Title	Virtual ID card : the future of identity proofing in Oman
Sub Title	
Author	Albusaidi, Almuhannad(Sunahara, Hideki) 砂原, 秀樹
Publisher	慶應義塾大学大学院メディアデザイン研究科
Publication year	2021
Jtitle	
JaLC DOI	
Abstract	
Notes	修士学位論文. 2021年度メディアデザイン学 第866号
Genre	Thesis or Dissertation
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO40001001-00002021-0866

Master's Thesis
Academic Year 2021

Virtual ID Card: The Future of Identity Proofing in Oman

Keio University
Graduate School of Media Design

Almuhannad Albusaidi

A Master's Thesis
submitted to Keio University Graduate School of Media Design
in partial fulfillment of the requirements for the degree of
Master of Media Design

Almuhannad Albusaidi

Master's Thesis Advisory Committee:

Professor Hideki Sunahara	(Main Research Supervisor)
Professor Hiroyuki Kishi	(Sub Research Supervisor)

Master's Thesis Review Committee:

Professor Hideki Sunahara	(Chair)
Professor Hiroyuki Kishi	(Co-Reviewer)
Professor Keiko Okawa	(Co-Reviewer)

Abstract of Master's Thesis of Academic Year 2021

Virtual ID Card: The Future of Identity Proofing in Oman

Category: Science / Design

Summary

Technology has been an essential part of today's world, and nothing can be done without it. Meanwhile, all the systems have shifted to digital media and software that people nowadays use digital apps to access their private data. Some users who don't have much awareness are taken advantage of by people who try to hack their personal data spoofing.

This research paper is a deep and thorough collection of all the research papers and mainly concentrates on the importance of proofing identity in Oman. Moreover, it aims to present how digital mechanisms can be used for identity proofing, how the Advance authentication process would make people's lives more accessible, and how cryptography facilitates the users who have previously experienced spoofing. The advanced authentication process has made the whole process much easier and less time-consuming. Advanced authentication ensures the protection of the user's data by providing secure options to access it digitally.

Furthermore, it gives more security options like passwords, one time pin "OTP", and bio-metric data. Cryptography is also used to keep the data secure; it is used in applications such as internet banking transaction cards, the passwords of laptops, and commerce transactions. It provides confidentiality, reliability, security, integrity, and data protection by assuring information guarding and authentication.

Keywords:

Electronic services, Digital identity, E-transformation, Digital government

Keio University Graduate School of Media Design

Almuhannad Albusaidi

Contents

List of Figures

Acknowledgements

Malcolm X once said, "The future belongs to those who prepare for it today".

The above quote has inspired me to pursue the knowledge and excellent education that would benefit my community and my beloved nation. I have always believed in the importance of gaining knowledge, especially internationally, as it provides an outsider insight and different perspective in education and other aspects of life. Moreover, I think the opportunity to acquire an international educational experience had allowed me to enhance and expand my intellectual abilities and positively influence developing multiple skills.

First, I want to thank my family, wife and daughter, and parents for their endless support from the scholarship application until the last examination in my degree program. Their encouragement gives me the strength to continue my journey easily and overcome obstacles and challenges without any matter.

Furthermore, I would like to thank my supervisors' professors Hideaki Sunahara and Akira Kato, for their constant assistance and guidance through my research and their motivation to explore new ideas in my project. Also, I thank my colleagues in the network media research group for supporting time and enriching my knowledge by taking part in their weekly meetings and listening to their great ideas and projects.

Additionally, I thank Dr Amer Dheedan for his teachings and mentoring me from my undergraduate period until now. His infinite motivation, belief in my potentials and guidance encouraged me to seek knowledge and continue my studies in any University in the world.

Furthermore, I thank my sponsor, Sumitomo Corporation, for sponsoring my study and giving me the chance to live and study in Japan and experience everything it could offer, such as the rich culture and fantastic nature. Likewise, I appreciate the efforts of Asia Seed employees and their assistance in all aspects related to life in Japan.

Finally, I acknowledge the graduate school of Keio media design for providing me with a fantastic life experience to enlighten my future and expand my prospects. Also, I express my gratitude to my friends, classmates, and college faculty, who enrich and positively influence me by providing knowledge and different perspectives through valuable discussions, ideas and expertise during classes and workshops.

Chapter 1
Introduction

"There is a way to do it better-find it ", Thomas Edison.

Towards the soon future, the whole world stepping too fast to catch up with the technology, to improve the humanity lifestyle. By Looking deep into the culture around, many barriers are slowing down the development wheels in the country. Based on this principle, an existing idea in Oman matches with a new scheme that leads to a brain map for Innovation to be born. This Innovation will encourage advancing development in the Omani society and worldwide.

The Omani society is based in the sultanate of Oman, an Arabic and Islamic country located on the Arabian Peninsula, known as part of the "middle east". It is one of the oldest self-governing states in what is known as the "Arab world". Oman is divided into seven governorates, and each has its main tribes and families with different cultures and views. Moreover, the geographical, natural and cultural diversity of Oman makes some challenges to unify the services provided by the government to the community, such as the service that require identity proofing.

Through the years, Oman is considered a developed country with a vision of converting its standard government into the new model of "e-government". "E-government" uses technological communications devices, such as computers and the Internet, to provide public services to citizens and other persons in a country or region. E-government offers new opportunities for more direct and convenient citizen access to government and government services directly to citizens [1]. However, still, a lot of documents are required to provide those services, and personal information needs to be presented, typed or photocopied. Although the idea of an ID card with multiple functions, integration and benefits will be a big step for any country to keep up with the world development speed. Nevertheless, copying or typing the information will cause an issue on the accuracy levels of the information required, affecting the speed and quality of the service processes.

1.1. Statement of problem

From the past era to the current days, the procedure of identity proofing prerequisite several steps to apply and receive any services. Moreover, identifying persons relies on the human element by comparing some information on the card to visible beforehand. Firstly, a physical ID card, must be submitted to the service provider to confirm the person's identity. Furthermore, a manual comparison between the personal photo and the look of and the ID card bearer affirms that the person is the same in reality. Secondly, to make sure the information provided in the card with the person seeking the service is correct. The service provider might ask some verbal questions about some info on the card or stored inside its microchip.

Thirdly, some personal information that doesn't appear on the card needs filling in the application form. For instance, the complete home address, phone number, and email should be handwritten by the applicant. Before receiving the requested service, as the last step, a photocopy ID card is taken as proof that the person has applied for such a service. Finally, a hand signature may be necessary on the photocopy of the ID card.

From the existing proofing process, it's noticeable when specific information is copied or typed, they are high chances to forget some information, or by mistake, a letter is typed instead of another. This process may lead to incorrect data, which will result in imperfect information. Moreover, relying on a non-systematic mechanism means there are high possibilities of inaccuracy in identification, which means this could be an issue, especially in forged or fake identities. Therefore, The accuracy levels are possibly low by using non-digital mechanisms to prove identity while applying for services, which is considered the main problem.

1.2. Motivation

While the population is growing worldwide, the variety of services provided by the government and other sectors are increasing with the development wheel. ID cards have become essential documents not just to prove your identity but to request and receive services. Moreover, it has many possible potentials that could expose if it developed in the right way, presenting new ideas that would enhance

people's lifestyles and ease receiving all kinds of assistance from all sectors.

Furthermore, it is one crucial part of digital transformation in Oman, which aims to shift providing services in traditional procedures into a new era of digital and online services available for public consumers all the time. Hereafter it's become a necessity to make significant technological changes in the domain of services to facilitate utilities for the country's people, which would benefit both the individuals and those in charge of providing services.

1.3. Research objectives

The main objective of this research paper is to acknowledge readers about:
-The digital mechanism of identity authentication in Oman
-The importance of digital cards in Oman's digital transformation
-The unified digital identifier for all services in Oman

Identity proofing is a vital process to apply for any service. It ensures that only an eligible person is requesting that particular service. Moreover, it checks if the person who asks for the service is who they claim to be or not. Furthermore, It provides some percentage of justice for all the people living in the country, so only entitled persons to receive service.

This research aims to replace the mechanism of identification, which is presently using standard methods to prove the person's identity while applying for services provided by public and private sectors. Moreover, it would provide a digital mechanism for identification procedure, which could eliminate the weakness of human intervention and replace it with electronic process. This process would increase the accuracy and credibility of the ID card by introducing the latest technologies such as bio-metric data, which is known for its distinctiveness and difficulty to counterfeit or replicate even if very high techniques are used for it.

In addition, this objective is to propose a digital platform that could integrate electronic systems of public and private organizations with the proposed digital platform. This digital platform would ease the flow of information and data between all related parties. Besides, it would provide a secure channel for data transmission, which may help reduce the risks of cyber attacks and the possibility of data breaches.

Moreover, multiple physical cards are currently issued by government units and require regular people to carry them at all times, such as national ID cards, driver license, labor cards, etc. Although every card has its distinctive purpose, they are all linked and belong to one person. Having multiple cards requires financial investment to issue those cards and operate public offices to apply and receive cards from those offices. Moreover, it means having different systems to manage those other cards, adding extra pressure in various government aspects to succeed in operating them all.

Therefore, having a unified digital identity card for all services could be more convenient and reliable, offering many benefits to governance organizations by having all information related to a person combined and available in one digital platform. Additionally, it may reduce costs to produce such cards. Also, it can enhance security by proposing new methods to use and operate the new digital cards to help transform all given services into fully digital, which may ease access to those services and reduce the necessary time to perform and complete applications.

1.4. Proposal

National ID cards in Oman are vital documents. They include personal information and other related data, such as a copy of the card bearer's hand signature. It is the official and standard proof of a person's identity, registered at first card issuance and then linked to a person's identity to be used as an identifier in future applications, processes and services. Consequently, whenever that person requires to prove identity, they have to submit a copy of their ID card and sign on an official paper provided by the organization which provides the service. However, hand signature proves in many cases to be an insecure element to be used as a unique identifier, as it is easy to forge and copy, making it less convenient to choose as a secure identity proof.

In addition, although the Omani government emphasizes the digital transformation of services provided by both public and private sectors, the process to verify identity while applying to those services is still a standard non-digital process. Moreover, while requesting most of the services, the applicant must submit

a physical copy of the ID card to the employee of that organization. The employee would examine that card and check information written on or stored in it. Then the applicant will need to sign the application to verify his identity, which the employee also does. However, doing such a process would take time first to check the info and compare hand signature, then doing the entry process in the organization's system physically. Moreover, comparing hand signature copy on the card and application paper could be uncertain as it is not a systematic digital procedure. Therefore, the accuracy of such a process might have low percentages of success compared to the same operation done digitally, and there is a need for an electronic approach to verify personal identity rather than physical examination.

Additionally, in Oman, some social and cultural restrictions may affect identification and make it challenging to succeed. For instance, to compare the look of the applicant and the image on the ID card the person who makes the regular identification need to take a deep look on applicants face, which is not accepted in the culture to look deeply on women's face. Moreover, in the current situation, some information such as full name, birth date and place, etc., is print on the card itself, besides some other data stored inside the microchip. However, people think they don't have control over their data, as they can't decide which information should be available while applying for a specific application or service.

Based on all those factors discussed, this research proposes a virtual ID card that could be either an application installed in smart devices such as smartphones and tablets or a digital portal available on the internet web. Moreover, this proposal would provide a digital mechanism, which would ease the transfer of data and information from card bearer to service provider. Furthermore, this method would increase the speed of completing identity proofing using a digitized mechanism to transfer the data without doing any paperwork like copying the id card.

Moreover, it will introduce advanced authentication technology, such as biometric data, known for its unique characteristics and difficulty replicating by identity theft. Also, the security would increase by using a very secure network like peer-to-peer and cryptography, which will encrypt the data moving from the user to the service provider Furthermore, the research may plan to target the people in Oman between 21 and 60. We choose this age group because they are

aware of using technology appropriately and utilizing it within legal boundaries. Furthermore, this targeted group will include the minimum legal age in the country to apply for most services provided by all sectors without the need to have a guardian like people less than 18 years old. Additionally, the people above the maximum targeted age either retire from work, as per local laws or have special treatment while applying for services. Therefore we only recommend targeting choosing age group in the first phase of implementing virtual Id card solution.

In addition to identity proofing, the virtual ID card is expected to act as a hub that combines all services provided by all sectors in one digital place, which will help expand integration between units and government within the country. Moreover, it would offer the ability to check the personal information, periodically update variable data such as a home address, and select sharing only required information by service providers. Furthermore, it would solve some social and cultural issues related to existing ID cards, such as the influence of family names on receiving services.

1.5. Research goal

As mentioned in the previous section, a standard way is currently used to prove the identity of any person in Oman. This traditional way consists of physical attendance to the service office as a prerequisite. After that, an ID card needs to be submitted to the employee of the service provider. Then a lengthy physical id card examination is conducted, a copy of the id card will be taken as reference proof that the applicant requested and provided this service. Moreover, a signature may also be required to add extra authentication of that application. However, this process is taking time to serve each applicant. Its accuracy would decrease within time because the employee might get tired or try to finish a large percentage of requests by checking documents quickly.

Consequently, to increase the accuracy and efficiency of identity proofing in Oman, the researcher aims to present a digital process or mechanism to prove a person's identity, accelerating digital transformation in Oman by providing services online and authenticating identity without the necessity to go to services providers offices.

1.6. Contribution

This project proposes a new idea of identity proving and personal information, which could be available digitally. Furthermore, It helps people to be easy and secure access to their information such as personal details. The primary purpose of this project is to enhance and improve the mechanism of identity proofing by using bio-metric technology to validate a person's identity and ensure only authorized person could access and use that information whenever needed. Moreover, it aims to replace existing physical ID cards that has some challenges to use them, like finding a copy of them or extracting stored information inside their microchip. In addition, it offers a new capability to the card owner of controlling shared information with any requested party, either its private or government unit, which may solve some social and cultural issues related to existing cards.

The research will start by examining current identity cards and what kind of technology they use to achieve their target. Then, it will move to evaluate the benefits that they possess and work on some methods and procedures to enhance them, and determine potential risks and disadvantages to find a proper solution to not fall in them. In addition, it will examine some initiatives from different countries around the globe, which's already started to experiment, develop or work on more similar ideas or technologies to provide their people with the highest value of satisfactions and top electronic services. Furthermore, this research will evaluate and take some positive points that could be included in proposed solution,

Furthermore, a new process will be developed to verify identity and control shared data and information with all related parties. Then, an interview will be conducted with different potential users or benefices of the virtual ID card to examine their perception of this new concept and get their feedback and comments about it. Finally, the research will propose a prototype that could simulate how the new idea could work in reality and how the users could interact with it. At the end of this research, it's expected to achieve some or most targeted goals.

1.7. Background Information

An identity card is a card in which any citizen of a particular country is identified based on a specific identification number. Each citizen is assigned an identification number that acts like that person's identity.

The identity cards were introduced in 1987 in Oman; however, the global standardized ID card size was decided in 1985 according to ISO 7810 standards. The latest ID cards have a microchip inside them, which stores personal data like name, residence address and other related information. Furthermore, it is easy to read the information electronically, which helps to extract accurate data. However, currently, traditional ways are used in identification, and the identity is not verified electronically, which means citizens required a physical submission of documents before applying for any services.

Nowadays, digital ID cards are used in many places globally. For example, in Colorado, a digital card has been introduced, ensuring legal personal identification. The world is progressing, and the digital mechanism of identity proofing has become a necessity to provide quick and quality services. Moreover, the advanced authentication process has made the whole mechanism process much easier and less time-consuming, plus more accurate and secure.

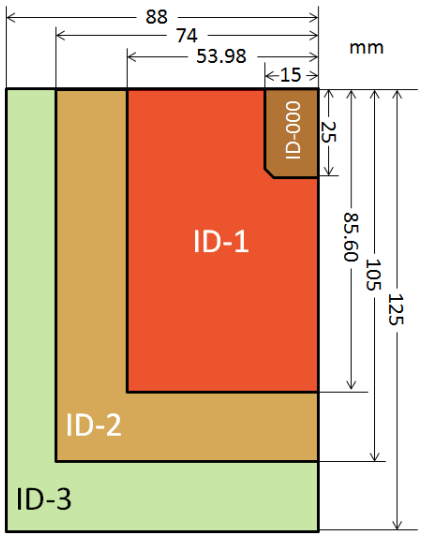
In addition, Cryptography is one of the main factors that ensure the security of data, which provides confidentiality, reliability, safety, integrity, and protection of the data by assuring information guarding and authentication process.

Chapter 2
literature review

2.1. Overview of Identity cards

Identity (ID) cards are an identity document known as identification or(IC, ID card, citizen card, etc.). This document used to prove a person's identity. Mostly, it issued in a small, standard credit card size form. It is usually named an identity card [2]. ID cards typically have a photo of their bearer and other essential information like full name, age, date of birth, home address, identification or national number, card number, gender, citizenship and more. The size and shape of ID cards were globally standardized in 1985 by ISO/IEC 7810 [3] as illustrated in Figure 2.1. In addition, specific physical characteristics were defined and standardized by ISO, including card materials, construction and dimensions of four types of cards sizes. Those four cards sizes are ID-1, ID-2, ID-3 and ID-000.

The main requirements for ID cards are bending stiffness, resistance to chemicals, toxicity, durability, dimensional card stability and warpage with temperature and humidity, resistance to deterioration from exposure to light and heat [3]. ID cards become an essential document to prove who they are before attainment access to multiple services, such as banking, healthcare, education, government services, etc. For example, you cannot open a bank account or request governmental service without providing it to authorized personals in many organizations. Therefore, in most countries, governments have a decisive responsibility to provide their citizens with identity cards by offering them a secure and long-term document to use in both physical and digital worlds.



(Source:ISO/IEC 7810 Identification cards)

Figure 2.1 Illustration of ISO/IEC 7810 sizes in millimetres

2.1.1 Evolution of ID cards

The idea of the national ID card started a few centuries ago. It initiated a proper record of people living in one country besides simply recognizing them accurately whenever there is a need to verify someone's identity. The first model of national ID cards emerged during the 19th century in France. It introduced a system of internal ID documents for workers. Yet, the French pass cards intended for only workers travelling across France, other countries in Europe, such as the Ottoman Empire, implemented more comprehensive ID systems than France. However, most countries started to adopt national ID cards systems after World War II [4]. In the past, most ID cards made of paper materials and all the information handwritten by employees in the issuance entity. This process has a considerable drawback of finishing one card because it relies on human power. It also fails to copy the information from physical records and raises the chance of inaccuracy in basic information related to the card owner. However, this process replaced during the last decades by accurate and efficient printing machines that prints multiple cards in a brief period. In addition, modern cards considered to be smart cards. As a definition, a smart card or chip card is a physical and electronic authorization

device used to control access to a resource. It is usually a plastic card in credit card size with an embedded integrated circuit (IC) chip [5] as shown in Figure 2.2. Moreover, most smart-chip cards include a pattern of metal connected to the internal chip electrically. Smart cards can also offer personal identification, authentication, data storage, and application processing [6].

Traditional techniques of identity verification are outdated in the new digital world. In the present time, most identity documents such as ID cards and driving licenses are issued in a physical format and issued from specific locations (Government authority). And with the emergence of information technology in the last era and its integration with many parts of people's daily lives, the necessity for a digital ID card to replace standard ID cards has become a vital fact. Digital ID card is a fundamental enabler for modernizing public services such as healthcare, education, licenses and permits. From a government perspective, using this technology improves administrative efficiency—reducing paperwork, speeding up processing, and reducing the risk of identity fraud. Furthermore, improve accessibility for citizens, eliminates potential mobility costs, and minimizes the required time to apply and receive services. Beyond public services, a digital ID card may also support citizen participation, for example, through electronic voting. However, preserving high levels of security most significant challenge when it comes to digital ID cards.

2.1.2 Advantages of ID cards

Multiple countries worldwide, including the middle east, are issuing advanced national identification cards and oblige their citizens to carry them all the time. Also, they need to display them whenever they apply for public and private services, such as banking and money transactions services. Using those identity cards creates extra trust and accountability in the identity system.

There are some broad benefits of possession and using new ID cards, especially the latest generation, which contains all information related to the person who carries them. Initial, those benefits could contribute to countries national security by proofing identity efficiently and competently, leading to controlled details about individuals and eliminate or decrease the risks of misusing the identity [7]. For instance, to use ID cards with a microchip, a pin, or a password might require

(Source:National identity card (Sweden))

Figure 2.2 National ID with micro-chip

using the card to verify somebody's identity. This feature would add an extra layer of security to the card so that the only authentic person is authorized to use it. Additional, the cards would prevent or reduce the chances and possibility of identity theft and fraud by having some security features on the card, such as hologram prints and embedded codes.

Moreover, ID cards would effectively deliver government services to targeted and only eligible citizens or ex-pats living in the country, such as health care and education. For example, using the ID card helps to avail associate information related to a particular person. So in emergency cases, the hospital or any Health institution could obtain important information about medical history. Also, in other cases, if the person is unconscious, they could identify him/her by that particular card. Furthermore, ID cards could support governments trend to offer a variety of electronic services via the Internet or public portals and act as an enabler for both individuals and entities towards more access to those services.

2.1.3 Disadvantages of existing ID cards

With the introduction of any new technology, some challenges could face it and decrease its success or progress. For example, implementing an ID card system can be very expensive. Hence, it is not surprising that some countries stopped in a particular generation of ID cards because current cards might be enough to fulfil their requirements and needs. Additionally, acquiring a new system for identity to replace the existing might require huge investments and high costs at the beginning of such a project. For instance, according to James Hall, who heads the Identity and Passport Service, £257 million has been spent developing the identity card scheme in the United Kingdom before it was abandoned [8]. Moreover, there is an increased risk of fraudsters acquiring people's identities. For instance, all national ID cards have a unique number(national number). It would be a tremendously trusted identifier and would be used widely by many organizations. Yet, it would eventually be more accessible for fraudsters to obtain the information without proper permission [9]. Therefore, there should be an adequate security measure to ensure the safe use of ID card by only authorized persons. However, using regular PINs to check a person before using the ID card might also be considered a risk if the pin falls into the wrong hands.

Additionally, traditional ID cards still in use in most countries are in physical form and lack security features, making it difficult to copy or duplicate or forge an identity. So maybe the fake ID card won't apply for government services or any process that could expose its owner. Still, it could help get some unauthorized products such as buying cigarettes by people under the legal age to purchase such a product. Furthermore, the physicality of the ID card makes it a potential threat by damaging the card or losing it. Furthermore, some advantages of ID cards, especially the new generation, which has microchip, could be considered as a potential threat at the same time. Microchips, which are embedded inside ID cards, store all information related to their owner. In some countries, there are no proper security techniques to protect this information. In other cases, a high technology might be available in other countries, making extracting data from that microchip isn't a tricky thing to do, leading to the possibility of stealing the information and the potential of misusing it. Moreover, those identity thieves perhaps sell specific data to companies interested in such info for their profit.

In summary, the current ID cards lack high-security levels, making them a very risky information document to lose. Moreover, the physicality of standard ID cards makes them fragile and easy to be stolen or misuse if it falls into the wrong hands. Furthermore, although having the capability to store information inside them is advantageous, it makes them a regular requirement to use or apply for any services with integrated authorized organizations. However, that didn't fully support the digital transformation and didn't aid towards the full benefit of possible electronic services.

2.2. Related works

Many countries around the world have adopted or developed new types of identity cards. Some of them kept the current physical ID card with some new features. Other countries advanced and introduced a new concept of digital cards as future generation and natural successor to standard ID cards.

2.2.1 Micro-chip cards in China

Figure 2.3 National identity card in China

ID card is known as "The Resident Identity Card", an official identity document for personal identification in the People's Republic of China. According to the Resident Identity Card Law, residents must apply for resident identity cards designated by government offices throughout the country [10]. Before the year 1984, it wasn't required for citizens of China to acquire identity card. However, in 1985 new identity card act and a unified authority has been appointed to become responsible for regulating and governance of those new ID cards. As a result, from 2003 on wards, an estimated 1.14 billion cards have been issued in China [11].

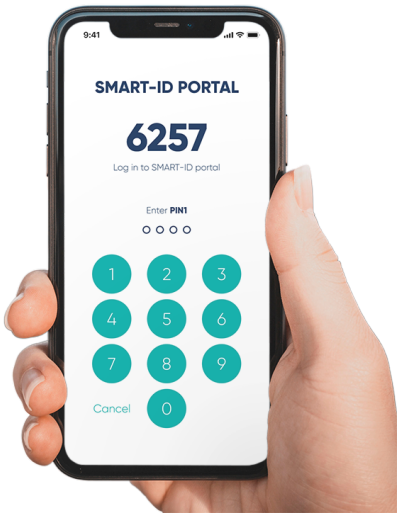
Basic information is printed on cards such as full name, gender, ethnicity, date of birth, etc. The ID card evolved through two generations, where the first generation was a simple plastic card, while the second generation card, as shown in Figure 2.3, contains a microchip that stores personal information. The main criticism of china's id cards that they use older technology, which is similar to the technology used for transportation cards, which lacks the proper encryption of personal data, making stored information accessible by any card reader [12].

Chinese administration has progressed throughout the years and always tries to use technology in many aspects that benefit both individuals and government. However, the national ID cards developed rapidly. They failed to match or imitate successful examples around the euro, leading to electronic or digital cards maybe because the scalability of the country and the vast population makes it challenging to move forward to a newer version of ID cards. Besides the cost to shift to a new system and difficulty administrating and managing many such cards.

2.2.2 Digital cards in Estonia

Estonia is well known as one of the top countries in the euro that rapidly develops its ID card during past decades. Besides being an identity proof document in Estonia, physical identity cards establish personal identity in an electronic environment and provide a digital signature for every person. Moreover, Estonia offers over 600 e-services to citizens and 2400 to businesses that could be accessed using an ID card [13]. In addition, all leading banks, many financial services support ID card-based authentication.

Like most countries, Estonia introduces a new type of ID cards. The card contains a chip that stores digitized citizens' data, including complete informa-



(Source:smart-id.com)

Figure 2.4 New concept of smart-ID in Estonia

tion, and most importantly, cryptographic keys and public key certificates. The cryptographic-key primary purpose is to encode or decode cryptographic data. Therefore, the significant strength of this key is to ensure high levels of security while exchanging data between two or more parties. The chip has two interfaces: regular contact interface and contact-less interface (NFC). It enables services to authenticate the user by a wave of the ID card. Furthermore, the capacity of the new chip has increased, allowing to add new applications such as electronic tickets in public transportation or other electronically issued certifications [14]. In addition, millions of digital signatures have been provided in Estonia since its first introduction in 2002.

Furthermore, a Mobile-ID introduced to citizens of Estonia in May 2007. To get a Mobile-ID, the user needs to replace his SIM card with a PKI-capable one. As the mobile operator performs the registration process, it is not considered trustworthy enough. Therefore the user needs to activate Mobile-ID with their ID card. Thereby issuance of the Mobile-ID is bound to the security and quality of the ID card. Mobile-ID certificates contain the exact personal information on the subject. Mobile-ID provides certain advantages for the end-user than the ID-card: the user does not need a smart card reader or any specific software. Currently, the

Mobile-ID is available from one mobile operator only, and the number of active users is below 100 000.

Since the establishment of Estonia ID, everything was working smoothly without any significant issue. Nevertheless, in 2017, a security threat affected around 750000 ID [15]. The responsible organization for the ID cards has released an update and published the detailed walk-through of performing it and its particular website [16]. However, they temporary suspend the update due to the imminent risk of cyber attack and disable all affected cards [17]. The Estonian id cards are one of the tops not just in euro but globally. They might have some problem as multiple cards offer similar services such as Mobile-ID, Smart-ID and regular ID. If all cards combine in one complete solution, it will make it easier for them to have one united platform. Also, it will reduce costs for the government to develop and maintain a single application and simplified the control and management of ID solution.

2.2.3 Identity documents in United States

United states always have different rules and regulations from other countries around the world. For instance, issuing identity and drivers license is in a regional-state based in the sense that no federal agency with nationwide jurisdiction directly gives an identity document to all US citizens for mandatory regular use. Therefore, no national government organization is responsible for providing that kind of cards, and there is no unified ID card for all citizens living in the country.

The Social Security number (shortly known as SSN) is a card issued by the Social Security Administration in the United States. Almost all legal citizens have it, even young children. In the absence of a unified national identity card, the Social Security number has become the de-facto national identifier for an enormous variety of purposes, both governmental and non-governmental services. However, social security number isn't the best choice to be used as a unique identifier because it doesn't have a personal photo printed on it and doesn't have an expiry date or require to renew it. Therefore, the card is not commonly considered as proof of identity. Instead, it only proves that the person named on the card holds the number indicated on the card.

Colorado digital card initiative

(Source: mycolorado.state.co.us)

Figure 2.5 MyColorado digital portal

Although most states have a standard ID card, Colorado has initiated a new digital ID card in 2019. It is part of my Colorado mobile application with multiple electronic services provided by secure and convenient access to the state government services from any place and time. The application (MyColorado) as shown in Figure 2.5 is a collaborative project between the Governor's Office, Office of Information Technology (OIT), Department of Revenue (DOR), Division of Motor Vehicles (DMV), Colorado Department of Public Safety, and Colorado State Patrol [18]. This digital card replicates the Colorado driver license and state identification card and provides state residence with an electronic version available on their smartphones. Moreover, by the force of local law and executive orders from the provincial governor, this digital ID card is recognized as a legal form of identification and could prove identity within the state. Thus, this kind of digital ID card significantly impacts the digital transformation of state services, which provides convenience and fast access to those services. Moreover, it offers all information related to its citizens in a secure place.

However, this digital ID has concerns like renewing the digital ID card simultaneously with a driver and state ID card. Yet, this procedure is not very convenient, as it bonds the digital ID to the physical ID card, which means the digital ID is only an extension of the other and not an independent identification document.

Moreover, the requirement to always present the physical ID card and the digital ID card simultaneously serves as an extra verifying factor, ensuring that only authorized person's carry and use digital card. Therefore, this process could present inconsistency on identity proving besides decreasing the importance of the digital ID card, which is supposed to replace the standard ID cards subsequently.

Without any doubt, the Colorado digital ID card initiative is the exact replacement for current ID cards. Therefore, it could be considered a bright example of how digital ID cards would help better transform digital services in the aspect provided by all sectors within the country. Furthermore, I expect that Colorado digital ID will evolve as a national standard identifier in the United States. Additionally, it possibly will be adopted to be the example that other states would follow, with the capability to use it not just in Colorado but within other states across the country.

2.2.4 Finland shift to digital ID cards

The first Finnish ever operational national electronic ID card scheme was introduced back in 1999. In the following years, the second generation of ID card which has a chip, was announced. It enables digital signature instead of old one and allows a secure transaction with public authorities, businesses, and other service providers by the Internet. Furthermore, a new integration between health insurance and ID cards established. This integration combines the two cards into one. Making the persons carry one card instead of two. To offer the latest technology and solution for identity cards following their neighbour country's steps (Estonia). Finland aims to establish its digital ID card during the upcoming years(2023) [19]. The main goal of the Finnish government is to develop electronic ID cards for all the people living in Finland. Using this new card, the users can manage personal information and access public services from a unified portal. Those public services expect to have adequate support and would ensure equality for everyone. According to the responsible authority, the new digital ID card will be easy to use for individuals, even those who have difficulty using mobile devices and other digital devices. Moreover, the mobile application won't be the only option to access the digital ID as the authority propose an alternative device (pen) that can connect to computers. Furthermore, the digital Id card will help individuals authenticate

themselves and make business and digital transactions via web services [20].

Lately, Finland partnered with Estonia to develop a joint data exchange platform that provides electronic services mutually accessible for citizens of both countries. This platform would support ID cards in both countries and recognize electronic signatures as well. Finland is gradually changing and developing its identity card and starting the transformation to a digitized form of cards, which is the expected future. Whether Finland succeed in the adoption of a new digital ID card or not. It is working on the right path and doing the right thing by partnering with other countries that already provide such a service and prove their success in this field.

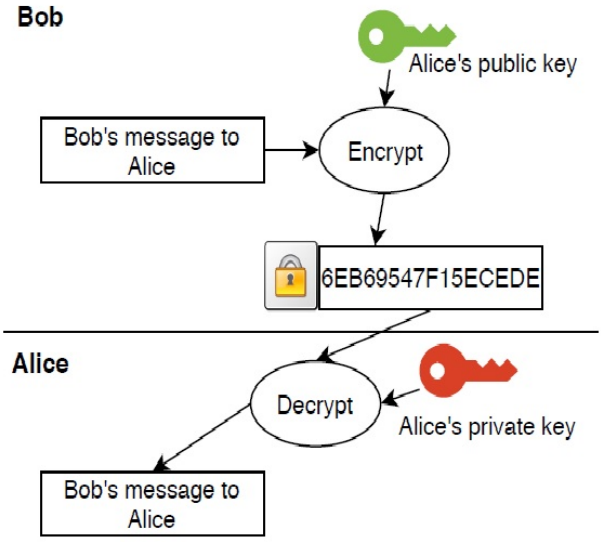
2.2.5 Block chain technology and identity verification

Numerous technologies developed and emerged to simplify processes and make the lives of individuals and corporations much more accessible. Blockchain technology is one of those technologies that made transactions easy, secure and decentralized. The definition of Blockchain could be simplified as distributed ledger technology (DLT), making the history of any digital asset unalterable and transparent. Moreover, the process goes through decentralization and cryptographic hashing methods.

Transnational records store as a block in several public databases in a network connected through peer-to-peer nodes as a chain. Blockchain is a promising technology because It uses a digital signature feature to conduct fraud-free transactions, making it impossible to corrupt or modify an individual's data without a specific digital signature. Furthermore, the transactions are done in common consensus between the users, making the transactions within this technology much smoother, safe and faster. Moreover, it combines leading technologies such as cryptographic keys and peer-to-peer network, which offers a high level of security and safety for processes and transactions.

Cryptography includes two keys, which are private and public. Those keys ensure the success of securing transactions between two parties. Moreover, each party has those two keys that generate a protected digital identity reference responsible for authorizing and controlling all transactions between them. In addition, Blockchain technology uses the hash encryption function to secure data

and information transmitted between two parties, relying on the "SHA256" algorithm. Practically, the "SHA256" algorithm encrypts all information exchanged plus the sender and receiver addresses, then adding it hash encryption to the Blockchain after verification. The algorithm contains a preceding hash, the hash address responsible for locating the previous block, transaction details, and nonce, an arbitrary number given to differentiate the block's hash address. The hash address contains 256-bit, a 64 character length value, making it almost difficult to hack this encryption. The figure 2.6 illustrates the encryption and decryption mechanism.



(Source: Towards a blockchain based digital identity verification, record attestation and record sharing system)

Figure 2.6 Cryptography mechanism in Blockchain

Identity is a claim about personality, consisting of name, birthday, nationality, and other identifiers such as ID cards, driving license, and passport. In many countries, governments issue such physical documents and store their information in centralized databases. Although identity data is related to people's identity, they don't have complete ownership or control. Nevertheless, Blockchain technology could solve identity issues such as inaccessibility, data insecurity and identity

fraud. Moreover, Blockchain identity solution using mobile phones could propose a suitable alternative to physical documents, as mobile phones become widely used by different people in society.

Additionally, Blockchain could introduce enhanced secured access and personal identity data exchange between the organization that stores citizens data and other related counterparts such as citizens and private organizations. Furthermore, moving towards digital oriented services for the public without having a proper standard identity makes it a weak link between real identity and digital identity, making it more exposed to fraud and deception of identity. However, using such a sophisticated technology with advanced cryptography could set a framework to be the base for future digital identities. The virtual ID card is one of those digital identity concepts that could use mentioned technology to achieve its objectives and solve regular ID cards.

There is a concept within Blockchain technology called "identity and access management", which involves processes and technologies in a particular organization which used to identify, authorize and authenticate person access to services or systems in that organization.

The first model of digital identity management was a siloed one. It proposed that each organization issued a digital identity credential to a user to access its services. Moreover, the user needed a new digital identity credential for every new organization he engages with, which resulted in a poor user experience. The second model of digital identity management is called the "Federated" one. Because of the poor user experience of the first model, third parties began issuing digital identity credentials that allow users to log in to services and other websites. The best examples of this are "Login with Facebook" and "Login with Google" functionalities. Companies "outsourced" their identity management to significant corporations with a financial interest in gathering such large databases of personal data, which resulted in raising privacy and security concerns [21]

In summary, Blockchain technology offers an advanced approach to verify and prove identity by using high-tech methods to encrypt data exchanged between two parties, resulting in high security and minimum chances of data leakage or hacking. Moreover, the technology used in the network that links all related parties offers a fast, smooth and safe connection and exchange, resulting in a

reliable, secure network. Therefore, the virtual ID card could use the Blockchain identity management model to authorize access to the users by verifying their identity using its unique mechanism. Also, ensuring required information is send and received in exceptional levels of protection and security between related parts.

Chapter 3
Overview of identity cards in Oman

3.1. Digital transformation in Oman

In many countries worldwide, governments have developed strategies to support the digital transformation of the services they provide. Digital Transformation is an essential asset for government and private sectors to deliver those services to the beneficiaries comprehensively and efficiently. Moreover, It would benefit the workflow of the services to the targeted customers or users in an easy and fast manner. As a result, digital transformation could reduce cost, save efforts, and improve operational efficiency and services. Furthermore, it may simplify them to propose new innovative services that will increase access to them and enhance customer satisfaction.

The Omani government considers the digital transformation program highly critical for supporting the strategic and vital sectors in the Sultanate. It has a significant impact on the national economy, and it is one of the essential requirements of modern lifestyles, facilitating services and procedures for beneficiaries in diverse fields

3.2. ID cards in Oman and common issues

ID cards are essential key document to prove identity whenever required to apply for public and private sector services. Furthermore, the government made the ID card a fundamental prerequisite for most services to have a unified document and encourage citizens to register their information in their national data registry to have updated information about all citizens.

The latest type of ID card is typical, as the last generation of cards used in many countries globally, which has a microchip that stores bearers information inside it. Although, storing data might give the benefit of extracting helpful information when needed by any official entity. Yet, it draws into the issue of falling into the wrong hands. With the existence of significantly advanced devices that could crack card security and extract its data, it can consider as a downfall to this type of card. Alongside that matter, governments spend a large amount of money on the cost to issue new cards and discard old ones. Moreover, it extends to the operating expenses of local offices, which has many employees to serve all the country's population.

3.3. Oman's special requirements for identification

In every culture, there are some social requirements or limitations for certain things. Oman is a country located in the middle east and has unique social and cultural traditions, some are different, and others are similar to neighbouring countries in the Arabian Gulf. For example, it's not acceptable for women to wear certain clothes because of religious and cultural values, or they may need to cover their hair and face. Those cultural requirements make identifying a person challenging and require a systematic approach to solve such problems.

Furthermore, there are some issues related to current ID cards unique to Oman's case. For instance, the overlook of persons is different in the photo taken for ID cards and the traditional look of a person. Moreover, it is mandatory to wear the national dress in the official image of any person, whether the person is a man or woman. Men must wear a white dress with a head turban (known as musar) for their official photo. Also, women are required to wear a headscarf with a dress for the same image. In the existing situation, identification happens by comparing a person's physical appearance with the photo of an ID card. Moreover, this procedure is basic and use human factor to resemble the image and the look. Most of the time, people don't wear the same official clothes during their daily lives while applying for certain services.

Therefore, most of the time, the accuracy of identification proof for people is

low and could be tricked in cases the forge of identity. Moreover, in the culture of Oman, ladies are well respected, and it's not acceptable to have a deep look over them even in case of identification. Besides, in other situations, some ladies wear Islamic face cover (like a mask) to cover their face, and it's not acceptable to ask them to remove that face cover to check their face for the case of identity proofing.In figure 3.1 it is obvious how the look of one lady could be different then the image on ID card.

Therefore, the person who conducts a traditional identity check could not take a deep look at the lady's face to compare it with an ID card photo. That may lead to inaccurate identity validation for such a person, then that would fall in giving a person a service which they may not be eligible to receive.

Figure 3.1 Different look of women compared to ID card

In addition, Oman as a society is tribal-based consists of multiple families from similar origins, which all form a tribe. Inside one tribe, there are ordinary members, and others are considered leaders or called in the local word "sheikh". Those

people have high status in any tribe, and their name has a significant influence on many things, like applying for specific services such as land from the government. The card holder's full name, including family or tribe name, is printed out on the card, and the title of the person, such as "Sheikh" shown on the card. Such information sometimes affects receiving the service, affecting how quick it would take to complete. This effect would injustice others who might wait in the same queue to receive the same service, but the details of family name or tribe name would have an unseen impact on the service process.

Additionally, in other cases, the details of family name or tribe name could negatively affect a person's social status. For instance, a person from a well-known tribe is applying for some financial support like older people support or retirement funding. The person who may work as a service provider might know that person family and then tell others that this well-known person has applied for such a service, which may embarrass the person who requested the support or put him in a position he wouldn't accept.

Moreover, Oman is a country with the majority of citizens who have Islamic beliefs. As you may know, in Islam religion a man is permitted to marry up to four wives. However, many people tend to hide the information about their second or third marriage to keep their family relationships strong and connected. In existing conditions, national ID cards store such details as marital status inside the microchip. While applying for some services, this information could be visible to employees working in specific organisations such as banks. Knowing this kind of information and sharing it with others might lead to reaching this information for the applicants family about his other marriages, resulting in social problems like asking to get divorced or others that could divide the family because of such a piece of information.

Furthermore, Oman is a country divided into Governorates, cities and villages (known as williat). The birthplace of a person or resident location for ex-pats is available as vital information to apply for any services. Those services such as healthcare and education are linked to the applicant's birthplace or resident address. For example, suppose a person's birthplace is Muscat city, and he had a medical emergency while visiting another location. In that case, it's not possible to get health care from hospitals in any area outside his city "Muscat". Therefore,

these restrictions would limit the ability to receive or apply for such services outside the residence city. To apply for those services, the applicant should either return to their city to get this service or change their address, which requires visiting local offices and going through a lengthy procedure to get that particular service.

This process is inconvenient for the people who live in the country, giving a negative impression towards government and private services. Also, it doesn't achieve the government vision of digital transformation by providing services around the day online from any place, using any digital platform. Moreover, it may delay or increase the required time to receive such services, which is not what it should be.

3.4. Solution and scope of work

The vision is to introduce an enhanced type of digital ID card, which is "virtual ID card". It could be an application installed in smart devices such as mobile and tablet or an electronic portal to access the world wide web. The virtual ID card would present multiple functions to the users like updating some information periodically, providing high-security measures to access and using the latest technologies such as bio-metric data and controlling shared information.

Moreover, it will combine all cards issued by government units in one place. For example, drivers license and personal data will be in the virtual ID card, so there is no need to own and carry multiple cards at once. Furthermore, it will enable integration with some government and private sectors services.

The solution in the first phase main targets is Oman citizens between the age of 21 and 60. Control shared data and information and authenticated electronically. In further stages, it might redevelop and add extra features to enhance users experience and value.

However, this solution might face some challenges to be successfully implemented and work in reality. Those challenges could vary, similar to not having legal support to give the user the right to own their data and information and share only those required by law. Additionally, technological challenges include not having proper bio-metric scanners to support the entire population covered during the first phase of the solution. Furthermore, the lack of IT literacy among

the targeted people or limited internet coverage could be an unseen challenge, especially in rural areas and places with rugged terrain like high mountains and desert areas.

3.5. Scenarios of using Virtual ID card

The virtual ID card is expected to offer services in public or private sectors online without to physically visiting service providers. Moreover, it provides the option of proving identity while applying for the same benefits in the service provider. For instance, a person wants to apply for an appointment for a medical check with a doctor. The user has two options: either to apply for this service by using a virtual ID online and when they arrive at the hospital or clinic, they only need to scan their finger to prove their identity. Or else, they could go to a healthcare institution and apply theirs from reception, requiring them to verify identity using virtual ID card as the same online process. However, applying online would give the advantage of not waiting in a long queue, just applying for that service and then scanning fingers to prove their identity before entering the doctor's room.

This solution would offer a fast process to apply and receive the service, besides providing reliable and secure methods to ensure the service identity received by the beneficiary.

Additionally, virtual ID cards would eliminate the procedure of renewing the card after passing its expiry date. Instead, it will propose a new idea of frequent updates of specific data to ensure all information related to a person is up to date without issuing a new card or going through a process. For example, the user will have to update some information that could be changed regularly, such as home address or photo. Every year the user will be requested to either approve a home address saved in personal details or insert a new address, providing evidence of the new home address like a rental contract. Moreover, a personal photo might require to change every number of years, like every two or three years.

Furthermore, updating that information should be digitally verified by using some technologies (e.g. Block chain technology). It would ensure inserted data belongs to the user, not any other random individual, to guarantee high security, authenticity, and reliability of information within virtual ID cards. Implementing

such technology would increase trust and confidence in the information provided by this solution.

Chapter 4
Implementation of virtual ID card

4.1. Requirements

Before implementing the virtual ID, there are some requirements to discuss and present to be considered and fulfilled to achieve the goals and target them.

4.1.1 National identity data

Data is the foundation of all kinds of ID cards; therefore, it is critical to realize the solution and turn it into reality. In most countries worldwide, a national data registry has all the data and information of their citizens, and other people live in it. This data store in a large data centre with proper databases organized, secured with the latest technology to ensure its safety and updated daily from multiple resources in the country. Moreover, there are various data within mentioned databases for each individual, such as date of birth, marital status, healthcare history, education, etc.

Therefore, to ensure that all the information in the virtual ID is correct and up to date, it is crucial to take or link such data from a reliable and trusted resource. However, it might be challenging to acquire all needed information because of a governmental entity's secrecy and sensitive identity data.

4.1.2 Reliable network

The computer network is crucial because it will be the focal point between users and service provider and the communication method to exchange information.

In any dependable system within any business, it's essential to have a stable network to help business processes and operations continue smoothly and consistently. For instance, if the network connection is slow or down, it will be complex and challenging to access or use the virtual ID. Therefore, it will lead to negative feedback and reception on such services and make the users untrust it because of its inconsistency. Even worse, it may open a gap that would lead to data breaches and cyberattacks that could harm the system by stealing or misusing data. A reliable network needs to be fault-tolerant, which means it requires the capability to continue delivering data in case of hardware failure. To achieve that, it needs to have an active continuous backup for the network hardware. Moreover, security is a significant factor for a reliable network. It consists of confidentiality, integrity, and availability. In addition, any network considered secure when security policies cover all loopholes in it.

4.1.3 Security

The protection of the application and its networks against theft or cyber-attacks is significant for any well-designed application. The impact could be by harm and damaged hardware, software, or digital data. Moreover, any breach or attack might disrupt or halt the services provided by virtual ID.

Security is one of the main elements in the application's success because it is regularly connected to several networks and cloud services, increasing vulnerabilities to security threats and breaches. The security measures at the application level aim to prevent data or source code within the application from being stolen, hijacked or tempered.

Numerous application security features can reduce security vulnerabilities and increase safety and protection—first, authentication procedures to ensure that only authorized users gain access. This procedure will define how required to access the application using Multiple authentication factors such as password, pin and bio-metric data (fingertip, facial, etc.).

Secondly, authorization to access and use the application by validating each user's permission and what features they are permitted to use. Finally, data encryption techniques encode and cypher data to protect digital data confidentiality and sensitive data from being seen or even used by cyber attackers while

transferring between users and different networks.

4.1.4 Fingerprint data

Bio-metrics, known as body measurements or unique physical features of an individual, distinguish that individual from other peers. Furthermore, the fingerprint, iris, retina, etc., are the types of bio-metrics used to identify persons. However, the distinctive fingerprint character of being different from one person to another, measurable, and simply finding devices that could read its data made me choose it to be part of the virtual ID identification and authentication.

In some countries like Oman, most citizens above age 18 must register their fingerprint data in the local authority to obtain regular national ID cards. Hence, it is possible to demand these data from the responsible entity or create an electronic integration between the virtual ID application and this unit. Suppose the data is not registered by the government or other types of organizations. In that case, the registration process should be initiated during the beginning stages of this project and store it properly.

4.1.5 Mobile number

Mobiles or cellphones become a daily companion for every individual, and their number usually registered under the name of the person who uses them. Therefore, it would be a key to verify user identity as a security measure during registration, login and some transactions. This verification ensures that only authenticated person could use the application and perform selected actions, such as updating their residence information. The mobile number will enable users to receive notifications and system messages, plus secure links to establish identity verification to multiple features and services within the virtual ID.

4.2. Registration and enrollment process

The registration is the initial step before starting to use any application or program. The main aim is to record the users' information and details, validate the

eligibility of only qualified individuals to register and use the mentioned application and issue particular login credentials like user name and password. The mechanism of registration is illustrated in 4.1

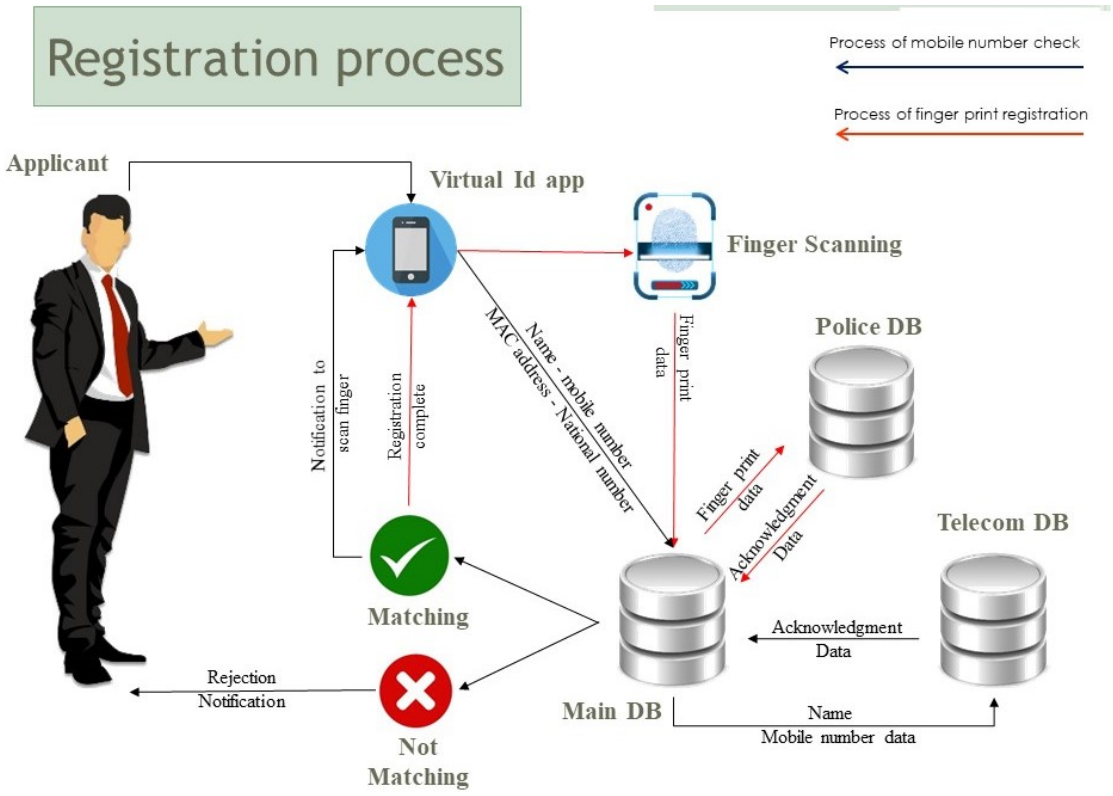


Figure 4.1 Diagram of registration process in virtual ID card

4.2.1 Registration

At the beginning of the registration process, the applicant should install the application on their smart device(mobile, tablet, etc.) from any digital application store such as google play or visit the virtual ID portal available on the world wide web. In addition, there is a "new user" link that would direct the applicant to the registration page. The applicant should enter the registration page and register basic info, such as name, national number, mobile number and email. However, the mobile number entered by the applicant has to register in a telecommunica-

tion company under the same full name. It is a security measure to guarantee the actual user will be receiving future notifications, "OTP" and secure links.

Upon completion of registration, if suppose one or more entries are not validated. In that case, the system will send an email stating refusal of registration, mentioning the reasons, and two more chances are given to do the process. If the applicant deplete given opportunities, they will be blocked from registration and need to contact the responsible authority to enable another try. If the information is correct, it will send the device MAC address to the virtual ID card database. The system will check filled information and compare details with associated identity via Integration with the national telecom database. There will be a comparison with the name and associated phone number, so if the registered name doesn't match the corresponding numbers, the registration will be rejected. Suppose the phone number and name match, an email with a secure link will be sent to the applicant. Moreover, notifications are sent to the applicant to proceed to the next enrollment step.

4.2.2 Enrollment

Once the applicant clicks on the secure link received after completing the registration stage, it will redirect them to the enrollment page, where they must type the desired password. Writing the password must be in English; a minimum of 8 characters include one capital letter, number and unique character. Then, the system will check if this password matches the password validation. Nevertheless, if it didn't pass this validation, the applicant will be given two more tries to enter a new password and block it if it fails to complete it successfully.

After the password is accepted, it will direct the person to the bio-metric enrollment page as shown in figure 4.2. On this page, the applicant is required to scan at least three fingerprints of each hand. The system will choose which precise finger to check randomly. Furthermore, to enter bio-metric details, it's required to have a smart device with fingerprint ability or a finger scanner for devices such as PC. Again, the system will check and validate fingerprint data and compare it with information stored inside the national data bank under the authority of the Royal Oman Police. But, if this stored bio-metric data doesn't match entered data, the system will deny this person enrollment and requested to contact the

local authority. Some people might be didn't register their fingerprint data by the local government in other rare cases. Therefore, they need first to record their data in a local government office, and then they get permission to continue the enrollment process.

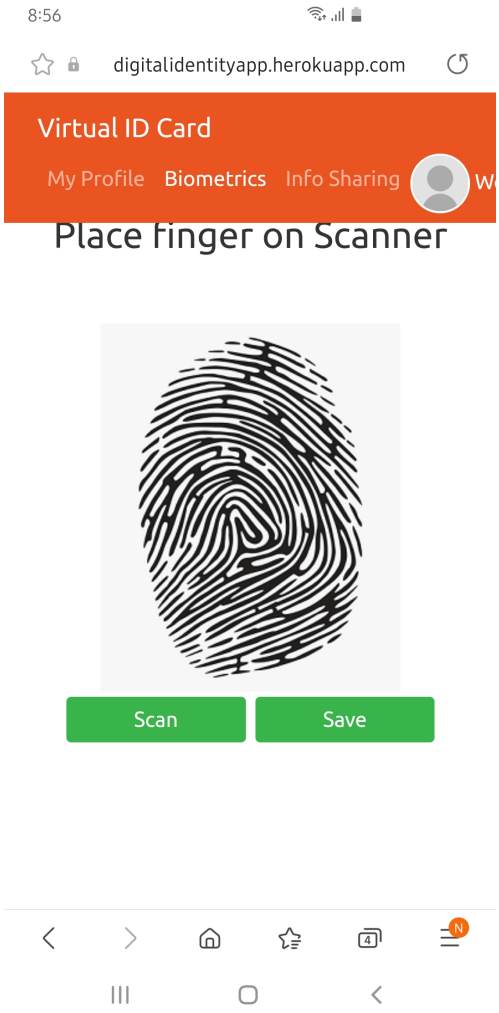


Figure 4.2 Screenshot of Bio-metric enrollment in Virtual ID card prototype

Anyhow, presume bio-metric data matches the data in the national data-bank. In that case, the registration and enrollment process is complete, and the applicant status change to a user. Finally, the user is authorized to log in and use the virtual

ID.

4.3. Login and using virtual ID card

4.3.1 Login process

Login is how an individual gains access to a computer system by identifying and authenticating themselves. The user credentials are usually in the form of a "username" and a matching "password." Aside from giving users access, this process prevents unauthorized users from accessing the application or system. Therefore, it avoids misuse of application by unproved persons. Adding an extra layer of security will use an additional authentication factor, an "OTP" (one time pin) sent directly to the user's mobile as shown in figure 4.3 .

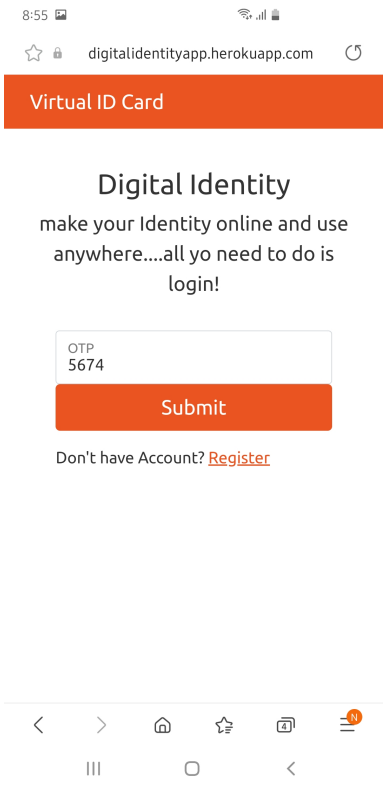


Figure 4.3 Screenshot of OTP for login process

First, the user must type the national number and password in assigned boxes. If one of those two entries are incorrect, a notification will appear to the user stating mismatching with data stored in the application databases. Furthermore, the user will get two more chances to type the correct requested information. If it's not right, they will get block from entering mentioned entries, and they need to contact the local authority to provide them with another chance to access the application.

In the event of matching between information entered and stored data, the user will direct to the next page where it's required to type "OTP". Then, the system will send an SMS to the registered mobile number, and the user will have a short limited time to write the received number in a designated place. If the number entered does not match the received one, the user will get another two tries to resent other "OTP" or use received. If it is not equal, the user will deny accessing the application for a specific time (maybe one hour), and then If this issue occurs twice in the same day, the user will reject login and need to contact authorities. If data entered equal received, the user would grant access to use the application and forward it to the main page of the virtual ID.

4.3.2 Using Virtual ID card

After successfully passing the login procedure, the user enables to navigate through different pages of the application. There are three main pages or tabs within the application. The first page has full details and information associated with the user, such as full name, date of birth, residence information, personal photo, etc. The second page has the services offered by virtual ID, like updating residence details, image, etc. Finally, the third page is for identity proofing and data control. On this page, the user can prove their identity when enquired by an authorized entity or personal such as police force, bank clerk, government employee, etc. Additionally, it provides the privilege to choose what information to share with other parties.

On the information page as shown in figure 4.4 , the user could only read the full details of him/herself without the ability to update, alter or delete data. The screenshot ability is disabled to add extra protection for the information within the page.

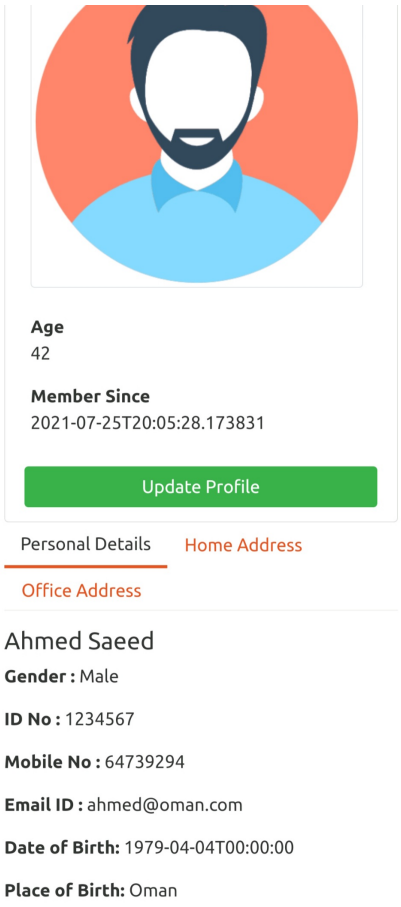


Figure 4.4 Screenshot of Information page in Virtual ID card prototype

In addition, on the modification page, there are few services the user could use. Primary, the user can update or change personal photo once a year. However, few requirements need to fulfil to accept a new image. For example, it should have a white background, only shows the upper part of the body(face and chest), and clothes must be formal. If those requirements meet, the system will forward to the next stage of authenticating the image. But, if one or more aren't matching, then notification would pop up to the user stating the issue. If it's typical, the system will analyze the uploaded image and compare it to the previous one. If it is not matching, it will deny the update, and in case it is identical, it will complete the update process. Lastly, the user can update some data such as residence info and employment details by uploading a soft copy of the official document like the rent or work contract.

4.4. Identity proofing mechanism

The primary purpose of most identity documents is connecting the person they belong to (him/her) to the information about them, whether it is printed on a card or saved in a database. For instance, the photo is one of the things any official person would look into to identify the person who submits it and clarify if it looks identical to the image. However, using rudimentary methods to identify a person could fall into some challenges, such as fraud or forged identity. Therefore, it is more beneficial to use secure ways to validate the identity by requesting to submit a password, secret number or pin to ensure that authentic person is who they claim to be.

The mechanism to prove identity in virtual ID is simple to use, and it's process is illustrated in 4.5 . Still, it has advanced technology behind it, which uses bio-metric data(fingerprint, iris, retina, etc.) as a unique identifier to prove and link this data to a genuine person. The primary reason to use bio-metric data as proof is its uniqueness, as it is a distinctive feature in every human being. Moreover, it's nearly impossible to have identical bio-metric data for any two people, even in the case of twins. Furthermore, it is tough to forge it or temper with it because of those characteristics, giving it an exceptional advantage over the standard security measures.

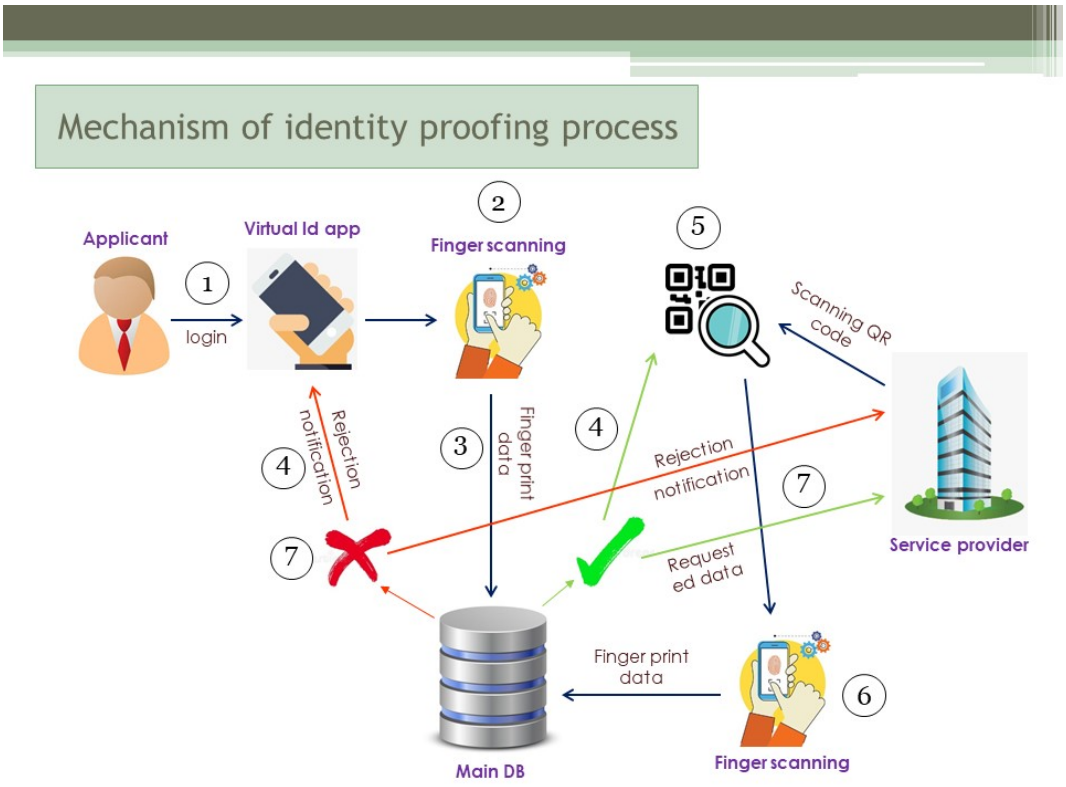


Figure 4.5 Diagram of Identity proofing mechanism

The user should click on the identity proofing page. On that page, the user requested to scan a finger to prove the identity. If it didn't match, this process would be halt and notification send to the user. If it matches saved finger data, a QR code as shown in figure 4.6 in the user device will appear for service provider employees to scan. This process ensures only authorized persons could receive information. Once the employee scan, he will ask to scan a finger to check if he is allowed to receive data.

Figure 4.6 Screenshot of QR code page in Virtual ID card prototype

After the official person scans that code, he/she will require to authenticate their identity by scanning a random fingerprint. The system then will check if that fingerprint data matches with data stored in the system's database. If it didn't fit, they would be denied and have two more chances to validate their

identity. If they fail again to prove themselves, they will be blocked and requested to contact the official unit to reactivate their access. If the authorized person's validation is successful, they will forward to another page to ask the user to scan their fingerprint to validate their identity. If it fails three times, they will be giving an extra chance to prove identity by checking a different finger, just in case the previous finger had some issues while scanning it. If it fails again, the user will be marked as fraudulent and will fall in proving their identity.

The authorized person (policeman, bank clerk, etc.) could contact the concerned party to take action or do their legal process towards the user. Assuming the user successfully scanned fingerprint and is identical to stored data, in that case, the requested data will be sent to the service provider's system, and the process of identity proof is complete.

In the mentioned process, it is in the case of identity proofing in person. But in case it is online, the only difference is there will be no QR code to scan.

4.4.1 Offline mode identity validation

In some rare cases, maybe the virtual ID card user is in an area without network coverage but requires validating his identity to an authorized person, such as a police officer stopping a driver to check driver's license information. In such cases, there is an offline mode that only shows only essential details of the person such as name, age, driver's license, etc.

The offline mode is offered only to identify a person without the need for approval. An offline page doesn't require a network to open and has a QR code. Moreover, the information about the user is embedded inside that QR code. The authorized person, such as a police officer, can scan that QR code and read the data stored inside that code. Furthermore, after scanning the QR code, the data should be transferred to the police device using NFC technology. NFC is known as a contact less communication technology using a radio frequency to exchange data between two devices [22]. Once the data appears in the officer's device, the identification process is complete, and the information officer seeks visible to him.

4.5. Data sharing control process

Information is a vital asset in the current era, and it is the foundation that most of the technology built on its base. With the merge of technology and the excessive use of information in daily life, the importance of controlling this data and information while sharing it with other concerned parties become a must to increase protection and security against misuse or exploitation.

Moreover, ID cards have multiple information and data printed and stored inside it's the microchip in the current situation. While the cardholder must submit it to prove their identity, some unneeded info could be seen or noticed by the person responsible for receiving it. For instance, you may require to submit your ID card to prove your identity to apply for government services, and the required information is your name, national number and photo. However, the employee in that unit can see other information like your birth date and place. Hence, the capability to share only required information is crucial in such a situation.

Virtual ID would enable the user to select only the requested data and information from official parties who provide services and transactions to people, whether government or private sector entities. Data selection is shown in figure 4.7.

Inside the virtual ID, there is a page dedicated to proof identity, which was explained previously. On this page, data and information sharing ability are available. In the predefined buttons, which integrate with certain services provided by other units, there is a standard identification button that has basic required information available to share like, for example, to open a bank account, all input related to the user listed there. Still, the user could select which wants to share with the clerk and not, based on the request from the bank clerk.

The process starts with a request from an official person to prove the user's identity, and then the user would enter the page of identity proof. Furthermore, it will prompt a page with either a QR code to be scanned by an authorized person to authenticate that person and ensure he/she has the right to ask about such information. After the official person scans that code, he/she will require to validate their identity by scanning a random fingerprint. The system then will check if that fingerprint data equals the data stored in the database. If it is correct, he/she will grant to request such information and forward it to another page to ask the user to scan their fingerprint to validate their identity. If it fails

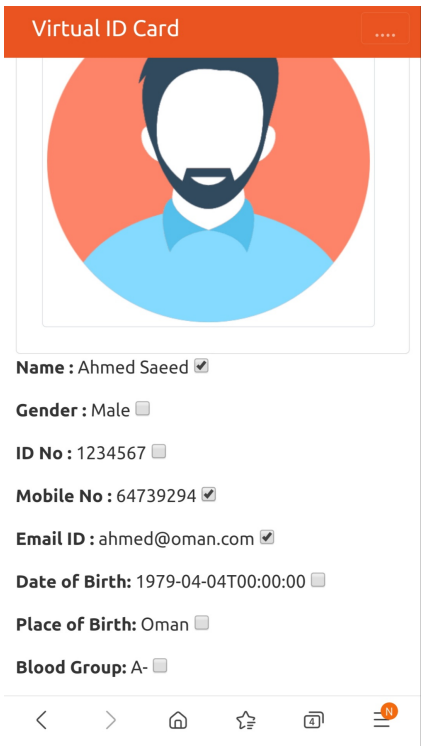


Figure 4.7 Selecting information in Virtual ID card prototype

three times, they will be giving an extra chance to prove identity by checking a different finger, just in case the previous finger had some issues while scanning it. If it fails again, the user will deny access.

Finally, if the user successfully proves their identity, they will direct to the preview page to check the information requested to share with that authorized person. Each input has a tick or select button, and the user could select requested info which is mark to indicate it for the user, then the user could approve it and send it to the authorized person. In conclusion, the process ends by providing only required information without showing unnecessary data for the associated party.

4.6. Expected Features

4.6.1 No expiry date

Generally, all kind of card has an expiry date, especially ID card. Therefore, it is a policy to force individuals to update their information regularly. An expired ID card is no longer usable because it has passed the expiration date determined by the local provider(authorized entity). Consequently, it's necessary to renew the ID card once every five or ten years, depending on local laws in this regard. The renewal process for regular ID cards requires visiting the local government office to apply for renewing and waiting in long queues to receive another copy of the same card used in the previous period. This process could be a challenge to every person as it needs a commitment of time.

Hence, the virtual ID could solve this matter by proposing a new idea of a non-expiry identity card. The virtual ID has a feature of annual self-update of attached information and data to implement this idea. To keep it active through the year, all users must do this process after one year of using the application or portal. The process is simple, an email or notification will send to the user, then specific info could present to him/her to either keep it as it is or change it to a new, like a home address. Once the user updates or keeps the information, then the card is renewed for another year.

4.6.2 Update personal information

In many cases, using a regular physical ID card to update particular info, such as employment details, is obligatory to hand over the card, ask the local authority to edit that info to the latest, and then print a new card with these new data. However, this procedure isn't convenient for both the card bearer and the card provider. Therefore, my solution offers an update feature for specific information related to the user inside the application/portal without visiting or contacting the concerned party.

4.6.3 Available online

Availability is one of the benefits of virtual ID. On the other hand, standard ID cards are physical and oblige to carry on all the time, just in case needed to apply for services such as opening a bank account or proving identity whenever asked by official personals like police officers. Virtual ID offers to access and use its information from any device other than your smartphone. For instance, there is no need to worry about forgetting your wallet, which contains all cards or your mobile application. Using your credentials (national number and password), you could log in to your ID and use it from any computer or electronic device.

4.6.4 Reduced risks

ID-card is a critical document, and losing it means that the cardholder is at risk of falling victim to identity theft or misuse of attached information. In addition, that stolen document may be used to perform transactions, sign deals, etc., by the person who stole it. Therefore, being in a digital form, virtual ID ensures that the only authenticated person can use it for any service requiring identity-check.

4.6.5 Enhanced security

Security is an essential asset in the success of any well-designed application because it guarantees the user information, data, and transactions are protected and safeguarded. Initial, there are a set of security policies applied to multiple processes within the virtual ID like register, enrollment and login. For example,

It is mandatory to update a user's password frequently during the year(every four months) to ensure the password is up to date and if any other party has tried to crack it. Additionally, bio-metrics is another security factor added to make an extra layer of safety while logging in and using the application/portal. Moreover, secure certificates used to protect data traffic and connection of virtual ID. Its primary purpose to encrypt sensitive information sent across the network so only the intended recipient could read and access it.

4.6.6 Data control

The concept of having control over your data and information attached to an ID card is a crucial topic. For instance, sometimes, you need to submit a copy of your ID card or show it to authorize person such as the hospital admin. However, the required info might be one or two, but there are other data you don't want that person to know. Moreover, some personal information such as family name could effect the duration to complete receiving the service. As a result, many have the desire to have the ability to share only requested data with concerned parties. Hence, virtual ID provides the power to the user to add an extra privacy level to achieve better results of data control

4.6.7 Validate identity digitally

Identity validation is a way to ensure that service clients or customers are the ones they claim to be by verifying the associated person's identity. For example, the process may verify physical identity documents such as an ID card or passport. Nevertheless, because of characteristics of standard identity documents, they may fall into the wrong hands and forged to use as someone else identity, to gain a benefit or apply for a kind of service only actual identity owner could get. For that reason, having a digital mechanism to verify the user's identity whenever asked by an authorized party is an essential feature to increase security and ensure high levels of verification whenever demanded to prove identity.

Summary

In summary, before implementing the virtual ID card, some requirements need to be fulfilled to ensure that the solution would work properly. For instance, personal information needs to be acquired from the local authority (Royal Oman Police), which currently stores and owns the data. Furthermore, integration between different stakeholders or parts in virtual ID cards needs to establish to ensure the exchange of required data to identify or validate some data such as bio-metric data and registered mobile numbers.

In addition, before the start of using virtual ID cards, few procedures need to be done, such as registering the user, then checking the authenticity of information and bio-metric data if it matches stored data in the local authority's database. Moreover, the user has to create authentication elements such as a password before signing in to the application. Furthermore, an overview of how to use the virtual ID card for identity proofing in person, online or offline has been explained to provide detailed information to expected users of this solution.

Finally, brief information about the expected features of using the virtual ID card instead of a regular card was presented at the end of this chapter. Moreover, The solution will introduce some features, such as high security, by demonstrating high encryption techniques, ensuring increased safety and reliability, with low chances of data leakage or interruption.

Chapter 5
Discussion

5.1. Research methodology

In this research, the qualitative method investigates the current ID card and its common problems. It started by interviewing people from different backgrounds and ages to ask them about their prospects of present ID cards and how frequently they use them. Moreover, what are the everyday struggles and things they think need to be improved or enhanced? Structured questions were conducted during the interview to have a single direction of the discussion, giving the interviewee the chance to add additional comments and feedback about each question. Finally, those interviews have been conducted to validate the concept of virtual ID and understand the person's perspective about current ID cards.

To have an excellent understanding of ID cards and their existing situation, we asked multiple persons about their general idea about ID cards. Furthermore, they provide some issues they face while having or using their cards. Moreover, we observed some problems which reduce or limit the benefits of those ID cards. Therefore, having that information serve as a starting base for the question in the interview about existing cards.

Regarding the new concept of virtual ID card, the questions about it focused on the new features and capabilities that it would present, such as bio-metric technology and how it would solve some current ID cards issues. Moreover, it would test the acceptance and readiness of general users to use this new concept as a replacement or secondary option to the cards we use now.

In addition, an online meeting were conducted with officials from different organizations to give them idea about virtual ID card and receive their reactions and feedback, besides test their willingness to participate and collaborate in such national project.

Furthermore, a users test for virtual ID card prototype has been conducted for limited participants. A few questions about the function and users acceptance have been asked to have an insight into potential users' reception of the solution, the ability to use it without matters, and its friendliness as software.

5.2. Interviews

A group of twenty participants take part in the interview phase. The participants are from different sectors within the country with various backgrounds, experiences and levels of education. Moreover, they work at a diverse organizational level, from top management managers down to operational-level employees. This deviation would give a diverse perspective and view of both current and new type of cards. Unfortunately, because of the current pandemic situation, which emphasizes social distancing and reducing involvement with other people, we couldn't take additional persons for the interview, adding extra knowledge, opinions and understanding about the subject we want to investigate.

Before the beginning of questions, few questions about general information of the participants were asked, such as age group, higher qualification and profession. Most of the participants are full-time employees working in both the private and public sectors. Additionally, a significant percentage of them have a bachelor's degree, with few with high Diploma, Master's and doctoral degrees.

The questions of the interview are divide into two sections. The first section is about existing ID cards, and the second section is about the concept of virtual ID card. The questions start with how frequently you use your ID card to indicate the importance of those cards and their regular uses—most of the answers, around 70% of participants, often use their ID cards. Furthermore, 15% of participants use their cards either monthly or once a year. They use ID cards to apply for multiple government services like healthcare, education, and more. Moreover, it enables to request services from private sector units such as telecommunications companies, banking services, money transactions, travelling to neighbouring countries, etc.

Additionally, some commercial shops request a copy of their ID card to save it in their records for warranty purposes. Nevertheless, police officers require an ID card as proof of identity in many cases and oblige all people living in the country

to carry an original copy of it all the time. Therefore, failing to submit the original copy of the ID card might lead to some legal accountability. The following are the remaining questions that used to validate users opinion regarding current and virtual ID cards, respectively:

• Have you ever forget your ID card?

45% of participants forget their ID card at least once, and most of them didn't matter, but others failed to request a service because they didn't have it at the time of their request. In few cases, some answers that driver's license or passport were an alternative to apply for services if they forget their ID card. On the other hand, participants(40%) never forget their ID card and always take it with them wherever they go because they don't want to be in trouble if a police officer asks them to submit it.

• How many cards issued by the government do you carry always?

This question asked to have a general idea of the average number of cards issued by the government institutions. The majority of participants (60%) carry more than two cards with them all the time. In addition to ID and drivers license cards, they have labour and healthcare cards with them. However, all participants said that only an ID card and drivers license are essential to have in position. The others only matter if you require to apply for a specific service, such as visiting a doctor in public hospitals.

• How do you evaluate the process to renew/issue an ID card?

The process is simple and regular; an equal number of 40% of both answers were from participants. They find the process familiar and straightforward. However, they said it is a very time-consuming process. The person has to visit the local authority office(civil status) to apply for card renewal and then wait in a queue to take a new head-shot. Additionally, if any update for related information, such as a residential address, they must submit it to the employee and then sign on the process document. Finally, waiting for the card to be printed and handed over. Few participants suggested shifting the renewal process to become online and prefer to receive their cards at their home address instead.

• What's the most significant disadvantage of an ID card?

It is clear from the answers that most participants (15 people) think the expiry of an ID card is a crucial disadvantage. They suggest that cards issued for once

in life or renew the card only you need to update your information at a particular time. Moreover, they also believe that being physical makes it very fragile and easy to lose. Besides, it has a microchip that stores data. Moreover, although the microchip is advantageous by storing all related data in one place, it's risky to fall into the wrong hands. Therefore, this microchip is unsafe because it lays all data and information with the person who steals it.

• Do you think current ID cards support digital transformation?

Neutral without negative or positive effect towards digital transformation, that's what 50% of contributors think about current ID cards. Moreover, they mentioned that there must be more integration's with multiple government entities to support digital transformation, especially in government electronic services. Additionally, they emphasize transforming remaining paperwork procedures into computerized systems. Nevertheless, 35% agrees that current ID cards enable digital transformation by using a microchip in the card to read information digitally, which makes a slow effect and shifts to a fully digital system. Finally, 15% thinks having the microchip doesn't mean an actual transformation happens. For example, you still need to hand sign printed papers and then scan them to enter them into the system, duplicating the process rather than simplifying it.

• Using a bio-metric to verify your identity would increase security?

75% thinks using bio-metric data such as fingerprint, iris, face-print, etc., would increase the security in verifying identity. Hence, they said the uniqueness of those data make them give higher results in identifying one person from another. However, they have some concerns regarding the security and confidentiality of those bio-metric data, besides health concerns if, for example, constantly scanning iris would affect eyesight in the future. The remaining percentage strongly agree with using such technology to improve security and efficiency of identity proving. Additionally, many contributors worry about the availability of such technology in all devices of targeted people. Such devices like the latest iPhone are expensive to purchase by the majority of them.

• The possibility to access your ID information from multiple platforms is an advantage?

The ability to access your information from your phone or laptop is a significant advantage; 70% of participants responded with this answer. They mentioned

that current ID cards have some data stored inside them, but they don't have access or authority to check it. Hence, having this ability a priority for them. Moreover, 20% answered with neutral thinking access to information should be an option for the card owner, instead of making it the only way to overlook your information. There is a shared concern among all participants, which is the security of information. According to them, by making them online, such information is more exposed to cyber-attacks or digital hacking. Moreover, they think making data accessible online makes them risky to be altered or tampered with by even the card owner themselves.

- Giving the card owner the ability to control data is essential?

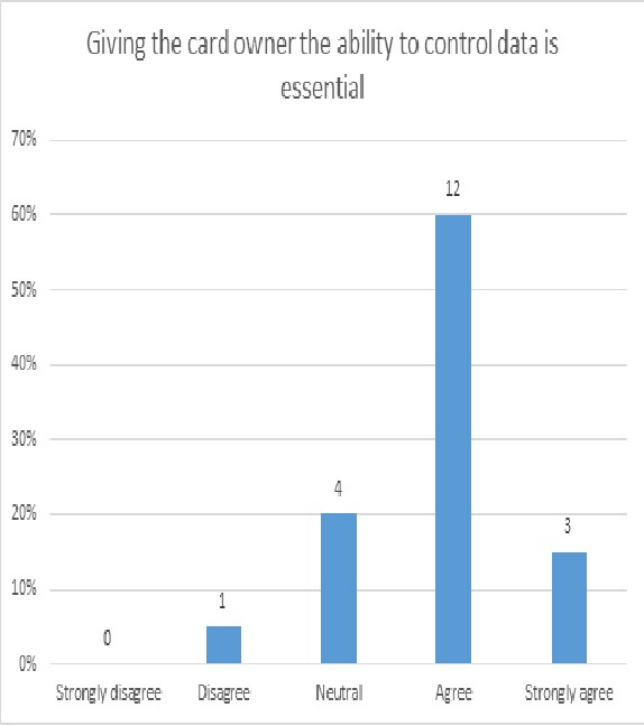


Figure 5.1 Participants response to control shared data

It's clear from the answers to this question that the majority wants to have the privilege to select shared data and information with other parties. Moreover, they said that the requester might access or figure unnecessary details by submitting standard cards in many cases. For instance, you apply for phone line service,

and the employee of the company might see some info like your marital status or birthplace, which are not required but could be overseeing by authorized personals. Therefore, it is crucial to have the control to give the requested party only what they need. However, 20% considers it not a vital ability, and 5% disagree with giving the power of sharing data to the user as shown in Figure 5.1. Their response is by law; it might not be possible to control your data. Further, although your card's data is yours, it doesn't belong to you, as ownership belongs to the public authority that saves all information. Therefore, you can't use it as you wish.

- Could virtual ID ease the process of updating variable information?

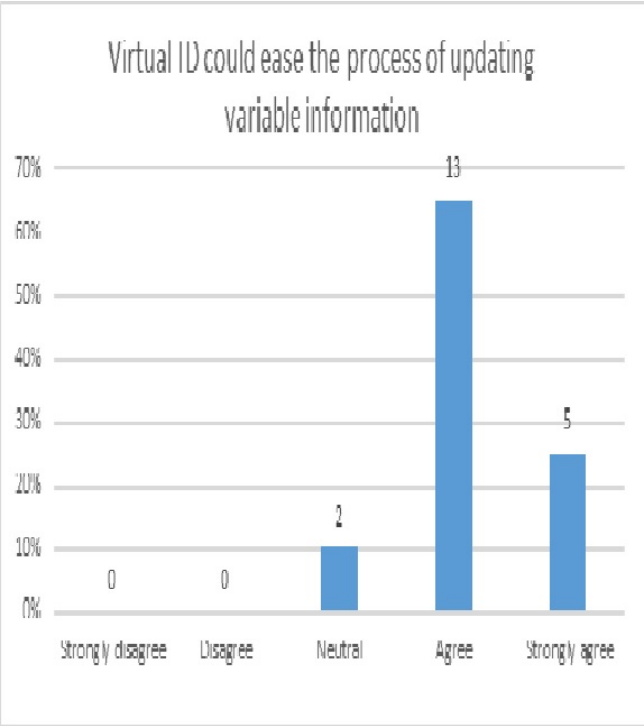


Figure 5.2 Participants response to online information update

This question proposes an alternate replacement to the expiry date of cards. Moreover, it may substitute the process of the renewing card with updating variable information like a home address and workplace periodically. The result as shown in Figure 5.2 was that 65% of participants agree and support this new ability to be an alternative to a renewing card. Many think the primary purpose

of the renewal of a card is updating information besides extending its validity. Furthermore, 25% strongly agree with this proposal adding that only certain information should be updated, not all personal data. Plus having a systematic procedure to verify updated data and ensure it is correct and authentic.

In addition, participants emphasize raising awareness of the community's people about the importance of correct information input if the system won't have the ability to check and verify it. Moreover, they think periods to update the info should be adequate—for example, the requirement to update on an annual basis only. Also, they suggest that the virtual ID card must have a notification or reminder process to inform the user about the update period.

• Probably virtual ID can act as an enabler to digital transformation? Around 90% of participants responded that having a virtual ID card integrated with many e-services could positively enable digital services transformation. They said such ID card could make the process of services in both public and private sectors faster and more efficient. Moreover, it might reduce operational costs for the organization responsible for ID cards by decreasing or eliminating paperwork in most processes. Furthermore, it will always make data up to date and ensure accurate information is available quickly.

• The accuracy of Identity proofing could increase by using the virtual ID instead of a traditional ID card?

15% of participants are uncertain if the accuracy to prove identity would increase if virtual ID cards are used instead of standard ID cards, as they responded by the neutral answer. Conversely, 75% agree that virtual ID would raise proofing levels, plus 10% strongly agree with that statement. Moreover, they mentioned using proposed bio-metric technology known for its uniqueness and eases the encryption securely. Additionally, it guarantees high levels of security and great accuracy to ensure each person is who he/she claims to be.

• Do you think virtual ID card should replace or implement with existing cards or never exist?

This last question was very vital to conclude the interview. It indicates if the audience could realize the potentials of virtual ID card or see the current ID card is suitable for this period, and it should never replace legacy cards. The result was 50% for replacing the current card with 50% thinking it should implement

with the existing ID card as shown in Figure 5.3

The participants who choose to answer by replacing present cards realize that this kind of digital ID cards is the future of identity documents. Moreover, they think it would move us forward to a fully digitized community, where all services could exist in cyberspace. Besides, it would solve many issues and challenges that face standard ID cards, like the ability to forge a fake identity and others. Furthermore, it could reduce costs to issue cards, operate issuing centres and offices, and make life easier by providing services faster.

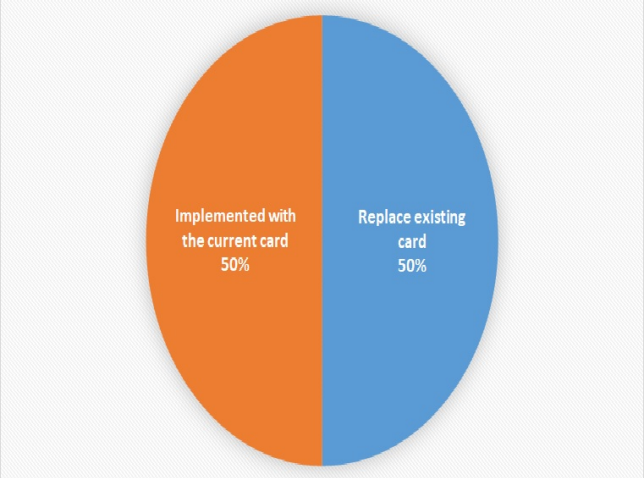


Figure 5.3 Participants response to implementing virtual ID card

However, the people who replied with implementing virtual ID cards alongside current cards are anxious to see immediate replacement without using and evaluating the new ID card. Furthermore, they want it to be well tested for few years while working on two versions of ID cards, the physical and virtual. Plus, they respond it could be an option for people to be an extra feature of ID card. Some have few concerns about not having a physical card in complicated cases such as natural disasters and medical emergencies. Moreover, they want it to have integration with almost all kinds of services available within the country. Hence, to reach expectations and have complete trust from all parts related to it, it should work, then evaluated and fixed any issue, and after a while, it could end the use of standard cards.

5.2.1 Online conversation with Omani officials

An online meeting using zoom (video call App) has been conducted with officials from different government and private organizations, which are potential beneficiaries of the virtual ID card in future. Those meeting attendees were from a private bank, the central bank of Oman, a lecturer at a private university and the Telecommunications Regulatory Authority.

A PowerPoint presentation was presented during the interview to introduce the virtual ID card and its operation briefly. Moreover, the presentation emphasizes how the virtual ID card could support transforming the current procedure to prove identity into a new digitized process. which offers improved security in exchanging data and accessing this type of digital card. Moreover, a brief explanation was given to attendees about the method to use the proposed solution and the features expected, which could solve technical and social issues that affect the accuracy and efficiency of existing cards.

In addition, a short video about how to use the virtual ID card and how the digital mechanism would work has been presented to the attendees to give them a visual perspective of the proposed solution. At the end of the presentation, there was a short session for questions and answers to participants to clarify some points during the presentation.

The first question was:
How Virtual ID cards could contribute to Oman?
The answer was, It would solve some technical and social issues related to current cards. Those issues are challenging and time-consuming, and solving them would positively affect the quality and efficiency of those services. Moreover, it would lower the costs to operate current services by shifting them to digital online-based solutions.

The second question was:
How it would support digital transformation within the country?
The answer was, it would assist in integrating systems of different units from all sectors with the virtual id card, hence to apply for those services, a person could prove identity and apply from any place using any digital devices. The expected result will be reducing cost, time, and effort to apply and receive services besides availability. This step would encourage many organizations that didn't

shift into electronic systems to develop their systems, which could easily integrate with Virtual ID card. Moreover, such a solution matches the government's vision for upcoming years to offer complete function services in digital and electronic platforms.

The last question was:
Could virtual ID card become a reality and be considered a national project?
The answer was, if this idea were present to the public authority responsible for national ID cards (Royal Oman Police) and other partners, it would establish and design to match the country's requirements and issues. Moreover, all stakeholders should provide an immense effort and worthy investment to turn such a project into reality. This project would succeed and become the first in the middle east region, which could provide consulting or the exact solution to neighbouring countries resulting in good financial income for Oman.

Overall, The officials welcomed this idea, especially after discussing the existing limitations of regular ID cards. Furthermore, they provided some insights into the benefits of such digital identities for organizations and individuals. Moreover, a suggestion about collaborating with other officials such as "Royal Oman Police" and additional expected partners in such a venture might boost and positively influence the odds of accomplishment for this project.

Furthermore, one of the attendees spoke about producing mobile phones in Oman during the upcoming years. He implied that such an application could be pre-installed in those mobile phones, which may help promote both the virtual ID card and locally made phones. In the end, all participants suggested that the country needs to move towards such a digital solution for identification, which may support the government's efforts in the digital transformation of public services.

5.3. Prototype evaluation

In this research, a prototype has been developed to provide a visual perspective for potential users of how virtual ID card screens and pages would look. Moreover, it would offer a simulation of the identity proofing process using the virtual ID card, which would help the users have an actual application and help to get their feedback. Based on those feed backs, the proposed application could be modified.

The prototype was programmed using Postgres SQL as a Back-end, while Web API was developed using Dot-net Core 5 web API. Also, the front end of the web page was created using Angular 11. Because of the limitation of programming skills and the short period to develop a complete system or solution, the author decided to create only main pages. The test users would need to have an overall experience of a virtual ID card. Moreover, the author developed a login page, registration page, main page, personal information page, identity proofing and identity sharing pages. Those pages should give test users the experience of the virtual ID card from the first step of registration until using it for proofing. Because of the current pandemic situation, only a few test users tested the virtual ID card prototype.

Only a few questions were given in to participants regarding the prototype of the virtual ID card. The first question is how the registration process was? Three participants answered that the process was simple and easy and didn't take a long time. However, two participants responded that the registration process was typical, and it could be done by any person regardless of their IT literacy level.

The second question was about login in and using the virtual ID card. Two participants answered that the process was normal and think "OTP" is an excellent technique to use as an added security measure. Moreover, two participants responded that logging into the virtual ID card is easy and fast. Yet, one participant answered of neutral that the process was not easy nor difficult.

The third question was about the identity proofing and information share procedures if they are practical and convenient for users. Four participants answer that the process is easy and short. Still, at the same time, it could be more reliable because it has digital mechanisms instead of traditional methods to prove identity. Yet, one person answered that verifying identity seems a bit complicated and should be more simplified. The fourth and last question was about the overall experience of the virtual ID card prototype and the friendliness of its pages, design and process for regular use to prove identity. Four participants said the pages are easy to navigate and look fine. They are user-friendly and don't need any further explanation to be operated by regular users. However, one participant answered that the design of pages should be more simple. For example, personal information pages should be divided into multiple pages based on relevant information

within them.

Participants suggested that using digital platforms and mechanisms to identify a person using bio-metric data would improve the levels of accuracy of identification instead of current procedures. Moreover, it would eliminate some weaknesses, such as human factors, to compare information on the ID card and physical appearance, which we discussed in earlier chapters in this research.

Overall, most of the participants give positive feedback on the prototype of virtual ID card, and they imply that using it looks easy and the process to register and use it are simple. Yet, it gives an impression that security could be high by using various methods and techniques to authenticate a person identity while logging in and proofing identity. Their only concern is will these security measures could eliminate the possibility of identity theft or data breach.

In summary, all users think the prototype gave them a good visual perspective about how the virtual ID card would look, how it will operate, and how it helps to identify a person. Moreover, they suggest using it for proofing identity would help solve social and cultural issues related to current ID cards and increase the accuracy of identification and ease the transmission of information and data between service providers and applicants positively. However, they have one concern: the security of their data and the guarantee that only required data is shared with the requested party without the ability to access other unrelated information.

5.4. Discussion

The virtual ID proposal has two main features which might contribute to achieving the main objectives of the research. Those features are digital mechanism for identity proofing and the control of shared data and information. To evaluate those features and see the point of view of potential users, an interview conducted with several people, which has been discussed in the previous section of this chapter(interview).

In the beginning, the interviewees asked about the standard ID cards to demonstrate their benefits, issues and possible developments. We asked the participants about the frequent use of their current ID cards to understand how important the card is in their daily lives and indicate its specific usages. The majority of them

use rarely use it. Moreover, they use it to apply for public services like healthcare and other private sector services such as telecommunication companies and banking. Although they rarely use their ID card, they said it's a must to carry that card all the time because it's mandatory to have it with all persons if they are out of their household. Additionally, they might need to prove their identity in case an officer asked for it.

Although most of the participants consider it's mandatory to have their card with them at all times, many of them forget it once or more during the previous period. However, thankfully, they didn't need it, but it would be an issue for them if they were required to submit it to authorized personnel. We believe the reason to forget ID card, in particular, is because every person in average have more than two cards issued from a public organization, and they carry it on their wallets with other types of cards such as bank cards. Therefore, combining all in a single card would be the better choice for people.

Moreover, when participants asked about how they assess the card renewal process, they respond that it's ordinary but somehow useless because it's just replacing old cards with new ones. Additionally, its primary purpose is to update personal information, receive fees for issuing new cards, and reactivate the ability to request government services, as expired cards are deactivated and denied from receiving any benefit. Furthermore, it is consuming time and money to go through that process. Nearly all of them suggested shifting it to an online process where you can apply and receive the card at your home, without the need to visit any local office. Furthermore, many want cards to have lifetime validation, giving the option to change the card if it was damaged.

Participants said the current ID card has improved over past years and become more sophisticated and can store data, which they see as an improvement and disadvantage at the same time. It is an improvement as it helps transform standard process and procedure within multiple organizations that provide public services to a digitized system. Moreover, those organizations could serve customers fast by reading all data stored inside the card and using what is required to receive that service. However, the possible disadvantage is security concerns about not having proper safety to protect that data from being abused by others in some cases.

Lastly, the participants deliberate about the virtual ID card and how they evaluate its potential features. Moreover, they discussed if that new feature could solve some challenges facing current cards or not. They show excitement about introducing technologies like bio-metric to validate a person's identity. Furthermore, they approve that using such a technology would increase the security and accuracy of that process compared to the current. However, few have shared their health concerns while using such technology as an iris scan or face scan, which they fear would affect the human body part if used constantly. Therefore, they suggest using it only for fewer processes and emphasizing finding an alternative solution.

In addition, participants had a positive response regarding accessing and viewing all of their related information. Moreover, they support the feature to control sharing data and information with authorized parties. They think at present there might be some carious people who work in certain places and can view some information, especially when they connect with ID cards with a microchip. Therefore, it's advantageous to control this type of information and hope some laws make managing data legal and give the ownership of info by a related person. Furthermore, they see a periodic online update of data and info such as residence address is an excellent substitute to replace expiry and renewal of ID cards, stressing good gaps between each update and systematic intervention to ensure high levels of accuracy.

Although participants are aware of the mentioned advantages, they worry about the security of information if they are available online and could access multiple devices or platforms. Moreover, they emphasize having very high-security measures to prevent any data leakage or loss while accessed or exchanged through cyberspace. Finally, almost all participants responded that they support virtual ID card to become the successor of current cards. However, 50% want to implement the virtual ID card with the current one, besides evaluating and improving it for a certain period until all associated parties are integrated and ready to make their main document for all services.

5.5. Findings

The first finding from the interview is people are tired of carrying out multiple cards for several services. For example, there are cards for healthcare, work and personal ID. However, one person owns all those cards. Therefore, combining all cards for one person in a single card with complete information for different uses in one place seems a suitable solution.

In addition, many complain about the need to renew cards from the official public office, which require visiting that office and wait in long queues to receive a new card. Also, considering the costs paid by the card owner to get the card and to travel to the issue place, and the cost to operate that office and to maintain machines responsible for printing cards. Hence, this process could be online, making it easier and more convenient in the long term for everyone.

Furthermore, a significant percentage of people supports replacing physical ID cards with virtual ID cards, which propose higher levels of protection and security to information. Moreover, it gives extra options for users like viewing their data, updating info online, and choosing what data to share.

Additionally, the online meeting gave a good perspective about the virtual ID card to public and private entities officials. Moreover, it presents how the idea would work in reality and the expected features that would benefit all related counterparts and solve many related issues in current ID cards. Furthermore, it provides an opportunity to get feedback and response from officials in Oman, which offers an insider view about what kind of requirements, collaborations, and integrations would need to connect all partners, resulting in achieving all targets and the success of such a project.

Moreover, regarding the virtual id card prototype, participants in testing the prototype gave positive feedback about the ease to use and function it as an application or web page. Moreover, it could replace the traditional method to prove identity, which may increase the accuracy and efficiency of the proofing process. Consequently, it will lead to a better quality of services and a fast approach to complete any application, whether in government or private organizations, resulting in higher levels of digital transformation in all sectors within the country.

This research suggest that standard ID cards have multiple issues related to it's characteristic such as physicality or lack of security, which could solve by moving

forward to the trendy concept of virtual ID card. Moreover, it would make it accessible from multiple places and add extra value for the users by presenting its new features. Furthermore, it could enable digital transformation in all related fields, which will benefit every party related to it.

Chapter 6
Conclusion

6.1. Conclusion

This research proposed an innovative concept of virtual ID card for Oman to increase and enhance security for identity proofing. Moreover, it presented a digital mechanism to prove identity instead of the existing non-digital process. Furthermore, it introduces the ability to control shared information with other authorized parties to protect data and provide only the required, besides solving social issues related to some information of regular ID card. Also, it aims to replace the validity of ID cards(expiry date) by proposing continuous updates of essential information during a specific period.

Based on the results and the impression of interviews participants, it is noticeable that the proposed solutions were received positively and meet many requirements. Additionally, it solves some standard card technical issues such as the renewing process and low security, especially with the existence of the microchip, besides Cultural concerns like hiding family names by using selection on shared data to provide equal services for all people in the country. Moreover, it could increase the protection and security of information by using the latest bio-metric technology to use and interact with the proposed solution. The reactions and answers approve the expectation of improving the precision of identity proofing if users use virtual ID instead of regular cards. It will replace traditional mechanisms to check a person's identity, like comparing the personal photo of the card owner manually. Furthermore, the control of shared info is highlighted as an essential aspect to card owners, giving them the right to select only relevant information.

Therefore, implementing and realizing the concept using the necessary resources and technology would make it succeed in providing a better experience as identity proof. Moreover, it would increase the accuracy and security of identity proof,

which will support the digital transformation of public and private services, enhancing people's lives by making services easy to access through online platforms.

However, this research finds that the new and current cards should operate in parallel for a particular period until all related parts are ready to use the virtual ID card without any issues or challenges for the first phase of implementing the virtual ID card. It would be time to abolish standard cards and replace them with virtual ID card after proving it's a successful solution.

6.2. Limitations

Although based on feedback from participants in the interview, plus the few who could test the proof of concept, we could reach a reasonable assumption. However, there were some limitations in realizing the idea and the technology that it would have. One of those limitations was the lack of programming skills to develop a proper application or system that could imitate what is expected to be from the solution. Moreover, the current pandemic situation made it hard to meet additional people and interview them to have a broader sight of the concept. Furthermore, it wasn't easy to communicate with the local authority responsible for national cards, as they don't prefer to share contact information due to security reasons. Moreover, it denies us from having their insights about ID cards and their impression of new digital concepts of those cards.

To enable the users to access and use virtual ID, they need to connect to the internet network. Most network connections are at places with internet lines or WiFi, plus the mobile phones internet access through satellite coverage. Moreover, to connect your device to the internet, such as mobile, tablet or laptop, you should be in a place where network coverage is available.

Network coverage is known as a covered geographical area by a network of a particular service provider. Inside that area, devices like mobile will be able to call or connect to the internet. Some factors could affect the distribution of network signals, such as mountains, buildings, and more.

Most places within big cities have decent signal coverage. However, In some countries, like Oman, many areas have high terrain like mountains or empty spaces such as desert, making them hard to install coverage towers to enable coverage

to expected customers. Therefore, people who live in areas near those locations might receive very weak signal coverage, or in some cases, they don't have any. Somehow, the virtual ID card relies on connectivity to the internet to use the solution to prove identity or other use of it. This limitation would make it difficult for targeted users to use this solution, making it a possible challenge.

As its mentioned in the previous point, network communication is a vital aspect that enables users to access virtual ID card. However, in some extreme conditions such as natural disasters like earthquakes, volcano eruptions, floods and more, communication infrastructure might be affected due to those elements. Moreover, communication infrastructure relies on electricity supplies, which could be damaged, interrupted, or destroyed, making the possibility of operating network devices hard or impossible.

Such conditions would limit the use of virtual ID cards to identify people and harden access to information until the communication infrastructure is recovering by using alternative resources to run again without any issue.

Virtual ID card depends on having particularly sophisticated technology such as bio-metric data for identifying people. Moreover, electronic devices like mobile and tablets capable of reading and scanning such data are limited and costly. Furthermore, a decent number of people's devices doesn't have bio-metric scanning capability. Therefore, maybe some targeted users won't be able to use this solution as their primary identification document, meaning it will limit the number of users.

Furthermore, acquiring a high technology to verify people's identity, with the highest security levels to ensure information storage and exchange safety, would require a massive investment from the public authority responsible for ID cards. Therefore, replacing current systems and procedures would need tremendous efforts and well plan to shift from the present to the new system.

Although information technology becomes a crucial part of people's daily lives, many have low IT literacy. Information technology literacy is the ability and knowledge of using Information technology or computer devices, which means having a basic understanding of how to operate and benefit from using such technologies.

In the case of Oman, although many citizens are well educated and have a basic understanding of information technology. However, a decent group of people

lack the simple knowledge of using high-tech, for instance, bio-metric devices. Although, the new concept would enable using technology to provide high security and digital processes instead of the standard cards. However, the low IT literacy would affect the success of virtual ID cards, as many might resist the idea of replacing a document they get used to using for a long time or have some difficulties to use and profit from it entirely.

This research proposes a new idea of giving the user or ID card owner the ability to control sharing data and verified parties. However, in most countries worldwide, the ownership of citizens' personal information is with the public authority responsible for storing national data or accountable for issuing ID cards. Moreover, the laws don't support or allow the card owner to select what information would share with all related parties. Therefore, providing such an ability would have a legal challenge and require the local government to either amend or declare new laws that suit the new concepts of digital IDs like virtual ID cards.

As explained in this research, the virtual ID card highly depends on using electronic devices such as mobile phones, tablets and PC to access and benefit from all the abilities that it would provide. However, if this device is damaged or out of charge, it would be difficult for the user to use it, especially to verify identity. For example, if a police officer requests the driver's license, which is part of the virtual ID card, and the mobile phone is shutting down because it's out of charge, it would be impossible to use the card, as supposedly there is no physical copy of it.

6.3. Future works

The vision for a virtual ID card is to replace standard ID cards and provide access to the information of the owners of the cards from multiple platforms, plus providing them with extra features like control sharing data. This type of digitized card would enable digital transformation in services provided by both public and private sectors. Still, to achieve higher conversion levels, the virtual ID card would initiate multiple integrations with significant partners at the beginning, such as healthcare institutes. Moreover, having such integration would enable further and better services and move forward to fully digitized procedures.

For example, enabling integration with healthcare could provide a new concept of e-medicine. People would take appointments, follow up with their health conditions and check their medical history from the virtual ID card. This ability would make virtual ID cards not just a tool to validate identities, but it would make it an integration hub that hosts any services requiring the use of ID cards to apply and use services.

Furthermore, the solution presented in this research could be officially realized to local authorities responsible for ID cards. Moreover, working with such an organization could make virtual ID cards revealed in reality and help the government achieve their vision to be fully digital by providing a digital platform to prove identity and apply for all types of services. This step may benefit the country to deliver many people by enhancing the quality of services and reducing costs and time to provide it, leading to improved levels of life quality for its people.

In addition to the above, in future, maybe the personal information linked with bio-metric data, so there won't be a requirement to have any ID cards carried by people. Instead, all data possibly will store in a secured national database. Whenever a person is required to prove their identity, they scan their fingerprint or eyes, and only the required information would be available to the requester. For instance, if a person wants to apply for a mobile service, the employee in the mobile company would scan that person's bio-metric part, and only necessary information would appear to the employee.

Therefore, the future may exclude the need to have a card in people's position; instead, to keep up with the future's speedy life, we need to scan, approve our identity, and receive the service in a faster manner.

Based on all discussed facts and proven outcomes, to catch up with the speed of global technology development, more researches and innovations are needed. Hence, it will enrich people's quality of life and ensure providing services in a practical, fast, accessible approach through various digital online platforms. Resulting in accelerate the wheel of development in the country, even in a minor way, to make all related parties feel satisfied and conventional.

References

[1] R. W. Caves. *Encyclopedia of the City*. Routledge, 2004.

[2] Ben Quarmby. The case for national identification cards, 2003.

[3] ISO/IEC 7810:2019. Identification cards, physical characteristics, 2019. URL: `https://www.iso.org/standard/70483.html`.

[4] Connor T. Jerzak. A brief history of national id cards. 2015.

[5] ISO/IEC 7816-2:2007. Assignment of contacts c4 and c8, 2007. URL: `http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=45989`.

[6] Hendry. Mike. *Multi-application Smart Cards*. Cambridge University Press, 2007.

[7] David Schultz. National identification cards. 2009.

[8] Yazeed ALKHURAYYIF. Security concerns with national id cards. In *International Journal of Computing Science and Information Technology*, Shaqra University, Al Quwayiyah, Saudi Arabia., 2013.

[9] E Guizzo. Britain's identity crisis (bio-metric id cards). *IEEE*, 43(1):42– 43, 2009.

[10] republic of china State council. URL: `http://news.sina.com.cn/c/2003-06-20/18411198235.shtml`.

[11] Sina English news website. URL: `http://www.gov.cn/banshi/2005-08/02/content_19457.html`.

[12] Yang Wenming Li Yanan Zhang Yang. Listen to transformation of china: Lost your id card, how safe is it?, 2015. URL: http://www.gov.cn/banshi/2005-08/02/content_19457.html.

[13] Economist Magazine. Estonia takes the plung, 2014. URL: https://www.economist.com/international/2014/06/28/estonia-takes-the-plunge.

[14] E-estonia. Estonia introduce a new id card, 2019. URL: https://e-estonia.com/estonia-introduced-a-new-id-card/.

[15] Tambur Silver. Possible security risk affects 750,000 estonian id-cards, 2017. Estonian World. Retrieved 2017-09-17. URL: https://estonianworld.com/technology/possible-security-risk-affects-750000-estonian-id-cards/.

[16] Nele-Mai Olup. The government decided to cut off more than half of id-cards from the e-state in estonian, 2017. Postimees. Retrieved 2017-11-03. URL: https://tehnika.postimees.ee/4297813/blogi-ja-fotod-valitsus-otsustas-e-riigist-valja-loigata-enam-kui-pooled-id-kaardid.

[17] Kristjan Jõevere. The certificates of vulnerable id-cards will be stopped from tomorrow evening, 2017. Delfi.ee (in Estonian). Ekspress Grupp. Retrieved 3 November 2017. URL: https://www.delfi.ee/artikkel/80046784/blogi-ja-fotod-turvariskiga-id-kaartide-sertifikaadid-peatatakse-alates-homme-ohtust?

[18] State of Colorado. About colorado digital id, 2017. URL: https://mycolorado.state.co.us/about.

[19] Ministry of Finance. Digital identity development project. URL: https://vm.fi/en/digital-identity.

[20] Javad Jarrahi. Digital id coming to finland, germany, and mexico, 2021. URL: https://www.biometricupdate.com/202102/digital-id-coming-to-finland-germany-and-mexico.

[21] Tykn.tech. Blockchain identity management: The definitive guide, 2021. URL: https://tykn.tech/identity-management-blockchain/.

[22] Cameron Faulkner. What is nfc? everything you need to know, 2015. URL: https://www.techradar.com/news/what-is-nfc.