law was enacted in 2000 with the purpose of regulating the use of the electronic signature, granting it the same validity and effectiveness as the use of a handwritten or similar signature that entails a manifestation of will. Under this law we understand an electronic signature as any symbol based on an electronic means used or adopted by a party with the precise intention of binding or authenticating a document fulfilling all or some of the functions. In this sense, it established a legal framework to organize roles, processes, rules, and technology to create a digital signature ecosystem.

f) Supreme Decree N° 029-2021-PCM, Digital Government Law Regulation

Consistent with the above, in 2021 through Supreme Decree N° 029-2021-PCM the regulation of the Digital Government Law was issued, this legal instrument establishes the governance and coordination mechanisms for the deployment of digital government in public administration in the different sectors and at all levels of government (National, Regional and Local).

Additionally, the regulation creates digital platforms as central building blocks in the digital architecture of the Digital Peruvian State, and in this way promote the implementation of a Government as a Platform, that is a model in which typically the user interacts with the government through web pages or mobile applications every time, everywhere, using every device (World Bank, 2016). The transversal platforms created under the Supreme Decree N° 029-2021-PCM are:

1. GOB.PE, It is the official electronic government portal at national level.

2. National Platform for Identification and Authentication of Digital Identity (ID GOB.PE): digital platform used to authenticate the digital identity of a citizen or person in general.
3. National Interoperability Platform (PIDE in Spanish), platform used to share data and information between public entities.
4. National Platform for Digital Signature (FIRMA PERÚ): digital platform that allows the creation and validation of digital signatures.
5. Cloud Services Peru (NUBE PERÚ), digital platform that takes advantage of cloud computing, such as economies of scale and flexibility and elasticity, seeking to provide local governments and other entities with the necessary and suitable infrastructure for the deployment of digital services**.**

Likewise, this regulation establishes measures to ensure confidentiality, integrity, and availability of the information, among which we have: the establishment of a digital security officer and data privacy officer, and the implementation of the standard ISO 27001.

g) Law N° 29733, Personal Data Protection Law

Based on the Law N° 29333, Personal Data Protection Law, the Government of Peru creates a framework to guide the establishment of technical, organizational, and legal measures to protect the personal information storage by public and private organizations when they carry out transactions with the citizens.

Drawing on the above, Peru shows a progress in its digital legal framework, basically because the issuance of the Digital Government Law, however, the enforcement of it and its implementation are big challenges in the short and long term.

h) Digital Security and Trust Framework

In terms of Digital Security, through Supreme Decree N° 029-2021-PCM and Supreme Decree N° 157-2021-PCM, the public administration must implement standard ISO 27001, report digital secure incidents to the Digital Security National Center, assign a Trust and Security Digital Officer.

Additionally, the Government enacted Urgence Decree N° 007-2020, with the intention to create a Digital Trust Framework composed of three main domains a) digital security, b) consumer protection online and c) personal data protection.

i) National Digital Transformation System

The Government enacted Urgence Decree N° 006-2020, with the intention to create a National Digital Transformation System which is made up of a set of principles, norms, procedures, techniques, and instruments through which the activities of the public administration are organized and the activities of companies, civil society and academia are promoted, aimed at achieving the country's objectives in terms of digital transformation.

According to its article 7 the Presidency of the Council of Ministers, through the Digital Government Secretariat, is the governing body of the National Digital Transformation System, becoming the national technical-regulatory authority on the matter.

4.2 TECHNOLOGY

The ICT infrastructure, hardware, software, algorithms, digital signature, and data are a key element in implementing and maintaining a digital identity scheme. In this section, we are going to evaluate the main ICT

components developed by Korea and Peru to create a Digital Identity Scheme, such as government enterprise architecture, one stop electronic government service portal, digital authentication service, data center, interoperability platform and open data portal.

As we noted in the previous chapters, digital technologies provide a variety of capabilities to the Digital Identity Solutions such as security, scalability, availability, and efficiency.

4.2.1 Digital Identity Technology in Korea

a) Government Enterprise Architecture (GEA)

In 2007, the Government Enterprise Architecture project started under the direction of the Ministry of Security and Public Administration, the purpose of it was to manage the information resources effectively and efficiently by preventing the overlap of resources (Kim S. , The Evolution of Korean E-Government in the perspective of Actor-Network Theory, 2014, p. 45)

To date, according to the article 45 of the Electronic Government Law, MOIS is responsible for developing the Information Technology Architecture. Additionally, in accordance with the articles 4, 5 and 46 of the Law, every agency shall introduce, operate, and maintain an information technology based on the standards approved by MOIS.

The benefits of maintaining an information technology architecture are re-use of technology components, save time in software development, avoid overlapping systems, facilitate the sharing administrative data among agencies (interoperability) (Korea Law Information Center, 2022).

According to the Government Enterprise Architecture Portal (EA Portal), the Government Architecture has five (05) layers Performance Reference Model (PRM), Business Reference Model (BRM), Service

Reference Model (SRM), Data Reference Model (DRM) and Technical Reference Model (TRM). TRM defines technology standards and supports the environment for secure exchange of administrative works and the compatibility between organizations (Kim S. , The Evolution of Korean E-Government in the perspective of Actor-Network Theory, 2014, p. 44).

In the context of Digital Identity, the importance of the GEA lies in the fact that it promotes the common use of standards among agencies. For example, if one digital public service wants to integrate KAKAO, for authentication, they need to use OpenID Connect.

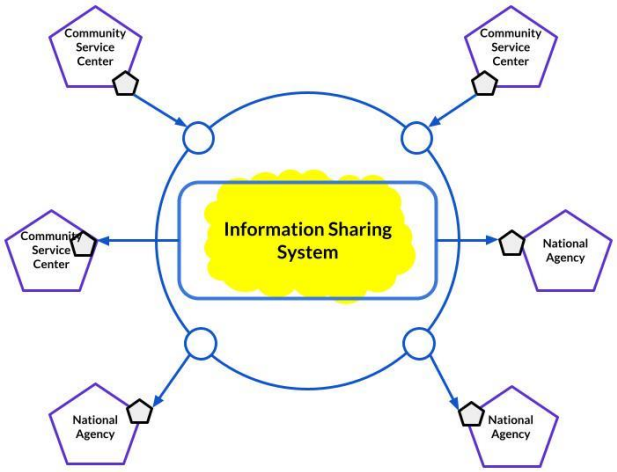
b) Public Information Sharing System (하나로민원)

Based on the Electronic Government Act, MOIS implemented a public information sharing system **(하나로민원)** which is a service that safely distributes administrative information between public agencies and financial institutions.

There are at least three ways to share the information using this platform: a) real time information distribution, b) mass information distribution and c) fact check.

a) Real time information distribution, the user organization gets information in real time from another entity who is responsible to maintain it.
b) Mass information distribution, the distribution of information is periodically, gather information of a certain size and then in a batch format deliver it through the platform.
c) Fact checks, a service that just answers and confirms petitions about facts, the public agencies, basically, just express in real time Yes or No based on the information maintained in their systems.

<Figure 36. Information Sharing System>



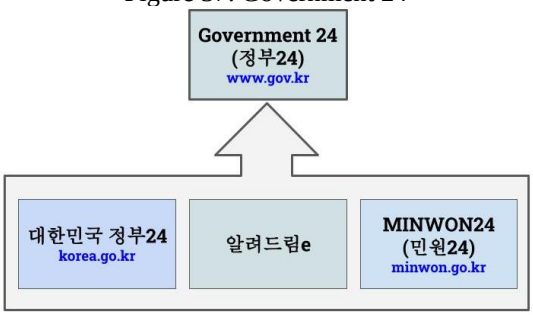
Source: Own developed, 2022

c) One Stop Service Portal - Government 24 (정부 24)

With the purpose to provide a convenient and single portal for citizen requirements, an ease access to digital services and integrate relevant information about the public services in just one point of contact, MOIS implemented a one stop electronic government service portal, which is called Government 24 (**정부 24**), whose online address is www.gov.kr.

Government 24 (GOV24) is the result of the integration of three (03) portals MINWON24 (민원 24), 알려드림 e and 대한민국 정부 24.

<Figure 37. Government 24>



Source:
https://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=55292

To date GOV.24 provides public services (search engine of the government), information about public policies, news about the official activities of the government, and one point to access and processing digital public services (MOIS, Digital Government, 2022).

Drawing on the above, if we use GOV.24, we can access to different kind of digital services (non-face-to-face) using different type of digital authentication methods such as:

a) Certificate-based authentication which has two kind of ways, one is simple authentication (간편인증) and the other is digital certificates-based authentication (공동금융 인증서),

b) Digital One Pass (디지털원패스)

c) Biometrics-based authentication.

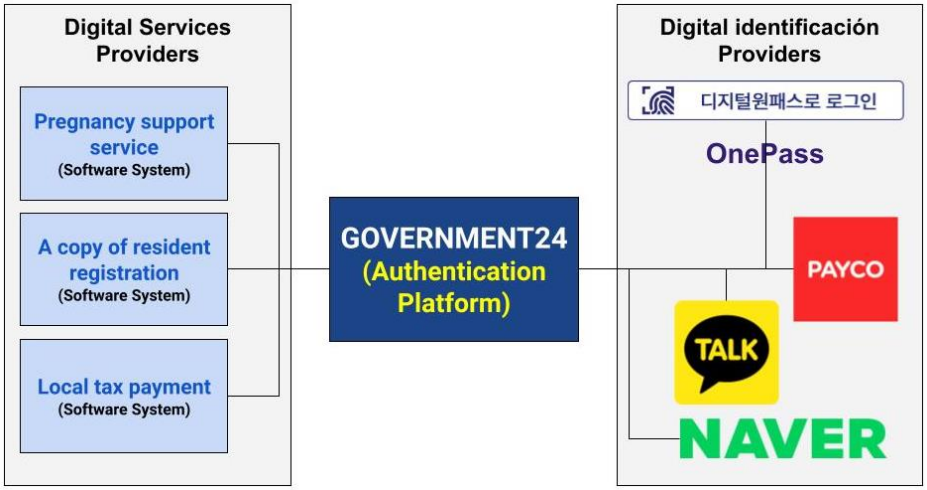
d) Username and password-based authentication, in the case of authentication based on an ID (아이디), Korean citizens must first register using their national identity number, which is validated by GOV.24, after which they must accept its terms and conditions and, finally, accept the personal information collection clause.

All these different kinds of authentication methods are possible because there is a Digital Identity Scheme working under scene.

Regarding services, GOV.24 has, to date, approximately ninety thousand services (90K), corresponding to twelve (12) sectors. The platform makes heavy use of interoperability (하나로민원).

To request services in GOV.24, citizens must authenticate through one of the available methods.

<Figure 38. Government 24>



Source: https://www.gov.kr/nlogin/?Mcode=10003

d) Digital OnePass (디지털 원패스)

Digital ONEPASS is a digital authentication service provided by MOIS that allows Koreans to use various digital services trustworthy and conveniently with various authentication methods (fingerprint, face, patter, i-PIN, join certificate “digital certificates”, SMS, among others) selected by the user.

Furthermore, the user has the autonomy to select the digital public services that will have Digital ONEPASS as their authentication platform. Currently, about two hundred and seven (207) digital services can be accessed using Digital ONEPASS.

<Figure 39. Digital Services available in Digital OnePass>

선택	그룹명 ▲	기관명 ▲	서비스명 ▲	서비스설명
☐	경제금융	고용노동부	월드잡플러스	월드잡플러스
☐	경제금융	고용노동부	근로복지공단 퇴직연금시스템	공단 퇴직연금 소개, 사업장/담당자 관리, 플랜정보관리, 가입자관리, 계약정보 조회, 가입자 교육, 운용지시, 지급신청, 상품별 잔고조회, 퇴직연금현황, 적립금운용현황, 지급진행조회, 증명서 발급 등
☐	경제금융	공정거래위원회	한국소비자원	소비자 민원상담 및 피해구제, 보상규정, 교육프로그램, 법령, 보호시책 제공.
☐	경제금융	공정거래위원회	기업집단포털	기업집단포털

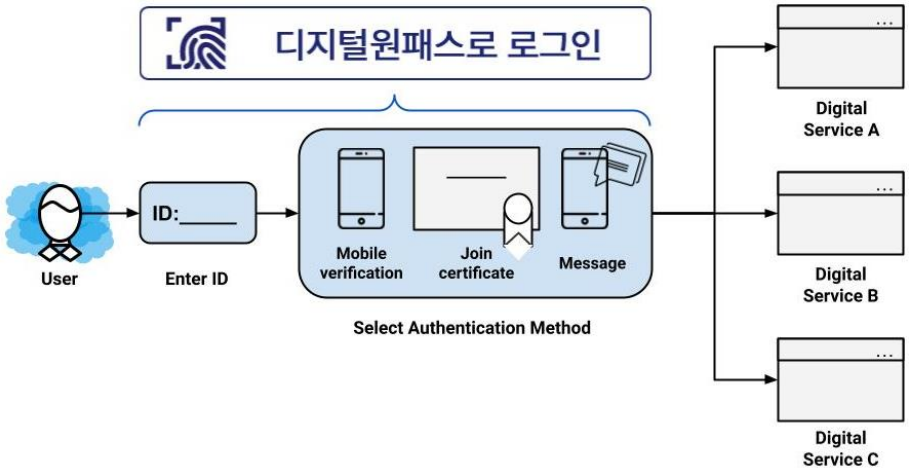
Source: <https://www.onepass.go.kr/about>

Digital ONEPASS is constituted as a digital authentication service (Digital Authentication One Stop) that seeks to solve the risks to digital security that comes with having independent authentication services, that is, authentication services by service or by entity. The risks can be unauthorized disclosure of information, loss of reserved information such as usernames and passwords, identity theft, etc.

We can point out that Digital ONEPASS seeks to replace the use of certificates and the i-PIN for online user authentication.

For integration purposes, Digital ONEPASS uses open-source libraries and Application Programming Interface (API), thereby ensuring interoperability and information exchange.

<Figure 40. Digital OnePass>



Source: <https://www.onepass.go.kr/about>

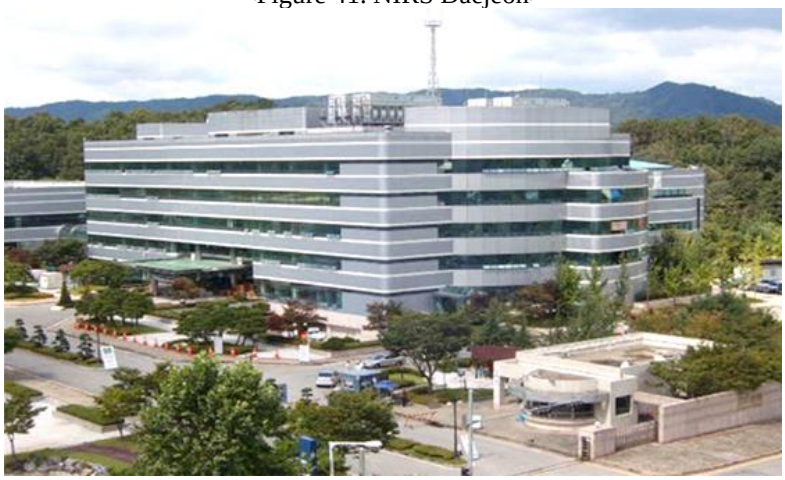
Its design began in 2017 and its implementation took almost two (02) years, in 2020 there were already 15 million users. In 2021, the FIDO (Fast Identity Online) standard was incorporated to allow fingerprint authentication and to date (2022) it has approximately 207 services integrated into it and has a mobile version. Digital ONEPASS is administered by MOIS, and it can be accessed through the following link https://www.onepass.go.kr

If one governmental agency wants to use the Digital ONEPASS, they should apply through an official letter to MOIS.

e) National Information Resource Service (NIRS)

Seeking to find a solution for different kinds of issues such as redundant investment in ICT, cyber incidents, problems to hire information security experts, increasing demands for good quality and best performance of digital public services, and lack of digital resources (hardware, software, and facilities), the government implemented an exclusive Data Center. The Data Center integrates data and information of central governmental institutions, it took advantage of the development started in 2003 with the Information Strategy Plan, after that in 2005, Daejeon Center implemented, time later, in 2007, Gwangju Data Center implemented, time goes on and in 2011, the G-Cloud Computer platform was deployment, and in 2015, the Big Data Division Starts to operate (NIRS, 22). According to the interviews with specialist G-CLOUD provides Infrastructure as a Service (IaaS).

<Figure 41. NIRS Daejeon>



Source: <https://www.nirs.go.kr/eng/contact/contact_02.jsp>

To date, the Data Center is under the administration of National Information Resource Service (NIRS), which was implemented in 2019 and covers all the resources above mentioned (UN, E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development, 2020, p. 196). The operation of the National Information Resources Service (NIRS) is based on ITIL (IT Infrastructure Library) and ISO 20000 Service Management, both are well-known standards in the IT Industry (NIRS, 22).

Understanding that the number is not important, it is known that only one Korean data center has more than 10000 servers.

f) Open data portal

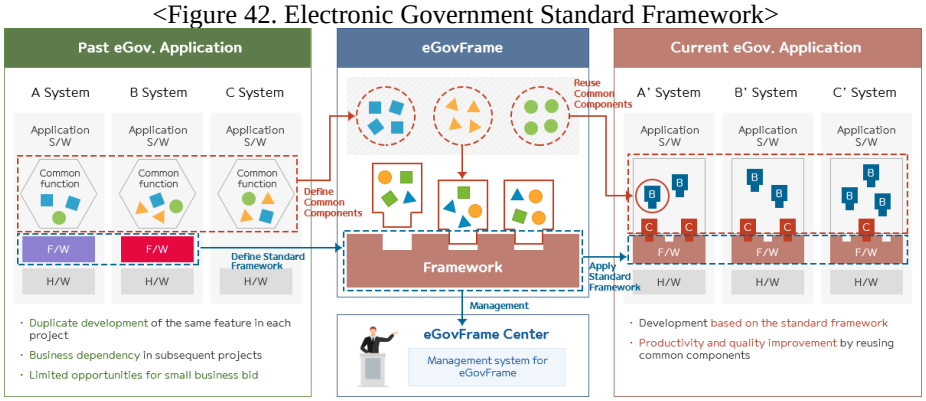
According to article 21 of the Promotion of the Provision and Use of Public Data, MOIS is in charge of implementing, managing, and promoting an open data platform (data.go.kr) for the provision of open government data (OGD). We can understand open government data like data open to and available in the public domain in various (including machine-readable) formats and normally licensed for all to access, use, modify and share; all OGD are government data.

Drawing on the above, Korea shows a striking progress in its digital technology infrastructure at national level, the Government Architecture, the National Information Resource Service (Data Center) and One Stop Service Portal (Government 24) are the cornerstones in its digital transformation, all of them approximately demanded 111 million dollars but the benefits (scalability, security, availability, etc.) are bigger than this.

g) Electronic Government Standard Framework (Egov-Frame)

With the purpose of increasing interoperability, resolving vendor dependency, adopting latest ICT trends, and reusing common features, MOIS developed a specific platform for developing IT projects in the public sector in Korea. The envision of the framework is improving service quality of electronic government and increasing efficiency of ICT investment. To do that, MOIS has established three (03) strategies a) standardization, b) openness, and c) community. Standardization means to establish software standards for electronic government projects and provide a trustworthy ICT infrastructure. Openness means the assets are open to the public, and Community refers to expanding and spreading the idea behind egov-frame through all public administration. There are different kinds of problems in the software development, for instance various development frameworks are used, therefore it is hard to manage the versions, and difficult to maintain the software without vendor's technical support (vendor dependency). Egov-Frame deals with these issues and promotes the standardization, reusability, and interoperability of components (MOIS, egov-frame Portal, 2022).

<Figure 42. Electronic Government Standard Framework>



Source: <https://www.egovframe.go.kr/eng/sub.do?menuNo=7>

Egov-frame establishes standards and best practices for presentation, business, data, integration, and development layers. Likewise, it establishes the software license that was secured, in this case Korea adopts the Apache License 2.0.

- Presentation layer: Ajax support, Internationalization, among others.
- Business layer: Process management
- Data layer: Data access and object relational mapping
- Integration layer: Web Services, Messaging Services
- Development layer: UX/UI Component and Device API

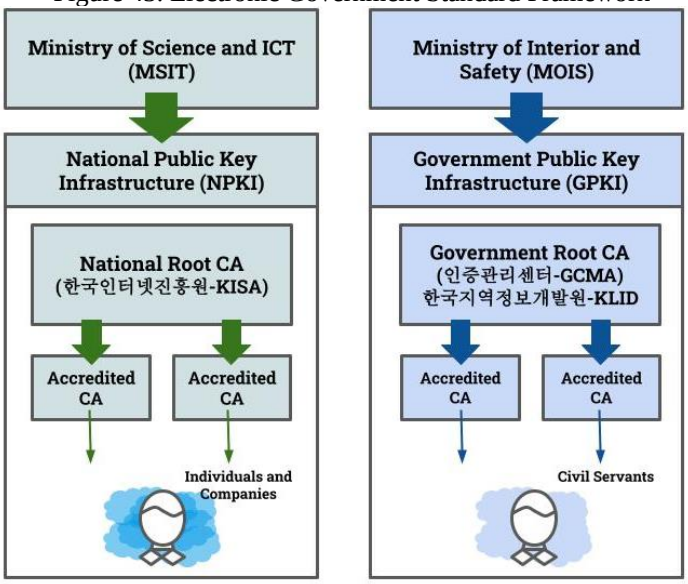
h) Public Key Infrastructure

The National Public Key Infrastructure (NPKI) was established in 1999 under the framework of the Electronic Signature Act, which establishes provisions for the a) accreditation of certification entities, b) operation of entities of certification, c) monitoring of certification entities and, d) Statements of certification practices (Certification Practice Statements).

The NPKI Competent Authority is the Ministry of Science and Information and Communications Technology (MSIT) and the Root CA is the Korea Internet and Security Agency (한국인터넷진흥원-KISA).

The main clients of the NPKI are natural persons and companies. At the beginning, there were only five certification entities (CA), but to date, with the changes established in the Electronic Signature Law, there are at least 50 certification entities and approximately 41 million subscribers.

<Figure 43. Electronic Government Standard Framework>



Source: <https://www.egovframe.go.kr/eng/sub.do?menuNo=7, 2022>

The Government Public Key Infrastructure (GPKI) was established in 2001 within the framework of the Electronic Government Act, its implementation took around six (06) months. The Government Public Key Infrastructure (GPKI) is a hierarchical structure, which has as its Competent Authority the Ministry of the Interior and Security (MOIS) and as Root Certification Entity the Government Certification Management Authority (인증관리센터- GCMA-KLID). Under the GCMA-KLID are the Certification Entities (CA) and Registration Entities (RA). To date, the GPKI has twenty-five Certification Entities (CAs).

The responsibilities of the Root Certification Authority for the GPKI, 인증관리센터-GCMA-KLID, are the following: a) Validation of certificates, b) Encrypt public keys, c) Issue digital certificates, d) Confirmation of identity and e) Verification of the authenticity of electronic documents. Currently, the MOIS has delegated certification services to the Korea Local Information

Research and Development Institute (한국지역정보개발원-KLID), an entity attached to it.

The main clients of the GPKI are public servers. To date there are at least 25 certification entities in the GPKI. RAs can be Ministries and local governments.

i) Open Cloud Platform (PaaS-TA)

PaaS-TA is the Korean Framework to boost the adoption of cloud services and foster competitiveness in the cloud platform market. PaaS-TA is made by NIA with domestic software companies and with the support of the Ministry of Science and ICT. PaaS-TA is an open source-based platform. PaaS-TA was released in april 2016, and nowadays it plays a key role in providing standard development and operating environment for cloud-based digital services.

The benefits granted by using PaaS-TA are a) infrastructure dependency, b) automatic scaling of Virtual Machines and containers, c) integrated monitoring from infrastructure to application services, d) integrated security, e) promote domestic solutions, f) reduces IT costs and g) rapid development and testing of digital services and applications.

From a technical standpoint, PaaS-TA provides container platforms, storage servers, database management systems, application platforms, open platform for integrating microservices, authentication services to provide user authentication management, load balancer, Application Program Interface (API), services as well as development and operation tools.

Finally, periodically NIA offers training courses to strengthen the knowledge about PaaS-TA among ITC specialists and practitioners.

4.2.2 Digital Identity Technologies in Peru

a) Digital Authentication Platform (ID.GOB.PE)

With the issuance of Legislative Decree N° 1412, which approved the Digital Government Law, digital identity is incorporated as one of the components of digital government, probably the most important. The law develops in its articles 13 and 14, the concepts of digital identification and authentication respectively.

The digital identification refers to "… the procedure of recognition of a person as different from others, in the digital environment. Public entities should establish the procedures for identifying the people who access the services digitally", while the second one, the authentication is defined as "… the procedure of verification of a person's digital identity, through which it can be affirmed that he is who he says he is. For access to a digital service, entities of the Public Administration must adopt the mechanisms or digital authentication procedures, considering the security levels to be established in the standard regulatory".

The law understands that they are different but complementary processes. Already with the issuance of the Regulation of the Digital Government Law, through Supreme Decree N° 029-2021-PCM, the Digital Identity Framework for the Peruvian State is created, which has as one of its components the Digital Authentication Platform (**ID GOB.PE**). This platform is managed by the Government and Digital Transformation Secretariat, however, is not implemented yet.

b) Single Point of Contact or National Portal (GOB.PE)

In the case of Peru, the single point of contact, sometimes called one stop shop, was created by Supreme Decree N° 033-2018-PCM in 2018, the

Single Citizen Orientation Portal (GOB.PE) integrates in a single point of contact information from the Peruvian state, its policies, and interventions, as well as access to digital public services. The State has an authentication platform, but intensive integration with digital public services has not yet been developed. It is expected that after the issuance of the Digital Government Law and its enforcement regulations, this component can be accelerated. This portal is managed by the Government and Digital Transformation Secretariat.

c) Open data portal

With the issuance of Supreme Decree N° 016-2017-PCM, the open data strategy and model in the Peruvian State is approved, and the Open Data Portal is also created. The Open Data Portal is managed by the Secretary of Government and Digital Transformation. To date, the portal provides information in CSV or XLS file formats, however, the current trend is to provide them through APIs so they can be processed by machine.

d) National Digital Government Platform (PNGD in Spanish)

Based on a loan with the Inter-American Development Bank (IDB), the Government and Digital Transformation implemented in 2022 the National Digital Government Platform (PNGD in Spanish).

PNGD constitutes a private cloud for public entities, which will provide cloud-based services such as Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). IaaS refers to the provision of computational storage capacity (virtual servers); on the other hand, SaaS refers to the provision of capabilities for application development, such as application servers and databases, ensuring their high availability and scalability. These capabilities are based on

clustering and container orchestration platform. PNGD has 10 hyperconverged servers, and a storage capacity of 1000 Terabytes.

e) National Interoperability Platform

The National Interoperability Platform is a building block of the digital transformation process in Peru, basically is an intermediary layer used to share information amongst public entities. Technically, it uses the SOAP and REST protocols to share information.

The National Interoperability Platform is administered by the Government and Digital Transformation Secretariat. Currently, around 90 entities are sharing information through this platform. The benefits of it are reduction of paper, more agile and dynamic digital services development and saving time and effort exchanging information entity by entity, making agreements which is a lot of effort in time and money.

j) Public Key Infrastructure

The Official Electronic Signature Infrastructure (IOFE) emerged with the issuance of the Digital Signatures and Certificates Law in 2002, which was then regulated in 2008 by Supreme Decree No. 052-2008-PCM. The IOFE is constituted by a set of procedures, technology, actors that seek to guarantee the security of digital signatures in public services and electronic commerce with a view to generating trust in the digital environment.

In the case of Peru, the Competent Administrative Authority (AAC) is the National Institute for the Defense of Competition and the Protection of Intellectual Property (INDECOPI), whose responsibilities include accrediting and supervising the Certification Entities (CA), Registration Entities (RA) and

digital signature software products. Consistent with the foregoing, INDECOPI maintains an Official Registry of Digital Certification Service Providers, which is publicly accessible. The registry is available in human-readable (PDF) and machine-readable (XML) versions.

In the case of the private sector, there is no root certification authority (Root CA); however, every certification entity must be accredited by INDECOPI if they want to offer products and services in Peru.

In the case of public entities, a Government Public Key Infrastructure (GPKI) has been established, which is a hierarchical structure, it has as its Competent Administrative Authority, INDECOPI, and as Root Certification Entity (Root CA) the Government and Digital Transformation Secretariat.

Drawing on the above, Peru shows a slow progress in its digital technology infrastructure at national level, the Digital Government Architecture is regulated by the Digital Government Law, but it is not implemented yet, and the Data Center it continues like an idea in the national digital agenda.

4.3 GOVERNANCE AND LEADERSHIP

The implementation of digital government entails the overall transformation and innovation of the government, it means in essence new ways of operation, redesign administrative process, change in administrative functions, structures, and civil servants' awareness, that is why it is a complex, difficult and steady process. We need the leadership of the top leaders, which is embodied by establishing a clear vision of digital government implementation, based on that, specific strategies, action plans, governmental bodies must be implemented in order to achieve the goals and objectives of the vision (Chong-sik, 2020, pp. 177,178).

We are going to analyze aspects related to the digital government and digital identity as part of the digital agenda beyond the individuals' boundaries of administrative agencies or branches of power, another important aspect to know which institutional arrangement is established to support the implementation of digital government projects.

a) Political leadership in Korea

According to the Government Organization Act and Electronic Government Act, MOIS, at national level, is the governmental body in charge of handling all the administrative affairs of the digital government, promoting digitalization of administrative processes among administrative agencies, sharing of information among administrative agencies, implementing electronic government projects and supporting the export of electronic government knowledge.

It means, basically, that MOIS is responsible for the digital government in the public sector and takes the leading role implementing and leveraging technologies for digital identity initiatives and projects to ensure a safety and ease interaction between citizens and government in the digital environment.

In addition, to get the full picture about digital identity governance in Korea, we must talk about the role of key Korean entities: Korean Internet & Security Agency (KISA), Korea Local Information Research Development Institute (KLID), National Information Agency (NIA) and Korea Communication Commission (KCC).

Firstly, KISA is an entity responsible for the Root CA of the National Public Key Infrastructure (NPKI) and cybersecurity issues in the Korean society, which includes the public and private sector.

Secondly, KCC, the governmental body in charge of the identification service provider selection process. We must notice that with the approval of the KCC, a new actor joins the Korean Digital Identity scheme.

According to article 72, KLID is an entity under MOIS responsible for implementing digital government in local governments (provinces and municipalities), following the policies and guidelines issued by MOIS, for instance, KLID is in charge of overseeing and implementing ON-NARA System (Korean National Document Management System) and managing the Government Public Key Infrastructure (GPKI).

Finally, it's important to mention the role played by the National Information Society Agency (NIA), which was founded as the National Computerization Agency in 1987, authorized to provide technical consulting services for electronic government in 2001, and designated as the chief managing body of Korea's electronic government projects in 2004 (Dongsung Kong, 2015, p. 63).

Additionally, in line with the article 10 of the Framework Act of Promoting Informatization and to support development of related policies for national agencies and local autonomies, NIA is specialized in national informatization, the informatization of local governments is responsible of KLID. NIA supports the distribution of services through implementation of electronic government projects. In this line, according to the articles 13 and 14 of the Enforcement Decree of the Framework Act on National Informatization, the NIA can carry out projects of national agencies when required by them.

Finally, one of the key factors for the good performance of the MOIS has to do with its close collaboration with the Ministry of Strategy and Finance (MOIS, Digital Government Policy and Best Practices of Korea, 2020, pp. 63, 66).

Table 20. Actors of Digital Transformation process in public sector of Korea

Entity	Description
MOIS	Leader of Digital Transformation in public sector.
KISA	Cybersecurity issues Root CA of the National Public Key Infrastructure (NPKI) Internet issues.
NIA	Federal ICT Solutions.
KLID	Local Government Solutions. ON-NARA System (Document Management System). Root CA of Government Public Key Infrastructure (GPKI).

Source: Own development, 2022

Drawing on the above, Korea shows a reasonable distribution of roles and duties to design, implement, and oversee the Digital Government process in Korean society. In other words, Korea shows that policy design and ICT solutions implementation can be handled by different coordinated organizations.

b) Political leadership in Peru

In the case of the Peruvian State, based on Supreme Decree No. 118-2018-PCM, we have a High-Level Committee for the development of the Government and Digital Innovation in the country, made up of the main Ministries; but in practice, its operation becomes difficult and complicated since agendas and interests must be reconciled.

On the other hand, the one who does have a leading role is the Government and Digital Transformation Secretariat, which seeks to coordinate the interests of different sectors in digital matters (digital security, cybersecurity, digital identity, document management), likewise, it is responsible for the implementation of transversal platforms, and establishing spaces for coordination with private actors and academies.

Drawing on the above, Peru shows an unreasonable concentration of roles and duties to design, implement, and oversee the Digital Government

process in Peruvian society. In other words, Peru does not have an efficient institutional arrangement to deal with digital transformation challenges.

4.4 BUDGET

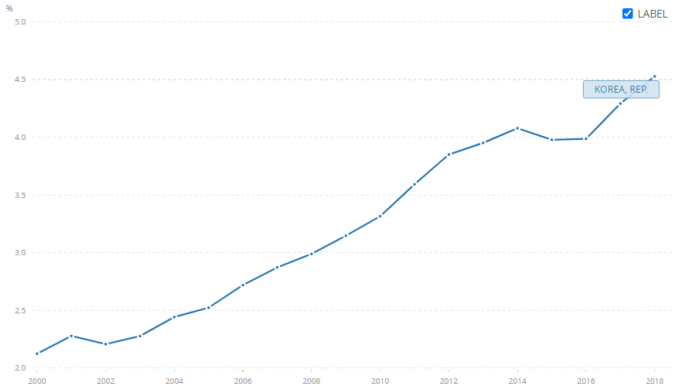
a) Korea

Besides political commitment, the Korean government allocated the necessary budget for the implementation of electronic government projects, a budget that has been increasing due to the benefits obtained both in terms of efficiency, competitiveness, and quality of life of its citizens.

In 2000 Korea invested approximately 2.13% of its Gross Domestic Product (GDP) in Research and Development (R&D), more than 19 times what Peru invests today.

This was gradually increased to 3.15% in 2009, until reaching 4.53% in 2018. It is logical to think that the Asian country's commitment to investment in research and development played an important role in the increase in its GDP (UTEC, 2022). As of 2017, we see that the Asian country increased its GDP per capita 36 times, reaching 30 thousand dollars per year, while our country increased it only 7 times, only reaching over 6 thousand dollars.

<Figure 44. Research and development expenditure (% of GDP) in Korea>



Source: World Bank (2000-2018), Link:
<https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=KR&view=chart>

Additionally, presently Korea is using private companies for Research and Development (R&D) using the Public Private Partnership Model (PPP model).

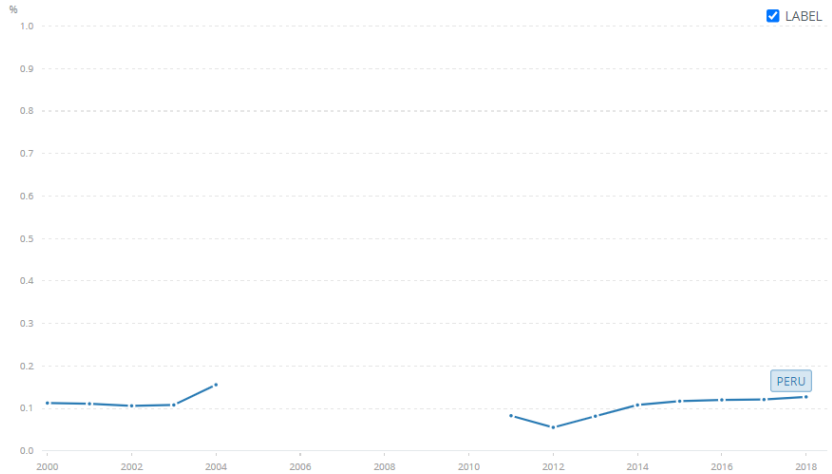
b) Peru

In the case of Peru, the investment on research and development as a percentage of the GDP is one of the lowest in the world and there has not been a big variation since 2000.

In 2000, Peru invested approximately 0.11% of its Gross Domestic Product (GDP) in Research and Development (R&D), and in 2018, it is almost the same (0.13%).

Logically to think about the reasons why Korea increased its GDP per capita 36 times, reaching 30 thousand dollars per year, while Peru increased it only 7 times, only reaching over 6 thousand dollars.

<Figure 45. Research and development expenditure (% of GDP) in Peru>



Source: World Bank (2000-2018), Link: <https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=PE&view=chart>

4.5 MARKET

a) Korea

In the case of Korea, based on the legal umbrella of the Promotion of Information and Communications Network Utilization and Information Protection Act and considering the fierce competition in the digital market, the three mobile carriers (SK Telecom, KT, and LG U+), Kakao, Naver, are entering to provide identification service. Moreover, presently the Korean government give a permission to six private companies a) Nice Information Service, b) Korea Credit Bureau, c) Korea Mobile Certification, d) Korea Mobile Certification and e) NHN KCP Corporation to provide mobile authentication service and related services.

b) Peru

In the case of Peru, we don't have the legal umbrella to approve private identification services provider, that is why, there are no private identification services, every business, financial entity, and even public entities remain using their own identification (user and password, application, fingerprints, among others).

4.6 FINDINGS

Although Korea still maintains the name Electronic Government, and Peru utilizes the name Digital Government, in practical terms they cover the same topics such as digital signature, digital identity, interoperability, digital security, digital services, and digital architecture.

In that sense, we are going to describe the main findings in legal framework, technology, governance, budget, and market as a component of the Digital Identity Scheme (ID Scheme).

a) Legal framework

Analyzing the legal framework, we observe that: Korea has a regulation with a national enforcement (Government Organization Act), It assigns the responsibility of directing, coordinating, and supervising the electronic government to MOIS. In the case of Peru, it also has a legal framework (Digital Government Law and Urgence Decrees No. 006-2020 and No. 007-2020), that assigns responsibility for digital government and digital transformation to the Presidency of the Council of Ministers, through the Government and Digital Transformation Secretariat.

Korea does not have an entity in charge of digital transformation at national level, in Korea, there is no entity that leads the digital transformation at the national level, it is still a pending issue that involves the articulation and coordination of two (02) entities: MOIS and MSTI.

However, something remarkable in Korea and very different from Peru is that Korea has ICT specialized agencies such as NIA, KLID, KISA and KCC to cope with the challenges of digital transformation and provide technical assistance in developing ICT solutions. NIA is the governmental entity responsible for supporting the digital government strategy (including digital identity initiatives) established by MOIS and MSIT at federal level, KLID is an entity under MOIS responsible for implementing digital government in local government, KISA is an entity responsible for the Root CA of the National Public Key Infrastructure (NPKI) and cybersecurity issues in the Korean society.

In the case of Peru, the Government and Digital Transformation Secretariat is responsible for designing policy and implementing it. Looking at Korean experience, the segregation of functions brings agility and flexibility in developing solutions. ***MOIS is a political actor, while NIA, KLID and KISA***

play a technical role in developing digital identity and digital transformation initiatives in Korea.

Peru has an entity in charge of digital transformation at national level, through Urgence Decree N° 006-2020, the responsibility of directing, coordinating, and supervising the digital transformation at the public and private sector level was assigned to the Presidency of the Council of Ministers, through the Government and Digital Transformation Secretariat.

There are differences between Peru and Korea, however there are also similarities, one of them is, for instance, that ***the citizens of Korea and Peru have a personal identification number, which is an essential element of their digital identity***, based on Resident Registration Act (RRA), every Korean has a Resident Registration Number (RRN), which is stored in the Resident Registration System (RRS). In addition, even when the head of the province (도), Metropolitan city (광역시) and County (군) is body responsible for initiating the registration process of a new resident, all this information is stored in RRS which is administered by MOIS. In the case of Peru, based on Law N° 26497, every Peruvian must have a National Identity Card and the law has set that RENIEC is the entity in charge of issuing it and maintaining the National Registry of Identification.

Digital identity is a political and legal issue more than technical, in the case of Korea, the main laws related to digital identity are the Digital Organization Act, Electronic Government Act, Digital Signature Act and Promotion of Information and Communication Network Utilization and Information Protection Act. In the case of Peru, we made good progress with the issuance of Digital Government Law, which includes rules for the implementation of a Digital Identity Framework in the public sector; nonetheless it is not enough if we compare it with the legal framework of Korea.

Another similarity between Peru and Korea is that they have a national information system that stores and maintains citizen information (Resident Registration System and National Identification Registry of Peruvian). Both information systems are a source of data and information that allows and facilitates the identification of people who interact with the public administration. ***Additionally, in both countries, public entities exchange data and digital information based on interoperability platforms based on international well-known standards such as XML, web services and APIs.***

Korean Digital Identity Scheme has passed through three stages, one related to the digitalization of the resident registration information, after that ***another upgrade was exerted with the adoption of accredited digital certificates and nowadays the Government is used digital platforms (digital one pass), mobile phones (Mobile ID) and social networks to authenticate citizen´s digital identity.***

Peruvian Digital Identity Scheme has passed through three stages either, one related to the digitalization of the information of the citizens, it started 1997 with the use of computers, after that another upgrade was exerted in 2013 with the adoption of National Electronic Identity Card and ***presently the Government is going through a further development, that is why, it has started to implement a national digital platform (ID.GOB.PE) to authenticate digital identity of citizens based on digital certificates, confidential questions, facial recognition and a unique personal account generated by ID.GOB.PE.***

Both countries have an enabling legal framework for the use of digital technologies in the State, Korea has the Electronic Government Law and Peru has the Digital Government Law. The difference between them is that Korea's law was approved in 2001, while in the case of Peru, the law was approved in 2018, almost 20 years after.

Both Korea and Peru have a legal framework that allows the establishment of technical, organizational, and legal measures to protect personal information in the digital environment. In the case of Korea, the standard is the Personal Information Protection Act and in the case of Peru, it is the Personal Data Protection Law.

Likewise, both countries have a standard that enables the advanced electronic signature or well-known as digital signature, a difference between the two approaches is that Korea defines digital signature as a means for digital authentication, although this statement is true, its main reason for being is to enable the manifestation of will. To implement safe and trustworthy digital signatures both countries implemented a Public Key Infrastructure (PKI). ***Additionally, in the case of Peru, Digital Signatures and Certificates Law enables electronic voting.***

In terms of cybersecurity, Korea has a national strategy that articulates the actions of different organizations in the face of risks in the digital environment. In the case of Peru, the Supreme Decree No. 029-2021-PCM establishes specific provisions to implement organizational, technical, and legal measures to preserve the confidentiality, integrity and availability of information in the public administration, which are based on ISO/IEC 27001. Likewise, through this Supreme Decree, roles such as the digital security officer and the data privacy officer were created. Even though we don't have a national cybersecurity strategy.

In 2020, through Urgence Decrees No. 006-2020 and 007-2020, the Peruvian State establishes the ***Presidency of the Council of Ministers as the unique entity responsible for digital government and digital transformation issues at national level, through the Government and Digital Transformation Secretariat,*** whereas in Korea to have a national authority on digital

technologies is a pending task yet, because MOIS and MSIT still have this definition pending.

In both Peru and Korea, the PKI infrastructure implemented to support digital signatures can be used to support digital authentication, especially for high-risk transactions or when ID CARDs that include digital certificates are used. Korea through The Promotion of Information and Communications Network Utilization and Information Protection Act enables the possibility to designate an "identification service provider", if they comply with designated standards, the screening process will be held by KCC.

Drawing on the above, to understand the success of Korea we must notice that Korea creates specialized entities (MOIS, KLID, KISA, NIA and KCC) to cope with digital transformation challenges and develops cutting-edge technology (Digital ONEPASS, MOBILE ID, GOVERNMENT24 and NPKI) to devise and maintain in a long time a Digital Identity Scheme based on a strong legal framework, in that sense, we can say that Enabling legal framework provides sustainable ICT solutions.

b) Technology

Korea and Peru have deployed digital technologies (information systems, digital platforms, portals among others) based on an enabling digital regulatory framework aimed at closing, safe and trustworthy relationship with the citizens.

Korea has implemented Government24 looking for a suitable and user-convenient digital service rendering, and It has implemented Digital ONEPASS aims to verify the digital identity of the users, Digital ONEPASS is a digital platform where you can use different kinds of digital credentials.

In the case of Peru, we have something similar. In 2018 we implemented GOB.PE as a single point of contact with the citizens and in 2020

Peru started the implementation of ID.GOB.PE a digital platform with the purpose to verify digital identity of Peruvians and Foreigners.

One very important aspect of Korea is that Government24 has an interface to undertake digital authentication using different credentials (digital certificates, telephone number, social networks and telephone number, finger printer, Digital ONEPASS, etc.).

In terms of interoperability, both countries maintain an interoperability platform, which allows the exchange of data and information among public entities at different levels of government. In the case of Korea, the platform is called "Sharing Information System", while in the case of Peru, the platform is called "National Interoperability Platform".

An important difference between Peru and Korea is that the infrastructure of the Sharing Information System is supported by the resources and capabilities (Infrastructure and cloud services) of the National Information Resource Service, the National Data Center of Korea. The cross-border digital platforms, solutions and ICT infrastructure is centralized in the National Data Center of Korea. ***In the case of Peru, even though with the PNGD implementation we just have almost 10 hyper convergent servers, in the case of Korea they have almost 1000 thousand times that number***.

Korea has a Government Enterprise Architecture which ensures the articulation among strategic objectives and ICT and prevents overlapping of investment and resources. Peru doesn't have an Enterprise Architecture, for that reason time after time, the Government and Digital Transformation Secretariat identifies solutions that have the same purpose and scope. Peru duplicates ***solutions, it means we are not efficient to use our budget and human resources.***

Korea has developed an e-government framework that contains standards, licenses, and reusable components to ensure scalable, secure, and interoperable solution development. Peru does not have this kind of solution, however, more sooner than later, it needs to develop it.

In terms of digital signatures, both countries maintain a Public Key Infrastructure (PKI) based on international standards, which allows them to use digital signatures and strengthen digital trust for electronic commerce and digital government.

In the case of Korea, it has a National Public Key Infrastructure (NPKI) which has KISA as a Root Certification Entity (Root CA). NPKI focuses on natural persons and companies. In addition, Korea has a Government Public Key Infrastructure (GPKI), which has KLID as a Root Certification Entity (Root CA). GPKI focuses on civil servants and public entities.

In the case of Peru, we have a PKI in which the Government and Digital Transformation Secretariat is the Root CA for Government; however, there is no Root CA for private organizations, they only need to be accredited by INDECOPI, which is a governmental entity.

Based on the above, Korea shows that it has a big difference with Peru, since ***its solution development and deployment process is much more agile, safe, and scalable than the one established in Peru,*** that is why, Korea has a Government Digital Architecture, Electronic Government Framework, National and Government Public Key Infrastructure, cloud-based services platform (PaaS-TA) and National Information Resources Service (Data Center), ***allowing Koreans to reuse components and deploy solutions more efficiently and safely.***

c) Governance

From standpoint of Korea, MOIS is the leader of digital transformation process, it plays a political role at national level, however, there are others essential entities for policy implementation (NIA, KLID, KISA and KCC).

MOIS has close coordination with the Ministry of Finance and Planning, ensuring an adequate budget, likewise, MOIS set up the digital government policy which objectives, initiatives and projects will be carry out by NIA, KLID, KISA and KCC.

In terms of "Digital Identity Scheme" is just outstanding the effort and work carried out by NIA, which coordinate the implementation of projects and digital platforms, including the one related to digital identity, in fact, NIA is the technical specialist that assists in developing strategic projects in Korea national government. KLID based on MOIS guidelines is responsible for implementing ICT solutions in Local Governments. KISA is responsible for internet issues and cybersecurity, and KCC plays the role of reviewer and auditor of compliance with standards for new identification providers.

In the case of Korea, the policy and its implementation are clearly differentiated tasks, on the one hand, the design and formulation of the Digital Government Policy is the responsibility of MOIS, while the implementation is the responsibility of specialized entities such as KISA, KLID, NIA and KCC.

In both countries, political instability affects plans and initiatives, however, by having an articulated regulation, implemented platforms and a distribution of responsibilities in terms of digital identity, the ecosystem is not affected too much.

Drawing on the above, whether we want to establish an efficient and sustainable Digital Identity Scheme Governance, we must assign

responsibilities at policy design and policy implementation level. It is going to be a huge challenge to cope with these duties for just one entity, ***Peru must evaluate and realize the complexity of implementing digital transformation at national level, and therefore, Peru must create specialized governmental bodies to address different areas of digital transformation such as ICT projects, cybersecurity, ICT research, so on.***

d) Budget and Market

Korea allocates approximately 4% of its GDP to Research and Development, while Peru less than 1%. This difference causes abysmal differences in the development of technological innovations. It is no coincidence that our main source of national income is mining, while in Korea the main source of income is the export of cars, telephones, and integrated circuits.

With respect to the Market, due to its technological advance, the digital identification market in Korea is more developed than Peruvian, companies such as Kakao, Naver, mobile carriers offer the identification service looking to position their brands and get benefits for each transaction and more clients. In practical terms, we can see fierce competition among these companies.

Although a deeper analysis of market concentration would be needed, according to the documentary analysis and interviews, we can indicate that we are in an emerging market and not concentrated.

The Research and Development investment ensure innovative solutions and new knowledge about cutting-edge technology, and a low concentration of the market encourage the entering of new providers, in that sense, R&D and Market promote a sustainable Digital Identity Scheme.

CHAPTER 5: CONCLUSIONS

This chapter provides the conclusion of the research. It combines four main sections, first, a summary of the thesis is depicted, second, policy recommendations are described, and finally, the limitation of the study.

Based on the framework to comparison explained in numeral 2.15 of Chapter 1, the interviews with ICT specialists and analysis of findings on digital identity. The conclusions of the thesis will be described in a brief way as follows.

5.1 SUMMARY OF THE THESIS

Physical and digital convergence is increasing, as a result social and economic activities depend more and more on digital technologies. In that sense, digital technologies are no longer a technical problem, they are a political, legal, economic, social, and collaborative issue in the national agenda. Digital technologies aim at providing accuracy, security, inclusive, and usable digital public services to the citizens. *However, we need to consider measures to prevent being a victim of cybercrime such as identity theft and fraud online.*

***Digital government is a new paradigm in public administration*, sometimes called the digital transformation of the government**. Those times when electronic government was the main topic in the reform of the government had finished. Korea and Peru are involved in a maelstrom of initiatives, plans and projects linked to digital government, being among the most important the one related to "Digital Identity Scheme".

There are frameworks to evaluate digital government at national level, both Electronic Government Development Index and Digital Government Index evaluate the use and adoption of digital technologies from a comprehensive perspective (legal, infrastructure, institutional arrangements,

and digital services rendering), which ensures a comprehensive view for the development of Digital Government.

Digital government is affected by political and social instability, in Peru, based on the regulation, the window policy that opens time after time and our social and economic context, digital technologies have been positioning themselves as a strategic element for the development of the country, and a key element to improve efficiency in the government and provide a better service to citizens. However, this mindset is affected due to political and social instability. *In this situation the regulation is an important tool to mitigate that threat. Korea and Peru have a Digital Government Law, both of which enable digital technologies adoption in the public sector and, above all, establish a Digital Government Authority, in the case of Korea is MOIS, while in the case of Peru is Digital Government and Transformation Secretariat under the Presidency of the Council of Ministers.*

In Korea MOIS is the digital government authority at national level, based on the legal framework (Government Organization Act and Electronic Government Act), MOIS is the authority that deals with digital government issues (interoperability, digital signature, information security, digital identity, digital architecture, among others) at national level (public sector). MOIS is accountable to build and maintain cross-functional digital platforms such as GOVERNMENT24, Digital ONEPASS, Resident Registration System among others, which are essential for implementing a National Digital Identity Scheme.

In Peru the Government and Digital Transformation Secretariat is the digital government authority at national level, based on the legal framework, the entity that deals with digital government and digital transformation issues in the public and private sector is the *Government and Digital Transformation Secretariat**,*** it enables a secure and predictable

environment to design policies and initiatives. Additionally, the Digital Government Law and its Enforcement Decree create cross-functional digital platforms to deliver services more efficiently and ease for users. *The big difference is that the regulation in Korea timely follows the national strategy, in Peru the production of regulation takes time, because of limited staff, specialists and resources.*

Korea has a strong institutional arrangement because it has a Ministry responsible for the digital government in the public sector, nonetheless, the digital transformation governance could be better whether MOIS and MSIT coordinate and establish measures to improve the institutional arrangements to address the digital technologies at national level from just one perspective, it means avoiding the idea of having an entity for the public sector and another one responsible for the private sector.

MOIS and the Government and Digital Transformation Secretariat are digital government authorities, they provide sustainability to Digital Identity Scheme *because their roles allow them to enact timely regulation, maintain current information systems and envision new objectives and cutting-edge initiatives.*

MOIS has a close relationship with the Ministry of Planning and Finance, reason why, it can organize and have a better planning of activities and projects about digital government. In the case of Peru, the ***Government and Digital Transformation Secretariat*** design and plan initiative and interventions without any interaction with the Ministry of Economy and Finance, as a result, just few projects can be supported with a reasonable budget.

In Korea there is no digital transformation authority at national level (public and private sector), based on the legal framework MOIS is the governmental entity in charge to coordinate and oversees the affairs concerning

digital government in the public sector, and MSIT is accountable for designing policies on science and technology on the private sector, based on that there is no ministry or organization in charge of digital transformation at national level (public and private sector) in Korea.

In Peru there is a digital transformation authority at national level, based on Digital Government Law and National Digital Transformation System the Government and Digital Transformation Secretariat is responsible for coordinating and overseeing digital government and digital transformation at national level, it means public and private sector.

Korea and Peru have developed an enabling legal framework to promote digital technologies. In accordance with the Electronic Government Act, Korea has the legal umbrella to work in strengthening interoperability, digital signature, security, cybersecurity and digital identity in the public administration. In the same line, based on the Digital Government Law, in Peru the Government and Digital Transformation Secretariat is responsible for promoting the adoption of interoperability, digital security, digital signature, enterprise architecture and digital identity in the public administration.

The first idea of digital identity is "Fingerprint". According to the interviews, the first idea related to digital identity is "fingerprint".

The Digital Identity Scheme has two essential processes, one of them is the Identification, and the other one is the Authentication. ***They are usually understood as the same concepts, but as we noticed in this research, they are different.***

Our digital identity is a strategic asset for the public and private sector, which can be exploited to develop new digital services and create disruptive business models. The datasets and information that we create and maintain in

the digital environment not only allow us to access information, services, or knowledge, but it also represents us as human beings, it is our "digital identity".

Digital identity is a field related to digital security, by asking participants about the main reasons to implement a digital identity scheme, the reasons are to strengthen user's trust and privacy in digital environment and accessibility for digital service and digital payments. It means that, for specialists' digital identity is a field related to digital security, more than user experience, digital transformation, and others. The answers of the specialists related to the benefits of Digital Identity Scheme implementation (digital trust, privacy, accessibility, among others) are like the benefits established by the studies made by OECD and other organizations. Digital security has influenced various areas in information technology such as digital government and digital identity. That is why, along with the ongoing digital transformation process, risks, and threats such as identity theft, cyberattack and cybercrime emerged in the society, hence, Korea and Peru need to develop sustainable, accurate, secure, inclusive, and usable Digital Identity Scheme.

Digital identity and digital signature are not the same. By asking participants about whether digital identity is the same digital signature, we notice that participants have a clear understanding about the difference between digital signature and digital identity; they are complementary fields, but they are not the same.

Cross-border digital authentication is the new frontier of digital identity. According to the experience of Estonia and Europe, the digital identity is no longer a national or domestic issue, step by step based on globalization and human mobility, it has been transformed into a cross-border issue.

Digital Identity Schemes implementation shall respect national context, style of government, culture, traditions, existing population registers,

political system, and history of the country. We must not establish a completely new scheme regardless of these aspects.

There is a consensus about components and main processes of a Digital Identity Scheme*, based on standards and well-known worldwide digital identity practices, the main components of a Digital Identity Scheme are Digital Identity Provider, Digital Service Provider, Digital Attribute Provider and User. Additionally, the main processes of a Digital Identity Scheme are Identification and Authentication.*

Although there are some similarities between Digital Identity Schemes in Korea and Peru, however, the outcomes are different, Korea has a Digital Identity Ecosystem implemented and operating, while Peru is still building it.

The risk level of digital services establishes its authenticate method, it| can be something that you know, something that you have, something that you are, or a combination of them.

Governance, technology, standards, and regulation are essential aspects of a digital identity scheme, the best practices on the Digital Identity Scheme of Estonia and Spain show that aspects like Governance, Technology, Regulation (Legal framework) must be considered to understand the dynamic and functioning of a Digital Identity Scheme. Additionally, wherever the Digital Identity Scheme is implemented, it is necessary to use technical standards such as OpenID Connect, Oauth 2.0, ISO/IEC 29115, among others.

The devised framework to make the comparison seeks to have a comprehensive approach of the digital identity, the Framework used to compare the Digital Identity Scheme of Korea and Peru was made by adopting elements and components identified on UN, OECD, ITU and IADB studies, for

that reason its approach is integral and comprehensive. The framework evaluates governance, legal framework, technology, budget, and market.

Both the National Registry of Identification of PERU and the Resident Registration System of KOREA have a centralized architecture model, it means one entity is responsible for managing and maintaining a unique information system where the fundamental information of citizen's identification is stored and managed.

Korea and Peru have a Digital Signature Ecosystem, based on the Digital Signature Act and the Signatures and Digital Certificates Law, both Korea and Peru have a legal instrument and digital technology (PKI) to promote the use of electronic signatures in digital interactions and coupled with that create a Digital Signature Ecosystem.

Korea and Peru have a legal framework to protect the personal information, considering the citizen's concerns about privacy and personal data protection, Korea and Peru enacted the Personal Information Protection Act and the Personal Data Protection Law, respectively. Both legal instruments provide a legal basis to establish organizational, technical, and legal measures to protect the personal information storage by public and private organizations in their information systems.

The Korean Digital Identity Scheme can incorporate identification service providers based on the Promotion of Information and Communications Network Utilization and Information Protection Act. Korea can include identification service providers to offer their services in the digital identity market such as Kakao, Naver and PASS. In the case of Peru, we don't have this legal framework to introduce digital identification providers.

In Korea MOIS is in charge of developing and maintaining fundamental digital platforms (building blocks) of the Digital Identity

Scheme, MOIS has implemented and maintains Government24 (정부 24) as official electronic government portal, Digital ONEPASS (디지털원패스) as a digital authentication platform to enable the no-face-to-face authentication of the citizens, and the resident registration system (RRS), as an information system to storage and maintain essential data of the digital identity.

The integration of the National Electronic Services Portal and the National Digital Authentication platform is an essential initiative to satisfy the citizen's needs. With the implementation of Digital ONEPASS and Government24, the Korean government demonstrates its effort to interact with citizens in a simple and accessible way. Digital ONEPASS is the National Digital Authentication Platform with the purpose to allow digital authentication of citizens. Both platforms, Digital ONEPASS and Government24, are integrated and they have been interoperating with the private sector, especially telecommunication and financial sectors to facilitate digital authentication.

In the case of Peru, with the implementation of GOB.PE, as a single point of contact for citizen orientation, and the ongoing development of ID.GOB.PE, as a national digital authentication platform, the building blocks for the development of a digital society have been established. GOB.PE takes as a reference the experience of GOV.UK, and according to this, all portals and governmental web pages of public entities, based on legal mandate, have been migrating.

MOIS is the organization responsible for governing the digital identity scheme in Korea, MOIS is the political responsible for implementing cross-platforms, issuing the RRC and Digital ONEPASS credentials, creating the guidelines and technical conditions to promote the digital identity in the public sector at national level.

The Korean digital identity market is dynamic because under the legal umbrella of Promotion of Information and Communications Network Utilization Act, KCC is responsible for assessing every new digital identification provider such as Kakao, Naver, PASS and so on .

In face-to-face interactions, Koreans can claim their identity using either a mobile driver license or physical driver license or their RRC. On non-face-to-face interactions Koreans can prove their identity using mobile ID (mobile driver's license, mobile public official ID, etc.) social networks (Kakao, Naver, Samsung PASS, among others).

To deal with face-to-face interactions Peruvians use the National Identity Card, and for non-face-to-face interactions the traditional user and password, Electronic National Identity Card and digital certificates are the most common, therefore, based on these facts Korea provides a better user experience and usability in digital interactions with citizens.

Timely policies and strategies developed demonstrate digital leadership, Korea has demonstrated through plans, strategies, programs that it has a strong digital leadership. On the other hand, Peru has demonstrated that even when there is a role in charge of leading the digital agenda at national level and overseeing its implementation, in the practice there are not periodical meetings, not long-term engagement, and discussion of the digital issues rarely are part of the political agenda. In Korea the leadership provides sustainability of resources to maintain platforms and services.

In the case of Korea, the legal framework provides sustainability to the Digital Identity Scheme because it organizes resources, actors, and different points of view, not only in the short term, but in the long time. In addition, the legal framework establishes measures to ensure the security, usability, and inclusivity of people in the digital environment.

Have an up-to-date regulatory framework that is appropriate to our context, in Korea, the legal framework seeks to be articulated and updated with changes on the local and global context. In the case of Peru, it is a big challenge to produce regulation and norms, because we have limited resources such as budget, staff, research, and development and so on.

Every provider of services in the Digital Identity Scheme must be evaluated through a screening process to ensure quality of the service, based on the Promotion of Information and Communications Network Utilization and Information Protection Act, Korea has a screening process, performed by KCC, through which the companies interested in being a digital identification provider need to apply and meet the criteria. In the case of Peru, we don't have this legal umbrella to promote a more competitive digital identity market.

Government Enterprise Architecture is an essential building block of the Digital Government, to avoid overlapping and waste of resources and time, Koreas has a Government Enterprise Architecture implemented, which provides to public sector a common understanding on national objectives functions, business rules, data, vocabulary, interoperability standards, software development practices, security measures, while in Peru the Government Enterprise Architecture is an ongoing process.

Korea takes advantage of the potential and benefits of Cloud Services, Government 24, Digital ONEPASS and other national digital platforms of Korea are supported by the G-CLOUD or PaaS-TA, a private cloud service, which basically, according to the interviews, provides an infrastructure as a service (IaaS) and Platform as a Service (PaaS). G-CLOUD is administered by the National Information Resource Service (NIRS). In the case of Peru, GOB.PE is supported by a public cloud service (Amazon).

To implement a Digital Identity Authentication platform or Digital Identity Broker depends on your context, structure, and ITC legacy, Digital ONEPASS is a digital identity authentication platform provided by MOIS, certainly, MOIS can do that because it manages the Resident Registration System, nowadays, Digital ONEPASS allows to access almost 203 digital services. In the case of Peru, the Secretary of Government and Digital Transformation, is implementing ID.GOB.PE which is going to be a digital identity broker, in charge of orchestrating services from digital identity providers (RENIEC and MIGRACIONES). The envision of IF.GOB.PE is to provide digital authentication of Peruvians and foreigners.

Korea has a strong Governance and Leadership because MOIS has a great level of coordination with various stakeholders such as the Ministry of Finance and Planning, international organizations, and others, which allows them to understand their needs and provides services to meet them. In the case of Peru, the level of Governance is increasing little by little because we are working on it. The Government and Digital Transformation Secretariat has put a lot of effort into generating spaces to discuss and hear the citizens and business concerns.

In terms of Research and Development, Korea invests almost 4% of GDP while Peru less than 1%, in that sense the policymakers, companies and society in Korea have a continuous stream of methodologies, knowledge and information of the latest advance on technology. The R&D provides sustainability of the digital identity scheme because the information and knowledge support changes on policies and business rules, which are essential to maintain in a long term the scheme.

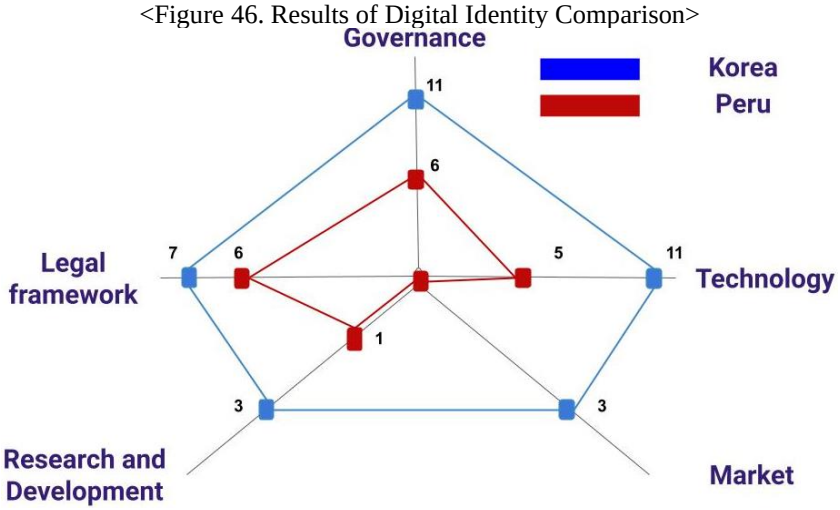
Korea has a low concentration of companies on the Digital Identity Market. Based on the Promotion of Information and Communications Network

Utilization and Information Protection, social networks and financial companies have seen this new market as a business opportunity to expand their products and services. KCC is responsible to ensure the accuracy, quality, and security of the digital identification providers.

5.2 POLICY COMPARISON

Based on the Appendix 2. Matrix of Comparison resumes of the findings and conclusions of the research, we can observe ***that the Digital Identity Scheme of Korea has a strong governance, enabling legal framework, modern technology,*** and if we combine this with the Research and Development (R&D) and Low concentration of the market, we can notice that the Digital Identity Scheme of Korea meets the citizens needs in better way than Peruvian Digital Identity Scheme.

<Figure 46. Results of Digital Identity Comparison>



Source: Own developed, 2022

Drawing on the above, the big differences are integrated in three factors: ***strong governance and continuous digital government leadership***, **MOIS** is

the digital government leadership at national level, it is in charge of digital government policy, and based on an effective coordination with KISA, NIA, KLID, MOIS can delegate the policy implementation, that is totally different from Peruvian digital government governance, because the digital government policy and its implementation is concentrated in just one entity. The Government and Digital Transformation Secretariat is overburdened as a single entity must design and implement the digital transformation policy at national level.

Other huge difference is ***the timely and enabling legal framework***, Korea enacted the Electronic Government Law in 2001, in the case of Peru it was enacted in 2018, apart from that Korea has guidelines and detailed standards to use and introduce digital technologies in the public sector such as cloud services, interoperability, digital signature and so on.

Another remarkable difference between Korea and Peru is the ICT sector. ***In Korea the ICT sector shows a fierce competition, because they try to solve social problems, meet citizen's needs and adapt their services to changes in the environment with new digital solutions***, however in Peru we do not realize the potential of data and digital technologies, we do not have a fierce competition to catch new users, or incentives to create an ICT industry, because Peruvian Digital Mindset is not developed. Policy agenda is focused on political problems as a result Peru has a small ICT market and our ICT sector is controlled by ICT vendors instead of ICT domestic makers.

The last difference but not least is ***the cutting-edge ICT technology to support development and public services rendering in Korea***. This is probably something difficult to achieve by Peruvian society.

Korea produces and offers digital technologies to the world, not only for domestic consumption. Korea has an export-driven digital technology

approach; in the case of Peru, we have an import-driven digital technology approach.

From a Korean standpoint, technology is not a tool, it is a way to improve the competitiveness and quality of life of Korean society.

5.3 POLICY RECOMMENDATIONS

Together with the existing work of OECD, ITU, WEF and UN on Digital Identity, and taking advantage that the current study has not yet been done in Peru, and, above all, considering the findings, success, and failure stories of Korean digital transformation the thesis will give some policy recommendations with the purpose to boost the digital identity implementation in Peru. The recommendations are related to different areas such as institutional arrangements, enhancing digital regulation, and optimizing the budget with the purpose to create a sustainable digital identity ecosystem.

C***reating a common understanding of digital identity*** by ***developing a glossary of terms that homogenizes concepts at the level of specialists and policymakers***. For example, there must be a clear understanding of digital government, digital identity, authentication, and identification at the national level, this will avoid confusion and waste of time and unnecessary technical conflicts.

Undertake the institutional arrangements to allow the Government and Digital Transformation Secretariat focuses on the development of transversal policies and digital platforms to promote the Digital Identity Scheme in all the country (public and private sector). This would necessarily

imply to define domestic roles and responsibilities for the Digital Identity Scheme at policy design and policy implementation level.

The first strategic institutional arrangement must ensure that the Peruvian government takes a leading role in managing the Digital Identity Scheme, and based on that raising the level from Secretariat to an Agency or Ministry, assigning it an adequate budget for its operation. Raising its level would also imply improving its level of coordination with other public entities and the private sector. In that vein, Peru should create a Ministry of Information and Communication Technologies (ICT Ministry) or a National Digital Transformation Agency under the Presidency of the Council of Ministers with specialized institutions dependent on it to address different areas of digital transformation such as ICT projects, cybersecurity, ICT research and so on. It ensures to establish a key difference between Digital Governance (National Digital Transformation Vision, National Digital Transformation Policy, National Digital Transformation Regulation, Digital Transformation Promotion, and National Digital Transformation Authority) and Digital Management. The new institution (Ministry or Agency) should be capable of coordinating with all the entities at all different levels, therefore, it needs to be autonomous or be in the center of the executive branch of power.

Develop a digital government framework that contains standards, licenses, and reusable components to ensure scalable, inclusive, secure, and interoperable solutions development. According to the experience of the digital government framework of Korea, the Government and Digital Transformation Secretariat must establish standards at technical level, including the processes, development, and data layers. The standards to be established must be in accordance with the advances in the ICT industry and the technological capabilities of the country.

Encourage adoption of cloud services in the Peruvian State, the Government and Digital Transformation Secretariat must leverage capacities and resources of the National Digital Government Platform implemented to provide cloud services to public entities **such as Ministries, Municipalities, and other public agencies**. Although it is a megaproject, international loans from the Inter-American Development Bank or the World Bank could be used to improve their storage and processing capacity. We must establish the "Cloud first" policy and follow it, to achieve that the high-level commitment is a key factor, that is why, the President, ministries, and decision makers at national level.

Establish a specific regulatory framework (Digital Identity Law) that guarantees privacy processing of personal identifiable data and ensures the digital identity is legally valid just like ID cards and can be used anywhere.

*In that vein****, it is recommended that Peru adopt a long-term vision for the Digital Identity, it means to have a Digital Identity Master Plan or National Digital Identity Strategy*** for designing and implementing a Digital Identity Scheme that responds to the needs of citizens, residents, and legal persons. *The National Strategy should be the result of an open and transparent process involving different kinds of stakeholders* (public, academy, and private sector), also it must include measures to manage digital security risk to foster trust and confidence in the digital environment and Digital Identity Scheme.

The strategy must devise and set up interventions to allow citizens, civil servants, residents, and legal persons to equip them with digital means (mobile applications, ID cards, contactless reading devices and so on) that enable them to easily identify themselves in their daily lives, it means give them ***more control and autonomy over their identity.***

The Government and Digital Transformation Secretariat cannot implement every component of Digital Identity Scheme, that is why, it must focus on Digital Identity vision, policy, strategy, and law. Based on the Korean experience, ***the Government and Digital Transformation Secretariat can make a Digital Platform that enables the exchange of Boolean personal information like a "Yes or No" signal between public and private organizations***. In addition, based on the lesson of the Korean case, the Government must promote the investment of the private sector in creating digital services via Digital Platform implemented by the Government.

Complete the implementation of ID.GOB.PE, the Peruvian national digital authentication platform, considering the balance between the level of risks and security. The platform must be interoperable by default and promote the use of international standards. ID.GOB.PE must be a vital part of a digital identification and authentication in a cross-border transaction.

The digital identity solutions need to be flexible and technology-neutral to foster trust and confidence in government interventions, that is relevant because the ***digital identity solutions*** must support strategies in different economic and social areas, that is why the Digital identity solutions must be ready to adapt to new needs, changes in regulation and technological advancements.

The Government and Digital Transformation Secretariat must promote the exchange of data and information among public and private organizations, especially those related to citizen authentication, given that it would be much simpler, and in turn more channels of access and interaction with the public could be established. State (digital certificates, cell phones, credentials of financial entities, among others).

The Government and Digital Transformation Secretariat must discover and develop areas for digital identity authentication while enhancing user's convenience, security, and trust. Those areas could be immigration procedures, public service rendering, cross-border e-commerce, electronic learning, financial transactions, residence registration, telemedicine, driver license, government subsidies, etc.

The Government and Digital Transformation Secretariat must take advantage of digital technologies such as mobile devices, open protocols, cloud computing, PKI encryption technology, facial recognition, and artificial intelligence to prepare convenient ways to identify, use, enroll, issue, and authenticate users anywhere online and offline.

The Government and Digital Transformation Secretariat must call on public entities and private organizations to minimize digital divides to the access and use of digital identity, thereby they must implement inclusive and affordable approach to enrolment and use digital identity solutions. Government must collaborate with service providers to anticipate and mitigate possible risks before rolling out a new digital identity solution.

The Government and Digital Transformation Secretariat must strengthen international cooperation and mutual assistance, it means to be part of international fora, and establish relationships to share knowledge, learned lessons and best practices, and experience about Digital Identity Scheme implementation and operation.

Peruvian State must establish a support and financing fund for research and development work in the technological field, especially those related to digital identity solutions and technologies for use and consumption by the ICT specialists, researchers, businesses, and industry. A sustainable funding mechanism for cutting-edge digital identity solutions is needed for

maintaining, establishing, and operating a digital identity Scheme at national level.

Peruvian State must strengthen research centers, especially those implemented by public universities and private organizations, research is the main source of knowledge in Korea, therefore, Peruvian national universities and ICT private organizations must be encouraged to research and develop technological innovations, Peru can set up a Public Private Partnerships Model (PPP) to improve the Digital Identity Research and Development in a short-term. By implementing Public Private Partnerships initiatives, the government encourage the private sector to participate in Digital Identity Researching and share the benefits from the Digital Identity Scheme implementation.

Peru must prioritize the development and implementation of a Digital Architecture for the State, which includes standards at the business level, processes, services, and information security. To prevent overlap of resources and ensure benefits of the investment.

In the case of Korea, perhaps the only point at the policy level that could be recommended is that both MOIS and MSIT be able to establish joint actions and define an institutional arrangement to address digital transformation in an articulated manner at the national level, covering the areas public and private.

5.4 LIMITATIONS OF THE RESEARCH

There is a lack of frameworks to compare digital identity schemes, to achieve that we built one, considering the standards, best practices, and previous studies on digital identity schemes. Our framework looks the digital identity scheme as a system, a set of components interacting among them and sharing data and information to achieve managing the digital identity lifecycle and promote trust in the digital environment.

Another limitation is the availability of the time of specialists in Korea and Peru, the development of interviews or surveys. Second, there are limitations in

REFERENCES

(UN), U. N. (2001). *Benchmarking E-government: A Global Perspective.*

Al-Sinani, H. S. (2011). *Integrating OAuth with Information card systems.* Retrieved from https://ieeexplore.ieee.org/document/6122819

Australian Government . (2022). *Digital Identity*. Retrieved from https://www.digitalidentity.gov.au/about-digital-identity

Ayed, G. B. (2011). *Digital Identity Metadata Scheme: A Technical Approach to Reduce Digital Identity Risks.* Retrieved from https://ieeexplore-ieee-org.libproxy.snu.ac.kr/document/5763568

Batista, G. C. (2022). *Security analysis of the OpenID Connect protocol.* Retrieved from https://ieeexplore.ieee.org/document/7833358

Bouzefane, M. L. (2015). *Digital Identity Management.* Great Britain: ELSEVIER.

Brubaker, J. R. (2009). *I AM AN ID: NON/PERSISTING OUR SOCIOTECHNICAL DIGTIAL IDENTITIES.* Washington, D.C.

Chong-sik, C. (2020). *Developing Digital Governance.*

Chung, C.-S. (2019). *A Comparative Study of Digital Government Policies, Focusing on E-Government Acts in Korea and the United States.* Retrieved from https://www.mdpi.com/2079-9292/8/11/1362/htm

DCMS. (2022, 27 05). *Digital Identity and attibutes trust framework.* Retrieved from https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/uk-digital-identity-and-attributes-trust-framework-alpha-version-2

DID Alliance Korea. (2020). *DID Alliance Official.* Retrieved from youtube.com/watch?v=4JaS_fONj3U&ab_channel=DIDAllianceOfficial

Dongsung Kong, M.-G. J. (2015). *The Cases of -E-Governance and Development in Korea.*

Eifter, M. (2004). *National Electronic Government.*

GOV.UK. (2022). *UK digital identity and attributes trust framework - alpha version 2.* Retrieved from

https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/uk-digital-identity-and-attributes-trust-framework-alpha-version-2#introduction

Husni, E. (2015). *Digital signature for contract signing in service commerce.* Retrieved from https://ieeexplore-ieee-org.libproxy.snu.ac.kr/document/7389757

IDB. (2017). *Identidad Digital y su Impacto en la Economía Digital.*

IDB. (2020). *Identidad Digital Autogestionada.* Retrieved from https://publications.iadb.org/publications/spanish/document/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf

Im, T. (2019). *The two sides of Korean Administrative Culture .* New York.

INEI. (2017). *Perú perfil sociodemográfico.* Retrieved from https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1539/libro.pdf

ISO. (1989). *ISO 7498-2.* Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:7498:-2:ed-1:v1:en

ISO. (2011). *ISO/IEC 24760-1.* Retrieved from https://www.iso.org/standard/77582.html

ISO. (2018). *ISO 27000.* Retrieved from https://www.iso.org/standard/73906.html

ITU. (2018). *Digital Identity Road Map.* Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-DIGITAL.01-2018-PDF-E.pdf

ITU. (2018). *Digital Identity Road Map.* Geneva.

Jorstad, I. (2009). *Releasing the potential of OpenID & SIM.* Retrieved from https://ieeexplore.ieee.org/document/5357063

Kenneth L. Judd, Y. K. (2000). *An Agenda for Economic Reform in Korea.*

Kim, S. (2014). *The Evolution of Korean E-Government in the perspective of Actor-Network Theory.*

Kim, S. (2015). *The Evolution of Korean e-Government.*

Kim, S. O. (2019). *Interoperable OAuth 2.0 Framework.* Retrieved from https://ieeexplore.ieee.org/document/8668962

Ko, K. (2021). *Understanding The Republic of Korea* .

Kong, D. (2015). *The Cases of E-Governance and Development in Korea.*

Korea Law Information Center. (2022). Retrieved from https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&section=lawNm&query=ELECTRONIC+GOVERNMENT&x=0&y=0#liBgcolor0

KOSTAT. (2021). *2020 Population and Housing Census (Register-based Census).* Retrieved from http://kostat.go.kr/portal/eng/pressReleases/8/7/index.board?bmode=download&bSeq=&aSeq=391585&ord=1

Lee, R. B. (2013). *Security Basics for Computer Architects.*

Lust, J. (2019). *The rise of a capitalist subsistence economy in Peru.* Retrieved from http://lps3.web.p.ebscohost.com.libproxy.snu.ac.kr/ehost/pdfviewer/pdfviewer?vid=0&sid=baa2afea-56b6-497c-acd7-a28050139aa1%40redis

Malca, O. (2021). *Relational flexibility norms and relationship-building capabilities as a mediating mechanism in export performance: insights from exporting SMEs in an emerging economy, Peru.* Retrieved from http://lps3.www.emerald.com.libproxy.snu.ac.kr/insight/content/doi/10.1108/IJOEM-09-2019-0735/full/html?&pds_handle=206202281635111787707323087471 3506&calling_system=primo&institute=

MOIS. (2020). *Digital Government Policy and Best Practices of Korea.* Seoul.

MOIS. (2022). Retrieved from https://www.mois.go.kr/eng/bbs/type002/commonSelectBoardArticle.do%3Bjsessionid=w05brhjGq1Ekv1m8EvIAMRMW.node10?bbsId=BBSMSTR_000000000295&nttId=58538

MOIS. (2022). *Digital Government*. Retrieved from https://www.dgovkorea.go.kr/

MOIS. (2022, 06 22). *egov-frame Portal*. Retrieved from egov-frame Portal: https://www.egovframe.go.kr/eng/sub.do?menuNo=7

MOIS. (2022). *Status of Government 24.* Retrieved from https://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1026

N. Hossain, M. A. (2018). *OAuth-SSO: A Framework to Secure the OAuth-Based SSO Service for Packaged Web Applications.* Retrieved from https://ieeexplore.ieee.org/document/8456096

NATGEO. (2022). *National Geographic*. Retrieved from https://kids.nationalgeographic.com/geography/countries/article/south-korea

NIRS. (22). Retrieved from https://www.nirs.go.kr/eng/key/key_01.jsp

NIST. (2017). *Digital Identity Guideline Authentication and Lifecycle Management.* Retrieved from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf

OECD. (2008). Seoul Declaration on the Future of the Internet Economy. Retrieved from www.oecd.org/dataoecd/49/28/40839436.pdf

OECD. (2009). *The Role of Digital Identity Management in the Internet Economy: a Primer for Policy Makers.* Paris: OECD Publishing. Retrieved from https://www.oecd-ilibrary.org/docserver/222134375767.pdf?expires=1649000020&id=id&accname=id13221&checksum=24551B1527B45F1E850690EE63425A28

OECD. (2011). *Digital Identity Management, Enabling Innovation and Trust in the Internet Economy.* Retrieved from https://www.oecd.org/sti/ieconomy/49338380.pdf

OECD. (2014). *Recommendation of the Council on Digital Government Strategies.* OECD. Paris: OECD Library. Retrieved December 16, 2021, from https://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf

OECD. (2019). *Digital Government Index.* Retrieved from https://www.oecd-ilibrary.org/docserver/4de9f5bb-en.pdf?expires=1653531711&id=id&accname=guest&checksum=840FFCC2FBEEC88982E07C269D1A4C3D

RAE. (2022). Retrieved from https://dle.rae.es/identidad

Rajendran, B. (2017). *Evolution of PKI Ecosystem .* Retrieved from https://ieeexplore-ieee-org.libproxy.snu.ac.kr/stamp/stamp.jsp?tp=&arnumber=8278951

RENIEC. (2020). *Memoria Institucional 2020.* National Registry of Identification and Civil State. Retrieved from https://cdn.www.gob.pe/uploads/document/file/2152637/Memoria%20Institucional%202020.pdf

RENIEC. (2020). *National Digital Identity Plan.* Retrieved from https://cdn.www.gob.pe/uploads/document/file/2799674/Plan%20Nacional%20de%20Identidad%20Digital%20y%20Servicios%20Disponibles%20%28PNIDSD%29%202022-2025.pdf

RENIEC. (2022). *Historia de documentos de identidad.* Retrieved from http://www.reniec.gob.pe/portal/pdf/museo/cronologia.pdf

Sadigova, U. (2014). *Implementation of E/government in Azerbaijan.*

Son, W. (2017). *The Government Role in digital era innovation: The case of electronic autentication policy Korea.*

Springer. (2008). *The Future of Identity in the Information Society.* Retrieved from https://link.springer.com/content/pdf/10.1007/978-0-387-79026-8.pdf

Srinivasan Madham Kumar, D. P. (2010). *A Roadmap for the Comparison of Identity Management.*

Sullivan, C. (2018). *Digital identity – From emergent legal concept to.*

System, U. t.-E. (2021). *Kilkon Ko.* South Korea.

Tolk, A. (2013). *Interoperability, Composability, and Their Implications for Distributed Simulation: Towards Mathematical Foundations of Simulation Interoperability," 2013 IEEE/ACM 17th International Symposium on Distributed Simulation and Real Time Applications.* Retrieved from https://ieeexplore.ieee.org/document/6690487

Turner, S. (2014). Transport Layer Security. *IEEE Internet Computing, vol. 18*, 60-63. Retrieved from S. Turner, "Transport Layer Security," in IEEE Internet Computing, vol. 18, no. 6, pp. 60-63, Nov.-Dec. 2014, doi: 10.1109/MIC.2014.126.: https://ieeexplore-ieee-org.libproxy.snu.ac.kr/document/6938667

UN. (2020). *E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development.* United Nations. Retrieved December 16, 2021, from https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020

UN. (2020). *Member State Questionary Korea .* Retrieved from https://publicadministration.un.org/egovkb/Portals/egovkb/MSQ/Korea_Republic%20of_24052021_041713.pdf

UTEC. (2022). Retrieved from https://www.utec.edu.pe/noticias/ciencia-tecnologia-investigacion-importancia-cifras-peru

Vatra, N. (2022). *Public Key Infrastructure for Public Administration in.* Retrieved from https://ieeexplore-ieee-org.libproxy.snu.ac.kr/stamp/stamp.jsp?tp=&arnumber=5509037&tag=1

WEF. (2018). *Identity in the Digital World a new chapter in the social contract.* Retrieved from https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

WEF. (2022). *The Global Risk Report 2022.* World Economic Forum . Retrieved from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

World Bank. (2016). *Digital Government 2020 : Prospects for Russia.* Washington. Retrieved from https://openknowledge.worldbank.org/handle/10986/24402

World Bank. (2022). *World Bank Open Data*. Retrieved from https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS

Yoon, J. W. (2015). *The Evolution of the Resident Registration System in Korea.* Republic of Korea. Retrieved from https://www.ksp.go.kr/file/krims/201806/20180605113331[1].pdf

Zhang, J. (2010). *A study on application of digital signature technology.* Retrieved from https://ieeexplore-ieee-org.libproxy.snu.ac.kr/document/5479249

APPENDICES

APPENDIX 1. QUESTIONNAIRE

Digital Identity Scheme of Korea
(한국의 디지털 신원 체계)

The DIGITAL IDENTITY is an essential component of the digital transformation, nevertheless, its development and trustworthy performance requires an articulated collection of policies, resources, and stakeholders.

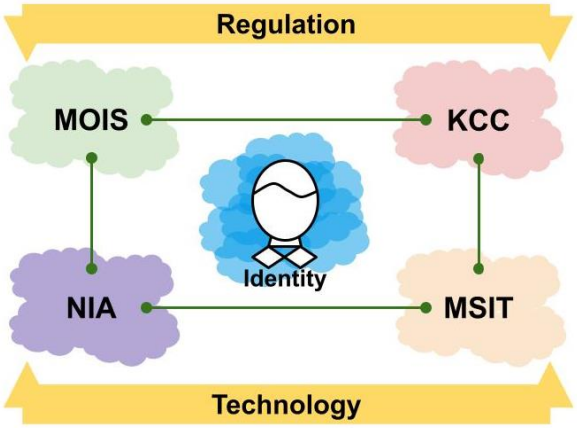
In this regard, for this research, DIGITAL IDENTITY is understood as a collection of attributes which can uniquely IDENTIFY a person during its interaction with digital platforms (digital services, information systems, applications). On the other hand, DIGITAL IDENTITY SCHEME is a collection of policies, technologies, organizations, and processes in charge of governing and managing the LIFECYCLE of the DIGITAL IDENTITY.

The main components in the DIGITAL IDENTITY SCHEME are USER, IDENTITY SERVICE PROVIDER, ATTRIBUTE SERVICE PROVIDER and DIGITAL AUTHENTICATION PLATFORM. In this case, the questions below are related to technological, organizational, and legal aspects of the DIGITAL IDENTITY SCHEME in Korea.

Considering the DIGITAL IDENTITY REGULATION such as Electronic Government Act (2001), Promoting informatization Act, and Promotion of Information and Communications Network Utilization and Information Protection Act and the essential roles and functions of Ministry of Interior and Safety (MOIS), Korean Communication Committee (KCC) and Ministry of Science and ICT (MSCI).

Please, share your opinion based on your experience about the DIGITAL IDENTITY SCHEME of Korea. The data collected will remain confidential and used solely for academic purposes.
[한국어 답변이 가능합니다]

Thank you very much! 감사합니다!



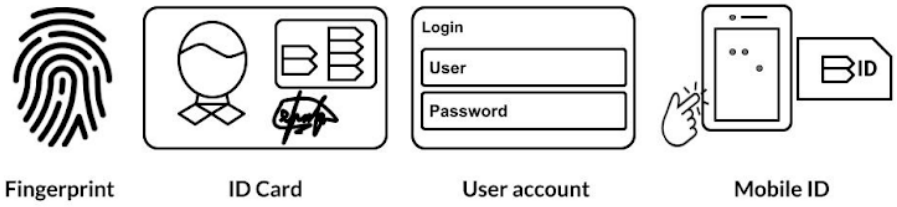
* **Name**:

* **Years of experience on ICT projects**:

A. General overview of Digital Identity Scheme in Korea

In this part, we want to know about general aspects of the Korean DIGITAL IDENTITY SCHEME. We try to discover your first impressions about DIGITAL IDENTITY, what you consider are the reasons for its implementation, what types of digital identity credentials have been accepted on dealings with government at national level, among other questions.

1 "Try to be quick in this question", What is your first idea or mental picture that comes to your mind when we say, "digital identity"?



a) Fingerprint
b) ID Card
c) User account
d) Mobile ID
e) Iris scan
f) Information System with personal information
g) Digital Certificate
h) Otro:

2 In your point of view, what are the main reasons to implement a Digital Identity Scheme? (You can choose more than one option)

- **a)** To enhace cybersecurity (digital security) of digital services
- **b)** To strengthen user's trust and privacy on digital environment
- **c)** To promote the electronic commerce
- **d)** To comply with digital regulation
- **e)** To comply with a Digital Government policy, plan or strategy
- **f)** To ensure a National Security on cyberspace
- **g)** To promote innovation and cutting-edge business models on digital environment
- **h)** To Enhance efficiency of public service delivery
- **i)** Otro:

2.1 You can extend and provide more detail about your previous answer:

3 In your point of view, digital identity and digital signature are:

- **a)** Different ICT fields
- **b)** Almost the same
- **c)** Different ICT fields but they are a good complement to promote digital transformation
- **d)** Otro:

3.1 You can extend and provide more detail about your previous answer.

4 Currently, when you carry out a face-to-face transaction with the public sector, banks, stores, among others. How can you proof your identity?

- **a)** I can claim my identity using my Mobile Driver License in my mobile phone or my Driver License Card
- **b)** I can claim my identity using my Resident Registration Card (RRC)
- **c)** Otro:

4.1 You can extend and provide more detail about your previous answer.

5 Currently, when you carry out a online transaction (non-face-to-face interaction) with the PUBLIC SECTOR. How can you proof your identity?

- **a)** I can use information of my Resident Registration Card (RRC) and answer questions
- **b)** I can use ONEPASS (디지털원패스)
- **c)** I can use information of my credit or debit card to claim my identity

d) I can proof my identity using my social networks (Kakao, Naver, Samsung PASS, among others)
e) I can use digital certificates issued by public or private organizations
f) I can use my telephone number to authenticate me

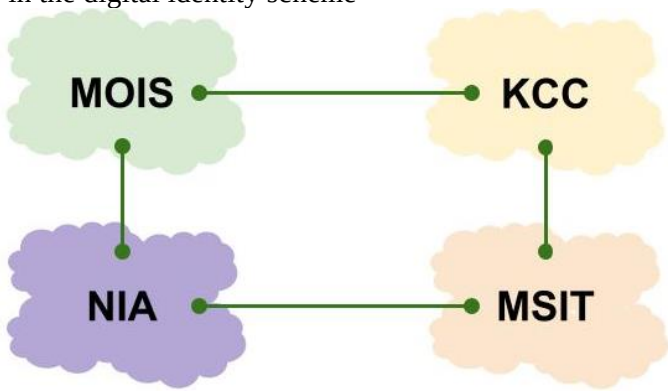
B. Digital Identity Scheme GOVERNANCE

In this part, we want to know about the institutional arrangements, roles, and responsibilities in governing, coordinating, and managing the Digital Identity Scheme in Korea.

It means, which governmental entities are in charge of leading and coordinating decisions on digital identity projects, programs in the public sector and at national level.

According to the regulation there are four key actors in the digital identity ecosystem Ministry of the Interior and Safety (MOIS), Korea Communications Commission (KCC), National Information Society Agency (NIA) and Ministry of Science and ICT (MSIT), we want to clarify their functions and roles.

Key actors in the digital identity scheme



6 Which is the governmental body (public entity) in charge of promoting, designing, and coordinating the DIGITAL IDENTITY POLICY or STRATEGY at NATIONAL LEVEL in Korea (public and private sector)?

a) Ministry of Interior and Safety (MOIS)
b) Korean Communication Commission (KCC)
c) Ministry of Science and ICT (MSIT)
d) National Information Society Agency (NIA)
e) Any of them
f) Otro:

6.1 Please extend and provide more detail about your previous answer.

7 Which is the governmental body (public entity) in charge of leading and coordinating decisions, projects, and initiatives on digital identity in the PUBLIC SECTOR?

- **a)** Ministry of Interior and Safety (MOIS)
- **b)** Korean Communication Commission (KCC)
- **c)** Ministry of Science and ICT (MSIT)
- **d)** National Information Society Agency (NIA)
- **e)** Any of them
- **f)** Otro:

7.1 Please extend and provide more detail about your previous answer.

8 Which is the governmental body (public entity) in charge of issuing digital identity credentials such as Resident Registration Card (RRC) and ONEPASS)?

9 Where can I see the NUMBER of Koreans WITH Resident Registration Card and ONEPASS ACCOUNT over time?

10 **What is the role (functions and duties) of Korean Communication Commission (KCC) in the Digital Identity Scheme? For instance: Is KCC responsible for assessing every new digital identification provider such a Kakao, Naver, etc. See the next link:** https://www.koreatimes.co.kr/www/tech/2022/05/133_305254.html?KK

11 What is the role (functions and duties) of Ministry of Interior and Safety (MOIS) in the Digital Identity Scheme?

- **a)** It is in charge of Maintaining the Resident Registration System (RRS)
- **b)** It is responsible for designing and implementing the Digital Identity Policy at National Level
- **c)** It is responsible for designing and implementing the Digital Identity Policy in the public sector
- **d)** It is accountable for implementing and maintaining the Digital Authentication Platform (ONEPASS)
- **e)** It is accountable for ensuring the integration of GOVERNMENT24 (정부) and ONEPASS (디지털 원패스)
- **f)** It is accountable for elaborating and updating technical standards on digital identity and interoperability
- **g)** Otro:

12 What is the role of the Ministry of Science and ICT in the Digital Identity Scheme?

13 From a perspective of Digital Identity, what is the role of the private sector in the digital identity scheme?

- **a)** To manufacture and customize national identity cards (Resident Registration Cards)
- **b)** To provide software to improve security and meet new citizen demands
- **c)** To support users and business which use or want to integrate ONEPASS, Kakao, Naver, or another one with their digital services
- **d)** Otro:

14 What is the role of NIA in the digital identity scheme?

- **a)** Implement Digital Identity Platform according to law and MOIS technical specifications
- **b)** Provide technical assistance to all public sector
- **c)** Provide a base of knowledge about standards and guidelines to implement digital identity.
- **d)** Otro:

B. Digital Identity Technology

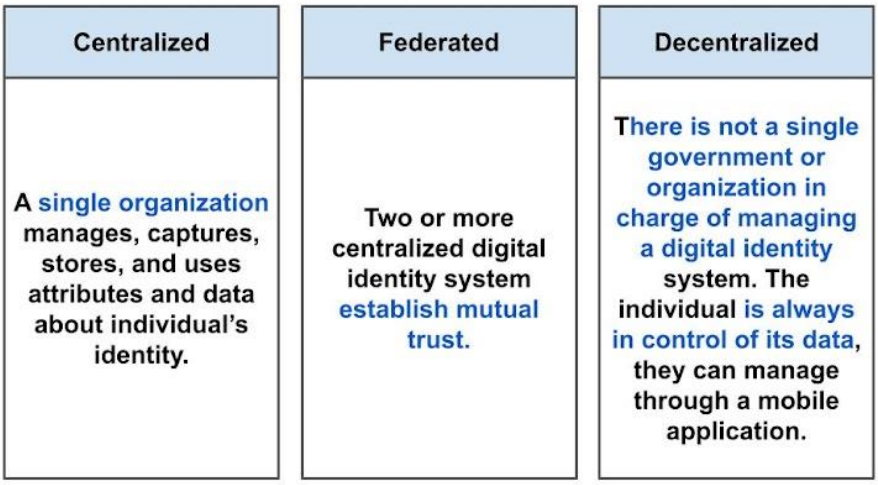
In this part, we want to know about the digital platforms or technology, which have supported the digital identity deployment, FOR INSTANCE GOVERNMENT24 and ONEPASS are essential and relevant platforms in this regard.

15 Some scholars categorize the evolution of digital identity scheme in Korea in three stages, such as: a) based on physical card (Resident Registration Card), b) based on accredited certificates and c) based on digital cards, digital authentication platforms and digital identity services (Kakao, Naver, etc.). Are you agree with this categorization or is there something that we are missing?

16 What are the fundamental components of the successful implementation of Digital Identity Scheme in Korea?

- **a)** Safety, interoperable and scalable ICT Infrastructure
- **b)** Collaboration between public and private sector
- **c)** Campaigns or programs to strengthen digital skills of the citizens and stakeholders
- **d)** Leadership of MOIS
- **e)** Leadership of MOIS and MSIT
- **f)** Otro:

17 Basically, there are three kinds of Digital Identity Scheme Archetypes.
What kind of Digital Identity Scheme has Korea implemented?



- **a)** Centralized
- **b)** Distributed
- **c)** Descentralized
- **d)** Otro:

18 Who is in charge of the Government Enterprise Architecture in Korea?

- **a)** Ministry of Interior and Safety (MOIS)
- **b)** Ministry of Science and ICT (MSTI)
- **c)** Ministry of Security and Public Administration
- **d)** Otro:

19 What is the importance of Government Enterprise Architecture to deploy the Digital identity Scheme in Korea?

C. Resident Registration System

Under the Resident Registration Act every Korean has a Resident Registration Number (RRN), it means that every Korean has a personal identification number. The next questions try to understand the issuance of RRN.

20 Is The head of the province (도), Metropolitan city (광역시) and County (군) is the accountable for initiating the registration process of a new resident.

21 Is the information of the Resident Registration System (RRS) shared across the different levels of administrative agencies, public entities using the interoperability?

22 Is the information of the Resident Registration System (RRS) used by ONEPASS (디지털원패스) in order to verify identity of Koreans?

23 Who is the gubernmental entity responsable to storage and preserve information security of foreingners in Korea?

24 How ONEPASS use the information of foreigners to identify them? Which entity provides the information of foreigners?

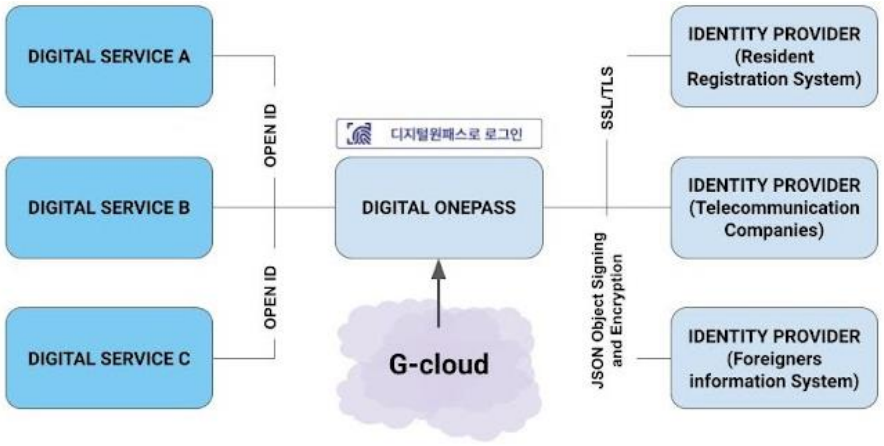
25 How Korean Government ensure the scalability of Digital ONEPASS**?**

26 When a citizen uses Kakao, Naver, PASS or Samsung Pass to claim your identity on GOV.24, The government need to pay something to these digital service providers? What is the benefit for Kakao, Naver, PASS, could you give some ideas?

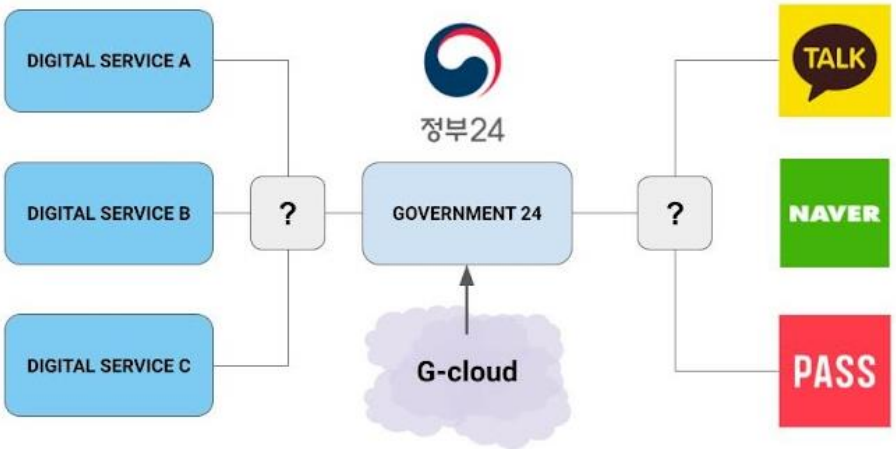
27 Do ONEPASS use CLOUD SERVICES from National Information Resource Services (NIRS)?

28 What is the regulation which allows to Kakao, Naver and Samsung PASS to provide identification services?

29 What is the standards to integrate a digital service and identity provider with ONEPASS? For instance, to integrate to Digital Services we use OPEN ID, on the other hand to exchange information with Identity Providers we use SSL/TSL and JOSE (JSON Object Signing and Encryption)



30 How Government24 integrate different kind of digital authentication services KAKAO, PASS, NAVER or ONEPASS? What kind of technical standards are required to use Naver and Pass, Kakao in the public sector?



APPENDIX 2. MATRIZ OF COMPARISON

	Components	Korea	Peru	
1.	**Governance Strong=5p, High=3p, Medium=2p, Weak=1p**			**Criteria**
1.1	Institutional arrangements	High (Ministry of Interior and Safety – MOIS, Ministry)	Medium (Government and Digital Transformation Secretariat, Secretary under the Presidency of the Council of Ministers)	Sustainable
1.2	Leadership	Strong	Medium	
1.3	Collaboration and coordination	Strong	Medium	
		11p	6pt	
2.	**Legal framework (Have=1, Don't have =0)**			**Criteria**
2.1	Electronic Government Law or Digital Government Law	**Have** There is an Electronic Government Law, it was enacted in 2001	**Have** There is a Digital Government Law, it was enacted in 2018	**Sustainable**
2.2	Legal disposition which assigned the responsible to maintain the basic identification system of citizen	**Have** (Resident Registration Act – MOIS maintain the Resident Registration System)	**Have** **(**Law N° 26497 RENIEC maintain the National Register of Identification, to date, 99% of the population are identified)	
2.3	Regulation for digital Identification Providers.	**Have** Based on the Promotion of Information and Communications Network Utilization and Information Protection Act, there is a screening process to approve the entrance of new digital	**Don't have** There is not regulation.	

		identification providers.		
2.4	Regulation to protect the personal information and privacy of the persons.	**Have** (Personal Information Protection Act)	**Have** (Law N° 29733, Personal Data Protection Law)	
2.5	Regulation on interoperability	**Have** (Electronic Government Act)	**Have** (Electronic Government Law)	
2.6	Regulation on information security (cybersecurity)	**Have** (National Cybersecurity Strategy), for public and private sector.	**Have** (Electronic Government Act), but is just for public sector	
2.7	Regulation on digital signature	**Have** (Digital Signature Act)	**Have** (Signatures and Digital Certificates Law)	
		7p	6p	
3.	**Technology (Have=1, Don't have =0)**			
3.1	Government Enterprise Architecture (GEA)	**Have** Korea has a Government Enterprise Architecture implemented and regulated by Electronic Government Law	**Don't have** Peru has a Digital Government Architecture regulated by Digital Government Law, but it is not implemented yet.	**Sustainable, scalable, inclusiveness and safety**
3.2	Public Information Sharing System	**Have** (하나로민원)	**Have** (National Interoperability Platform)	
3.3	National Data Center	**Have** National Information Resource Service	**Don't have** (We are implementing a National Digital Government Platform)	
3.4	Authentication Platform (Public Sector)	**Have** (Digital OnePass -디지털 원패스)	**Have** (ID.GOB.PE, it is in progress)	
3.5	National Electronic Service Portal	**Have** (Government24 정부 24)	**Have** (GOB.PE)	

3.6 Open Data Portal	**Have**	**Have**	
3.7 EGOV-FRAME	**Have**	**Don't have**	
3.8 Public Key Infrastructure (PKI)	**Have** (NPKI and GPKI)	**Have** Official Electronic Signature Infrastructure	
3.9 Platform as a Service Framework	**Have** (PaaS-TA)	**Don't have** (National Digital Government Platform is an ongoing project)	
	9p	**5p**	
4. **Market No market= 0p, Low concentration= 3p, High = 1p**			
Concentration of the market	Kakao, Naver, Pass, and others.	There are no providers	**Sustainable**
5. Investment on R&D Low=1p, Medium=2p, Strong=3p			
Investment on research and development (R&D)	**Strong** 4.53% of GDP in 2018	**Low** 0.11% of GDP 2018	**Sustainable**

국문초록

한국과 페루의 디지털 아이덴티티 제도 비교 연구

-각국 디지털 아이덴티티 전략을 중심으로-

Yuri Aldoradin Carbajal

서울대학교 행정대학원

글로벌행정전공

디지털 아이덴티티는 디지털 서비스와의 상호작용에서 개인을 고유하게 차별화하는 속성을 의미한다. 따라서 디지털 아이덴티티 전략은 디지털 아이덴티티 라이프사이클을 관리하는 정책, 기술, 조직 및 프로세스의 잘 설계된 집합체이다. 이는 디지털 변환의 필수 요소이며 디지털 신뢰를 강화하기 위한 핵심 요소이다.

그런 맥락에서, 이 논문은 국가 차원에서 디지털 아이덴티티 체계를 관리하는 데 있어 어려움을 이해하는 것을 목표로 한다. 정확성, 포괄성, 안전성, 사용 가능한 디지털 ID 의 이점은 공공 및 민간 부문, 아카데미 및 국제 조직에 의해 널리 인식되고 있다. 이와 더불어 COVID-19 의 세계적인 확산으로 인해 사회적 거리두기 조치와 비대면 거래가

증가하면서, 우리는 정부와 기업에 의해 개발되는 디지털 인증 플랫폼이 발전하는 것을 볼 수 있다.

그 결과, 대한민국(이하 한국)과 페루와 같은 나라들은 핸드폰, 인공지능, 빅데이터, 상호운용성, 데이터센터와 같은 부상한 기술을 활용하여 식별 및 인증 프로세스의 효율성을 높이기 위해 서로 다른 종류의 이니셔티브와 플랫폼을 개발, 시행하고 있다. 이에 따라 현재까지 정부 24 를 전자정부 공식포털로, 디지털원패스(Digital ONEPASS)를 디지털인증플랫폼으로 구현해 시민 비대면 인증이 가능하도록 하고 있으며, 주민등록제도(RRS)도 한국 디지털 아이덴티티 제도의 핵심요소로 자리매김하고 있다.

이와 비슷하게 페루의 경우 기존의 전자정부 접근 방식이 디지털 정부라는 새로운 패러다임으로 변모하였다는 것과, 디지털 기술은 더 이상 기술적 문제가 아니라 정치, 법률, 협력적 문제라는 이해를 바탕으로 2018 년 디지털 정부가 제정되었다. 디지털 정체성을 강화하기 위해 두 개의 디지털 플랫폼이 시행되고 있는데, 하나는 시민 지향의 단일 디지털 플랫폼(GOB.PE)이며, 다른 하나는 디지털 신원 확인 및 인증을 위한 국가 플랫폼(ID)이다. 두 플랫폼은 정부에 의해 유지되고 개발된다.

이처럼 한국과 페루의 정책 사이에 유사점이 있지만 결과는 다르다. 전자정부개발지수(EDGI)에서 한국은 세계 2 위, 페루는 71 위, 한국은 디지털 인증 플랫폼이 구현되어 있고, 정부 24 는 다양한 인증을 사용하고 있다. ONE PASS, KAKAO, 삼성 PASS 등 시민을 위한 간편하고 편리한 인증 방법이 사용된다. 또한 2021 년까지 정부 24 를 통해 온라인으로 접수된 청원은 13202 만 5035 건에 달하며, 증명서와 문서는 시민이 직접 프린터를 통해 출력했다. 페루의 경우 디지털 아이덴티티 전략은 디지털 정부법이 규제하는 공공부문의 디지털

아이덴티티 프레임워크를 기반으로 정부가 기본적으로 주도하는 진행형 프로세스다.

따라서, 본 연구에서는 한국의 디지털 아이덴티티 전략이 개인의 디지털 아이덴티티의 정확성, 포괄성, 보안성 및 사용성을 강화하기 위해 어떤 성과를 내고 있는지 중점적으로 살펴보려고 한다. 우리는 유엔과 경제협력개발기구(OECD)가 사용하는 프레임워크를 적용한 비교 프레임워크를 활용해 유사점과 차이점을 규명할 예정이다. 한국과 페루의 비교 연구를 수행하는 시의적절하다. 왜냐하면 페루는 한국의 디지털 아이덴티티 제도의 모범 사례와 좋은 교훈을 활용할 수 있고 더 나은 정책과 결정을 설계할 수 있기 때문이다.

본 연구에서는 한국과 페루의 ICT 전문가와 온라인 인터뷰를 통해 양국의 디지털 아이덴티티 체계에 대한 심층적인 이해를 창출하는 정성적 연구 방법을 활용하였다. 총 10 명의 전문가를 인터뷰했는데, 전문가와의 인터뷰는 한국과 페루의 디지털 아이덴티티 진화에 대한 개요를 제공하고 페루의 디지털 아이덴티티 제도 구현 과정에서 발생하는 과제를 식별할 수 있다.

디지털 공공 서비스의 개발 및 제공을 지원하기 위한 강력하고 지속적인 디지털 리더십, 시의적절한 법적 프레임워크, 현대 ICT 기술이라는 세 가지 요소에서 큰 차이가 나타났음을 알 수 있었다. 하지만 이 연구결과는 또한 페루에서 디지털 아이덴티티 생태계를 조성하기 위한 목적으로 제도적 정비를 하고, 규제를 개선하며, 예산을 최적화한다면 큰 성과를 얻을 수 있음을 시사한다.

주요 키워드: 디지털 아이덴티티, 디지털 정부, 디지털 변환, 디지털 아이덴티티 전략

Acknowledge

I would like to thank my family (Rosa, Yuri Mariano, Gabriela and Hedda) and friends for supporting and encouraging me during the formulation of my thesis, without their words and good vibes this journey would be impossible.

Besides, I must thank the Professor Kilkon Ko and my advisor Professor Mr. Junki Kim, who really inspired me to be a better person and professional. Many thanks to Mr. Yongmi Lee and GMPA staff who remember me all the time my administrative duties which I used to forget.