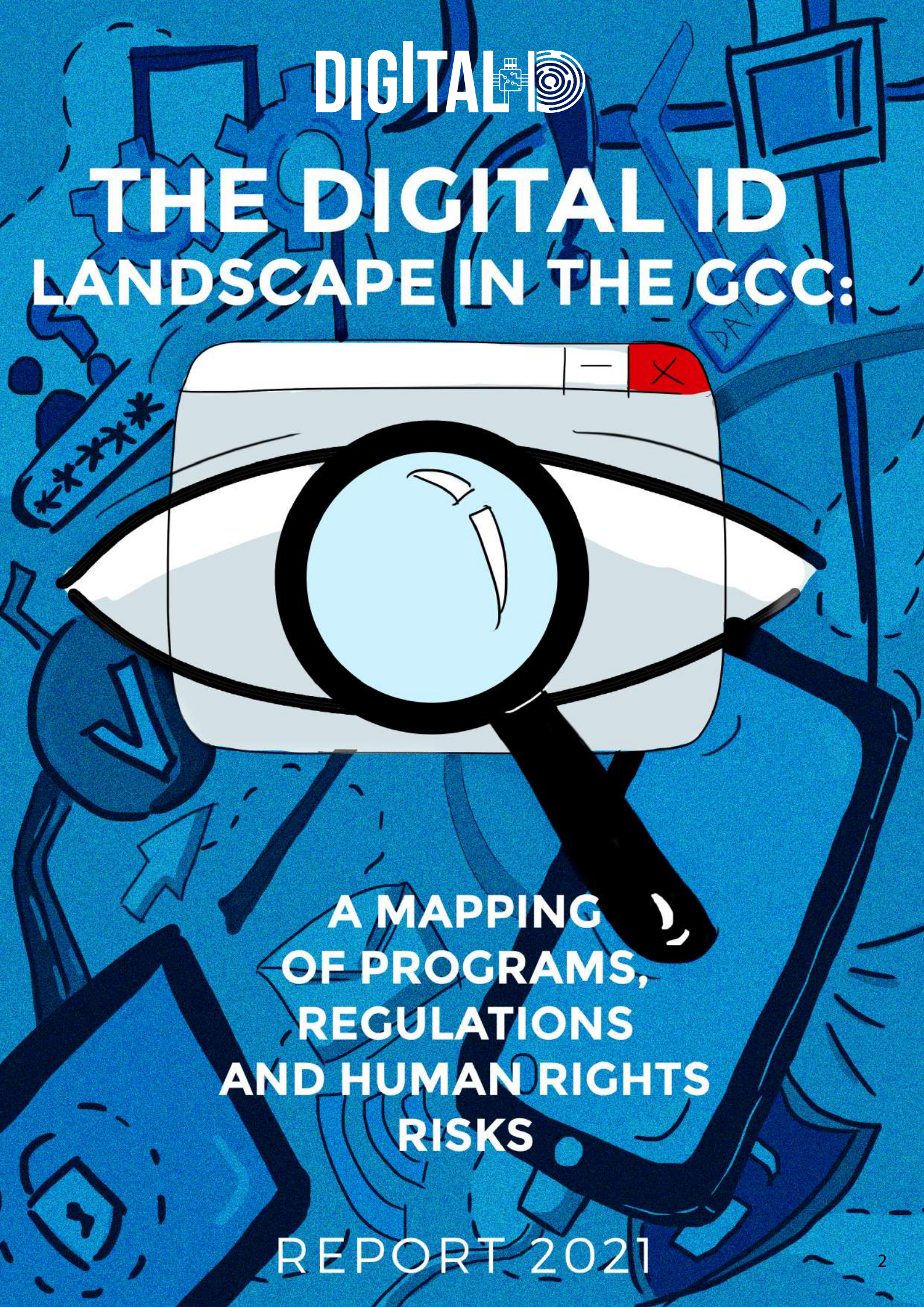
DIGITAL ID

THE DIGITAL ID LANDSCAPE IN THE GCC:



A MAPPING OF PROGRAMS, REGULATIONS AND HUMAN RIGHTS RISKS

REPORT 2021

ACKNOWLEDGEMENTS

Data collection: Afef Abrougui, Amre Metwally, Omar Daouk, Marianne Rahme, Nay Constantine, Sierra Terrana
Quality control: Nay Constantine
Additional research support: Nathan Silber, Sarah Cupler
Research supervision and coordination: Afef Abrougui
Report writing: Afef Abrougui, Omar Daouk, Marianne Rahme, Nay Constantine
Report editing: Afef Abrougui
Editorial support and proofreading: Sarah Cupler

The research was generously funded by Privacy International.

SMEX is a Lebanese NGO that since 2008 has worked to defend digital rights, promote open culture and local content, and encourage critical, self-regulated engagement with digital technologies, media, and networks across the Middle East and North Africa (MENA).

www.smex.org

A December 2021 Publication of SMEX.

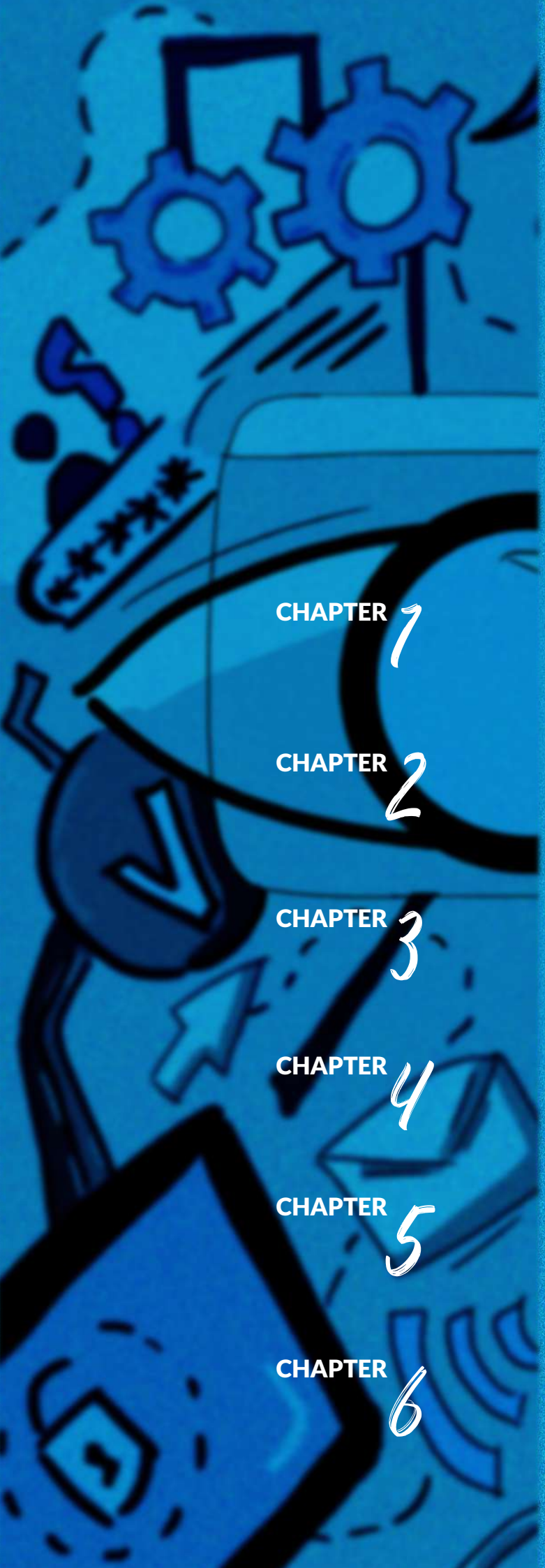


TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report analyzes the implementation of digital ID systems in countries of the Gulf Council Cooperation (GCC), also referred to in this report as the "Gulf". The GCC is an intergovernmental political and economic union made up of Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and The United Arab Emirates. The purpose of this report is to map the different digital ID initiatives in the Gulf and their impacts on privacy and human rights. It is an initial step of a larger research SMEX is aiming to conduct to map digital ID across the broader Arab region.

This report is specifically focused on Digital ID systems as promulgated by multiple UN agencies. It begins by generally explaining what Digital ID programs are and the standards and best practices needed that allow them to work safely and with consideration for individuals' rights. It draws upon these standards to compare it to the reality of implementation in the Gulf.

The report sets out the key authorities and service providers in each country and compiles all relevant legislation surrounding electronic transactions, personal data, right to privacy, government surveillance, and cybercrime and cybersecurity to map the regulatory landscape of digital ID in these countries (Chapter 3). The legislation was then analyzed, and legal and regulatory shortcomings were outlined in the next chapters. In Chapter 4, we explain how existing legal frameworks are falling short of protecting data processed by digital ID systems and adequately providing users with remedy mechanisms. In Chapter 5, we look at the data collected by (digital) identification systems in the Gulf and identify and analyze measures to ensure privacy of the data and user rights over the data. Chapter 6 identifies (potential) implications for the right to non-discrimination.

METHODOLOGY

We conducted desk research to collect information and data to map the different digital ID systems in the GCC, relevant legislation and regulations and how they compare to existing international best practices and standards. In the first step of primary data collection, information on digital ID programs in each GCC country were collected: authorities that initiated or implemented them, service providers involved in their rollout, relevant regulations and laws, types of data collected by the systems, user rights to access and control their data, security features and measures, forms of oversight over the data and and any documented cases or potential implications for human rights. A review and a quality control were then conducted to improve and expand the collected information to include oversight over ID, relevant cybercrime legislation and cybersecurity strategies and legislations and practices that enable or exclude marginalized groups in identification systems (such as stateless people and people living with disabilities). A review of existing standards and best practices for digital identification systems was also conducted, which helped us identify shortcomings in digital ID systems in the GCC and draft this report.

INTRODUCTION

The Arab Gulf States have been undergoing a digital transformation to help drive economic growth and decrease dependence on oil revenues.[1] The adoption and implementation of digital ID programs has been a key aspect of this transformation, and the first such program in the region was introduced in Bahrain in 2007 as part of an e-government strategy to facilitate access to government and private services. The other member-states—Kuwait, Oman, Qatar, Saudi Arabia and the UAE— followed suit and introduced their own programs, and in 2020, United Nations E-Government Survey ranked the GCC as a leader in e-government in the Middle East and North Africa region.[2] All GCC countries have focused upon a desire to create or bolster their digital infrastructure to facilitate access to services. Digitization is seen as a necessary aspect of modernizing the Gulf and benefiting from new technologies, advantages claimed can range from streamlining services to economic benefit.[3]

Digital ID requires a robust regulatory framework that encompasses data protection, privacy and security, cybercrime and cybersecurity legislation, and independent oversight. All countries analyzed do have a framework to regulate Digital IDs but the robustness differs; the protections are weak, include broad exemptions for public authorities handling of personal data, and lack independent oversight which coupled with poor human rights records, leaves the data used in digital ID systems vulnerable and at risk of government surveillance. The report reinforces this point by highlighting all the sensitive information collected and used for the issuances of ID cards and digital ID systems. Overall these systems can pose dangers to civil liberties and can also reinforce existing discrimination and exacerbate issues faced by marginalized groups. Although some areas are seeing improvement, there are still marked regulatory shortcomings which can negatively impact citizens and people living in these countries.

Key Findings include:

- As mandatory ID schemes are modernized and include new technology and biometric data, these schemes become more invasive and put personal data at risk.
- There is a distinct lack of strong data protection and of regulations curtailing government surveillance, which puts the privacy and data of users at risk. Only Bahrain, Qatar, and Saudi Arabia have passed general laws on data protection. Yet, these laws contain vague and broad exemptions for data processing by government agencies.
- All countries demonstrate a lack of independent oversight over both personal data processing in general and over the identification system itself, which can have harmful repercussions on personal data and human rights of ID users.
- Identification systems in the Gulf collect a broad range of data, including sensitive information, yet lack options to control such data.
- In some aspects, identification systems in the Gulf discriminate against women, girls, and marginalized groups. Such discrimination can be exacerbated when ID systems are digitized, further excluding people with disabilities, and rendering stateless populations or non-working people more vulnerable.

CHAPTER 1

DIGITAL ID: INTERNATIONAL STANDARDS AND BEST PRACTICES

CHAPTER 1

DIGITAL ID: INTERNATIONAL STANDARDS AND BEST PRACTICES

WHAT ARE DIGITAL IDENTITY AND DIGITAL IDENTIFICATION (ID) SYSTEMS?

Depending on each country and context, digital iden tity can have different meanings, but it is usually defined as a set of attributes (such as biometrics, name, unique identity number, place and date of birth, etc.) and credentials (such as identifying numbers, smart cards and certificates) that are electronically captured and stored, and that uniquely identify a person.[4]

Digital identity is used to identify and prove someone's identity online or offline (depending on uses and context in which it is being used). For example, people can use it to access government services, apply for welfare aid, vote in elections and digitally sign documents.[5]

For the purpose of this research, we are not looking at digital ID per se but on entire Digital ID systems defined by the World Bank's ID4D initiative as identification systems that ''use digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication.'' [6]

STANDARDS AND BEST PRACTICES

Given the risks that may emanate from digital ID, such as exclusion of vulnerable communities and privacy-related risks, a number of entities have sought to establish standards and best practices to ensure inclusion and protection of privacy and human rights in the implementation of digital ID systems.

In the context of the Sustainable Development Goals, the United Nations addresses the need for an identity document for every person in Goal 16:9 which encourages to "provide legal identity to all, including birth registration, by 2030". [7]

In 2017, multiple UN agencies (UNHCR, UNICEF, UNDP, ECA), alongside with other institutions and ledby the World Bank, endorsed the document, "Principles on identification for sustainable development: toward the digital age."[8] While the document focuses on the promotion of an identity for all, separate from a national document (especially for refugees), it includes principles on the protection of user privacy and data. In addition to this document, in 2016 the United Nations began to partner with ID2020, a private-public initiative to promote the access to identification documents (particularly digital identification) in the context of the SDG 16:9. ID2020 states that ''...doing digital ID right means protecting civil liberties and putting control over personal data back where it belongs...in the hands of the individual."

On the other hand, the World Bank, which has been making efforts and proposals towards the adoption of digital identification to combat poverty, inequality and social exclusion through its initiative ID4D (Identification for Development),[9] published a "Catalog of Technical Standards for Digital Identification Systems,'' offering an analysis of existing standards for digital identification. The report states: ''standards establish universally understood and consistent interchange protocols, testing regimes, quality measures, and best practices with regard to the capture, storage, transmission, and use of identity data, as well as the format and features of identity credentials and authentication protocols. Therefore they are crucial at each stage of the identity lifecycle, including enrollment, validation, deduplication, and authentication.''[10]

PRIVACY AND SECURITY BY DESIGN

A privacy by design approach entails the adoption of measures, policies and technical standards and features to ensure the protection of privacy and the security of the data from the earliest stages of the development process of a digital ID system.

Under Point 6 of the "Principles on identification for

DIGITAL ID: INTERNATIONAL STANDARDS AND BEST PRACTICES

sustainable development: toward the digital age,"[=] "Identification systems should be designed with the privacy of the end-user in mind. No action should be required on the part of the individual to protect his or her personal data. Information should be protected from improper use by default, through both technical standards and preventative business practices."[11]

Privacy by design features and measures in digital ID include, for example, encryption of data, minimization of data collection and disclosure, strong multi-factor authentication (for eg. through SIM Applet with PKI or Smartphone App in TEE with PKI, use of block chain technology, digital certificates and PKI, and providing users with options and platforms to control and access their data. [12]

SIM applet with PKI

The concept of applet is a small application within a bigger program with the sole purpose to perform one single task. A SIM applet is a small application dedicated to performing one single task within a SIM Card. When it comes to Digital IDs, SIM applets are usually used to securely create a signature. So these applets communicate with other applications (for example those that create and manage public keys) using the PKI technology.

Smartphone app in TEE

A Trusted Execution Environment (TEE) is a secure area inside a main processor. It runs in parallel with the operating system, in an isolated environment. It guarantees that the code and data loaded in the main processor are protected with respect to confidentiality and integrity. This includes the execution of authenticated code, confidentiality, authenticity, privacy, system integrity and data access rights.

Public Key Infrastructure (PKI)

PKI is a system of processes, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital IDs. PKI allows users to encrypt data, digitally sign documents, and authenticate themselves using certificates (which Digital IDs are based on).

Digital certificates

Digital certificates include three main components: identity (name, special code, expiry date), public key to encrypt holder data and signature to validate authentication. They are issued by Certificate Authorities (CAs) and are used to "facilitate secure electronic communication and data exchange between people, systems, and devices online" by verifying one's identity and encrypting/decrypting electronic messages. The distribution, revocation and authentication of digital certificates are managed by a PKI. [13]

PROPORTIONALITY AND MINIMAL DISCLOSURE

DIGITAL ID: INTERNATIONAL STANDARDS AND BEST PRACTICES

Minimizing collection and disclosure of data reduces the impact of a data breach in case of unauthorized access. "Data collected and used for identification and authentication should be fit for purpose and proportional to the use case, and managed in accordance with global norms for data protection," as stated by the "Principles on identification for sustainable development," adding that identification systems "should not disclose sensitive personal information."

Additionally, users of a digital ID system should have tools allowing them to access and control their data. For example, residents in Estonia can access and monitor their data through an online portal and decide which data to share and with whom.[14] They can also view logs of their previous transactions. The logs are automatic and tamper-proof, making them difficult to alter or delete.[15] Such logs are also essential for investigations of breach or fraud.

ROBUST LEGAL AND REGULATORY FRAMEWORKS

In addition to implementing privacy by design measures, robust legislation to ensure the protection of data and privacy of users in a digital ID system is essential. This includes robust data protection regulations, regulations curtailing government and commercial surveillance and comprehensive cybercrime legislation that safeguard human rights.

Principle 8 of the "Principles on identification for sustainable development: toward the digital age" states that "Identification systems must be underpinned by legal and regulatory frameworks and strong policies that promote trust in the system, ensure data privacy and security, mitigate abuse such as unauthorized surveillance in violation of due process, and ensure provider accountability."

Regulatory frameworks should further establish grievance and redress mechanisms that enable users to file complaints or legal disputes when a digital ID system interferes with their human rights particularly their rights to privacy and non-discrimination. When the disputes are not solved in favor of users, they should be able to escalate cases to an independent authority or a court with the prerogative to independently review initial decisions and provide redress to affected users.

INDEPENDENT OVERSIGHT

Oversight of the data and identification system should be established in law and enforced. For example, a digital ID system oversight body can be established (as in Australia[16]) or the oversight can be conducted by separate authorities overseeing the data (such as a data protection authority) and the identification system. Oversight of the data should include, for example, which data is collected and shared and for which reasons to ensure minimal collection and disclosure, how the data is stored and measures and policies to ensure its security, and whether users are able to appropriately control the collection, use and disclosure of their data.

Article 10 of the "Principles on identification for sustainable development: toward the digital age" states that "the use of identification systems should be independently monitored (for efficiency, transparency, exclusion, misuse, etc.) to ensure that all stakeholders comply with applicable laws and regulations, appropriately use identification systems to fulfill their intended purposes, monitor and respond to potential data breaches, and receive individual complaints or concerns regarding the processing of personal data."[17]

Further, any type of oversight should be the responsibility of independent authorities that are appropriately staffed and well-resourced to effectively carry out their missions.

DIGITAL ID: INTERNATIONAL STANDARDS AND BEST PRACTICES

CONSIDERATIONS FOR MARGINALIZED GROUPS

Exclusion and the disproportionate impacts of digital ID systems on marginalized groups should be taken into account. Assessments, including public consultations involving such groups, should start at the development stage and continue throughout the implementation of a digital ID system. Depending on context, marginalized groups can include people with disabilities, minorities, refugees, migrants, the elderly, and people lacking access to the internet and with low (digital) literacy. For example, in India, people receive an email notification when their Aadhaar number is used for authentication, raising concerns about those living in low connectivity areas and lacking appropriate levels of digital literacy.[18]

Exclusion can take place at different levels, and the more marginalized groups an individual belongs to the more likely they are to be negatively impacted by a digital ID system. Thus, adopting an intersectional approach can help those implementing a digital ID system better understand potential exclusion and discrimination, and take steps to prevent and mitigate their impacts on people's lives.

Among the best practices recommended by the Engine Room are, the prioritization of meaningful and ongoing public constellations that include ''people whose rights are often denied,'' adoption of '' rights-affirming legislation that prioritizes the needs of the people over the interests of the implementing institution,'' and making sure that ''information and all steps of thesystem are provided in relevant local languages, including those of significant migrant populations.''[19]

On the other hand, the "Principles on identification for sustainable development: toward the digital age'' emphasize the need for identification systems to be ''free from discrimination in policy, in practice, and by design,'' ''this includes ensuring that legal frameworks; requirements and procedures to register, obtain, or use identification; and the data that are collected or displayed on credentials do not enable or reinforce discrimination against particular groups, such as those who may face increased risks of exclusion for cultural, political, economic or other reasons...Furthermore, identification systems and data should never be used as a tool for discrimination or to infringe on or deny individual or collective rights.''[20]

CHAPTER 2

OVERVIEW OF DIGITAL ID IN THE GULF

OVERVIEW OF DIGITAL ID IN THE GULF

The six countries that make up the Gulf Council Cooperation (GCC) have all adopted and implemented digital ID systems allowing their citizens and residents to access services and perform transactions online. GCC governments have put in place ID systems for citizens and residents that rely on modern technology (often biometrics and smart chips) allowing them to (i) identify themselves, (ii) authenticate their identity online by using just one set of credentials (usually their ID card number), and (iii) become eligible for a certain number of online services, among which, electronic governmental and administrative services.

Of these countries, Kuwait and Saudi Arabia were the last ones to start implementing a digital ID program. In the midst of the COVID-19 pandemic, which further accelerated digital transformation, Kuwait introduced the Kuwait Mobile ID app in 2020.[21] The app acts as a portable mobile ID and allows citizens and foreign residents to authenticate themselves to government and non-government services online and digitally sign documents.

In 2020, Saudi Arabia launched the Unified National Platform (my.gov.sa),[22] which allows citizens and residents to access government services online using a "unified national profile" which "provides services and various information i.e. personal, educational, employment, commercial, ..etc" to citizens and residents across multiple sectors in order to create unique experiences available for use anytime, anywhere."[23] Users can log in through the Absher app, the ministry of interior 's e-services portal and app,[24] or through the National Single Sign-On system (SSO) developed by the National Information Center and the Ministry of Interior. To create their digital identities, users need to first register themselves on the SSO system.[25]

COUNTRY	NAME OF DIGITAL ID APPLICATION OR PORTAL	YEAR OF LAUNCH
BAHRAIN	BAHRAIN.BH	2007 [26]
KUWAIT	KUWAIT MOBILE ID	2020
OMAN	TAM	2013 [27]
QATAR	HUKOOMI	The Hukoomi portal was launched in 2003, and digital ID was implemented following the rollout of the biometric ID scheme in 2007.
SAUDI ARABIA	UNIFIED NATIONAL PLATFORM (MY.GOV.SA)	2020
UAE	UAE PASS	2018

TABLE 1: DIGITAL ID PROGRAMS IN THE GCC.

OVERVIEW OF DIGITAL ID IN THE GULF

In Bahrain, the Digital ID project was implemented as part of the 2007-2010 eGovernment strategy that's "focused on ensuring effective delivery of government services to citizens, residents, businesses and visitors (customers)"[28]. The e-government portal was launched in 2007. Users can register and log in through the eKey Single Sign-on-System to access government services. [29]

Oman's TAM is a digital certificate system provided by the National Digital Certification Center (NDCC) at the Information Technology Authority (ITA).[30] It allows citizens and residents to authenticate their digital ID online to access government services as well as to sign in and validate their documents electronically using an ID card and a PKI enabled SIM card.

In 2007, the Government of Qatar (GoQ) began rolling out biometric enabled ID cards that were ultimately leveraged to implement an e-Government scheme and allow access to e-services through a portal called "Hukoomi," hosted at the Ministry of Transport and Communications (MoTC) level (particularly, through ictQatar: Supreme Council of Information and Communications Technology).[31] The e-services are accessible to individuals through their e-ID card. Users use their e-ID as a secure credential and input a personal code to identify themselves. Further, the e-ID can also be used with a 6-digit pin for authenticating online transactions (such as signing documents electronically).

The UAE Pass,[32] launched in 2018, enables residents and citizens to access local and federal government services and sign documents digitally by authenticating their identities using a mobile phone application.[33] Users simply need to register with the app and scan their Emirates ID or passports, verify their phone numbers or email addresses and secure the accounts by creating a PIN, Touch ID or Face ID.

Key service providers and responsible authorities

For all GCC countries, Thales, a French multinational company that designs and builds electrical systems and provides services for the aerospace, defense, transportation, and security markets, has had a key role in implementing their digital ID programs. The extent of Thales' role in rolling out these digital ID systems differs between countries. However, in all GCC countries Thales had a role in rolling out their electronic identification systems. For example, Gemalto, acquired by Thales in 2019,[34] was contracted by the Bahraini government to not only provide smart ID cards, but to also "provide consultancy on smart card related solutions, including Public Key Infrastructure and smart card applications and training."[35] In the UAE, Thales contributed to the rolling out of the country's national eID program,[36] but the single identity solution was developed by Smart Dubai. In Qatar, using its Gemalto 2.0 solution, Thales worked with Qatar's Supreme Council of Information and Communication Technology (ictQATAR) to improve and simplify user experience on the Hukoomi portal and enhance security.[37] The solution offers single-sign-on to all services available on the Hukoomi portal and simply requires users to use their eID and a personal code as identification.

Additionally, other entities have had a key role in initiating and implementing these programs such as ministries of interior and the police, ID authorities, telecommunication regulatory agencies and cybersecurity agencies and companies. Below is a list of some of the key entities and authorities responsible for digital ID for each GGC country.

OVERVIEW OF DIGITAL ID IN THE GULF

COUNTRY	RESPONSIBLE AUTHORITY OR AUTHORITIES
BAHRAIN	• The Supreme Council for Information & Communication Technology (SCICT).[38] Chaired by the Deputy Prime Minister and established by ministerial decision in 2015,[39] it is tasked with implementing e-government directives. • The Information & eGovernment Authority of Bahrain (iGA). The authority, which is part of the Ministry of the Interior, issues ID cards and birth and death certificates. It is also tasked with "proposing public policies, suitable legislation, and decisions for the implementation of the eGovernment programs as well as necessary information technology and data programs." [40]
KUWAIT	• Public Authority for Civil Information (PACI).[41] Affiliated with the minister of planning, PACI was tasked by the Kuwaiti government to manage the country's smart civil ID card program. It released the mobile ID (Hawyti) application in 2020.
OMAN	• The Directorate General of Civil Status at the Royal Oman Police. It is responsible for the national ID system, it issues ID cards and maintains population registers.[42] Under Royal Decree No. 66 of 99,[43] the Royal Oman Police "made a decision to launch a smart card-based ID programme, not only to enhance the country's identification processes, but also to improve its IT infrastructure." • National Digital Certification Center at the Ministry of Transport, Communications and Information Technology (MTCIT). It provides the digital certification service, TAM. [44]
QATAR	• Supreme Council of Information and Communications Technology). The council sets the technology policy in Qatar.[45] It worked with Thales to improve the Hukoomi portal.[46] • National Authentication System (Tawtheeq).[47] It "acts as a national identity provider for all the government online services. It provides a secure authentication, digital signing and Single-Sign-On (SSO) services and is a key component in e-services development and security." • The General Directorate of Information Systems at the Interior Ministry. It is tasked with "develop[ing] the information technology at the ministry".[48] It lists among its accomplishments the "Qatari Smart ID Card system," although it is unclear what its role is or was in putting the system in place.[49]

OVERVIEW OF DIGITAL ID IN THE GULF

COUNTRY	RESPONSIBLE AUTHORITY OR AUTHORITIES
SAUDI ARABIA	• Digital Government Authority.[50] Created in 2021 by the Council of Ministers (Council Resolution No. (418) dated 25/7/1442 AH), [51] the authority is "concerned with everything related to digital government and it is the national reference in its affairs. It aims to regulate the work of digital government in government agencies, in order to reach a digital and proactive government capable of providing highly efficient digital services, and achieving integration in the field of digital government among all government agencies." It is responsible for the gov.sa portal.[52] • Interior ministry. It developed the National Single Sign-On system with the National Information Center.[53] The Agency of Civil Affairs at the ministry registers birth and death certificates, and issues and renews national identity cards. [54] • The National Information Center.53 It provides government agencies with "technology services and digital solutions."[55]
UAE	• Telecommunications Regulatory and Digital Government Authority (TDRA). Established by Federal Law by Decree No. 3 of 2003 (Telecom Law),[56] TDRA is tasked with regulating the telecom industry and enabling digital transformation.[57] • The Dubai Smart Government Establishment (or Smart Dubai). It is a government body tasked with "facilitating Dubai's citywide smart transformation."[58] It developed the UAE Pass after signing a MoU with the Telecommunications Regulatory and Digital Government Authority (TDRA) "to develop a single trusted digital identity solution in the UAE."[59] • Abu Dhabi Digital Authority (ADDA).[60] It is a government agency working to support and enable Abu Dhabi's digital transformation. • The Dubai Electronic Security Centre (DESC). It is a government department tasked with ensuring Dubai's cyber security. It served as a "strategic partner providing the underlying Digital Certificates contributing to safeguard UAEPASS." [61]

TABLE 2: GOVERNMENT STAKEHOLDERS AND ENTITIES RESPONSIBLE FOR IMPLEMENTING DIGITAL ID PROGRAMS

OVERVIEW OF DIGITAL ID IN THE GULF

Mandatory nature of ID

The mandatory nature of ID systems opens the door to increased government power to restrain freedoms and civil liberties of those who either refuse to or are ineligible to enroll in such systems. [62]

Further, in some instances, ID schemes can be mandatory for certain groups while remaining voluntary for others.[63] Such discrimination can also occur when ID is mandatory in effect rather than overtly, as state benefits may be directly linked to it and made unavailable for those who do not hold an ID.

As countries modernize their ID schemes and include technologies such as biometrics (fingerprints/irises/palms) and facial recognition, making such systems mandatory becomes more invasive and increases function creep (when personal information is used for purposes other than the original purpose or purposes for which they were collected) and risks of personal data protection violations.

Gulf countries are no exception to the rule: whether it is in Bahrain, Kuwait, Saudi, Oman or the UAE, enrolling in ID databases for both nationals and residents is required. Additionally, Bahrain, Saudi Arabia, and the UAE have mandatory biometric SIM registration laws.[64] This raises concern over the risks to ID holders' sensitive personal information and highlights the importance of safeguarding their individual right to privacy by surrounding the use of biometrics with protective legislation.

COUNTRY	MANDATORY NATURE OF ID
BAHRAIN	*Under Law No. (46) of 2006 regarding identity cards, it is mandatory to carry an ID card in Bahrain.[65] Neither the law nor its implementation regulation (Resolution No. (1) of 2007) specify at which age it is mandated to carry one. However, the Information and e-Government Authority (IGA) at the Interior Ministry offers a service for issuing ID cards for children below four years old.[66]*
KUWAIT	*A civil ID card is a requirement for any citizen or foreign resident. It is issued for anyone 16 years old and above.[67]*
OMAN	*Every male Omani citizen above 15 years old must apply for an ID card, it is optional for females.[68]*
QATAR	*Mandatory for all Qataris and residents (those staying in the country for over six months) aged 16 and above.[69]*
SAUDI ARABIA	*An ID card is mandatory for all citizens aged 15 and above.[70]*
UAE	*It is mandatory for all citizens and residents to apply for an Emirates ID.[71]*

TABLE 3: MANDATORY NATURE OF ID IN GULF COUNTRIES

EXISTING REGULATORY FRAMEWORKS

All GCC countries have in place legal frameworks that regulate Digital ID, although the framework's level of development differs from one country to another. The regulation of digital ID happens through different types of legislation: legislation on ID cards and national identification systems, electronic transactions, personal data protection and cybercrime and cybersecurity. The legal frameworks, however, present some shortcomings, most notably regarding the lack of robust data protection regulations, oversight and availability of remedy mechanisms (See chapter 4).

Legislation regulating identity cards and national identification systems

ID legislation is concerned with the procedure and conditions for issuing and reviewing ID cards, the establishment of population registers and the types of information they contain, and the prerogatives and tasks of ID-related bodies or departments. A number of countries also have legislation specifically establishing digital ID.

COUNTRY	RELEVANT LEGISLATION
BAHRAIN	• *Law No. 46 of 2006 regarding the identity card relates to ID cards containing an electronic chip which stores information and data to identify the card holder such as blood type, fingerprints, iris scan and prescribes punishments for fraud and other crimes related to ID.[72] The law's executive regulations (Resolution No. (1) of 2007 and Resolution No. 16 of 2011 amending it) lay down the procedures for issuing, renewing and replacing the ID card, data contained in the card, the responsibilities of the card holder, and other provisions.[73]*
KUWAIT	• *Law No. 32 of 1982 regarding the civil information system established a population register of the civil information of Kuwaitis and non-Kuwaitis in the country such as birth information, marriage data, religion, data related to military service for Kuwaitis, residence, etc. [74]* • *PACI decisions No.1 of 2012 dated 8 April 2012 regarding the civil ID card equipped with an electronic chip for Non-Kuwaitis and No.2 of 2009 regarding the civil ID card equipped with an electronic chip for Kuwaitis.[75]* • *Decision 1 of 2020 invoking the Electronic Civil ID card (Kuwait Mobile ID).[76]*
OMAN	• *Civil Status Law (established by Royal Decree No. 66 of 99 and amended by Royal Decree No.59 of 2021), which established a department within the Oman Police called the "Directorate General of Civil Status" and tasked with recording and keeping the data of citizens and foreign residents.[77]*

EXISTING REGULATORY FRAMEWORKS

COUNTRY	RELEVANT LEGISLATION
QATAR	• Decree Law No 5 of 1965 as amended by Decree Law No. 37 of 2005 and Decree Law No. 13 of 2013.[78] The brief law mandates that all citizens and residents aged 16 and above must have an ID card and specifies the types of data that appear on the card, the card's validity and the issuing authority.
SAUDI ARABIA	• The Ministry of Interior's instructions about National ID set the conditions and responsibilities for carrying a national ID card.[79]
UAE	• Federal Law No (9) of the Year 2006 on the Population Register and the ID Card System[80] and their Executive Regulations. The regulations[81] govern the population register system and Emirates ID card in the country and stipulates what information appears on the ID and its micro-chip, the process for obtaining an ID and the duties of its holder. • Federal Decree-Law No. (2) of the Year 2004 on Establishment of the Federal Authority for Identity and Citizenship. It establishes an authority tasked with "establish[ing] and updat[ing] the population register system and issuance of the ID cards for the citizens and residents, and for these purposes." Among the duties it performs is "Register[ing] the personal data of all the population in the State and save it on E-databases in coordination with the competent entities," "Register[ing] the essential statistical data of population and connect it with the personal data and "Issu[ing] ID cards having the unified number, readable data and data stored on E-chip to be used in all the entities."[82]

TABLE 4: ID-RELATED LEGISLATION IN THE GCC

Electronic transactions, electronic communications, and e-commerce legislation

E-transactions and e-communications laws primarily regulate communications and transactions that occur online, including e-government services that often involve the use of digital identification. Establishing such laws ensures an environment of trust and enables the use of digital identity in a safe manner by providing legal value to electronic processes and authentication mechanisms such as electronic signatures, granting them the same legal status as traditional paper-based processes.

EXISTING REGULATORY FRAMEWORKS

In the GCC context, several countries have adopted and implemented electronic transactions/communications frameworks. In Oman, for instance, the government launched the Electronic Certification (TAM) service provided by the National Digital Certification Center (NDCC) at the Information Technology Authority (ITA) to provide electronic access to government services and transactions using digital authentication.

Similarly, GCC countries seem to have either incorporated e-commerce provisions in their electronic transaction law (UAE) or enacted standalone e-commerce acts. By governing rights and obligations of online businesses and online users, e-commerce legislation fosters trust in the cyber space and allows for a safer use of digital ID in online commercial transactions.

COUNTRY	E-TRANSACTIONS LEGISLATION
BAHRAIN	*Decree-Law No. (54) of 2018 issuing the Law on Electronic Communications and Transactions. The law repeals the previous electronic transactions law (Decree-Law No. (28) of 2002) and "expands the range of transactions[83] that may be carried out electronically."*
KUWAIT	*Law No. 20 of 2014 Concerning Electronic transactions[84] and its Executive Regulations – Ministerial Resolution No. 48 of 2014 on 4 January 2015 (the "ET Bylaws"). "Article 2 of the ET Law provides for the scope of its application which includes electronic records, messages, information, documents and signatures related to civil, commercial and administrative transactions and to any disputes arising from or in connection with their use, unless the parties agreed otherwise, or another law applies." [85]*
OMAN	*The Electronic Transactions Law Issued by Royal Decree No. 69 of 2008.[86] It is the first E-transactions law in Oman. It applies to electronic transactions, records, signatures, and to any electronic messages.*
QATAR	*Decree Law No. (16) of 2010 on the Promulgation of the Electronic Commerce and Transactions Law.[87] The e-Commerce Law contains provisions on e-signatures, e-documents, and authentication. It addresses e-Commerce transactions in Qatar, as well as e-Government services.*

EXISTING REGULATORY FRAMEWORKS

COUNTRY	E-TRANSACTIONS LEGISLATION
SAUDI ARABIA	*Electronic Commerce Law (Royal Decree No. M/126 dated 10 July 2019).[88] It applies to products and services offered "in part or in whole, through an electronic medium" by service providers inside the kingdom and overseas to consumers in the country.* *Electronic Transactions Law (Royal Decree No M/18) provides a legal framework for electronic transactions and signatures. It defines electronic transactions as "any exchange, communication, contracting or other procedure, performed or executed, wholly or partially, by electronic means."[89]*
UAE	*Federal Law No. 1 of 2006 Concerning Electronic Transactions and Commerce. The law regulates "Electronic Records, Documents and Signatures that relate to Electronic Transactions and Commerce." Its objectives include "protect[ing] the rights of persons doing business electronically and determine their obligations," "promoting] the development of the legal and business infrastructure necessary to implement secure Electronic Commerce," "Minimiz[ing] the incidence of forged Electronic Communications, alteration of Communications and fraud in Electronic Commerce and other Electronic Transactions," and "Establish[ing] uniform rules, regulations and standards for the authentication and validity of Electronic Communications."[90]*

TABLE 5: LEGISLATION ON ELECTRONIC TRANSACTIONS AND COMMERCE IN THE GCC.

Legislation on privacy and data protection

Digital ID systems involve heavy processing of personal data and creates a real risk on users' privacy. Hence, establishing safeguards for data privacy, security, and user rights through a comprehensive legal and regulatory framework is essential to build trust in the ID system.

Digital ID systems must protect users' privacy and grant them control over their personal data as well as be compliant with internationally recognized standards and principles such as data minimization, purpose limitation, security, accountability and oversight.

EXISTING REGULATORY FRAMEWORKS

While most countries who have adopted data protection laws have resorted to standalone overarching legislation, in the GCC, only Bahrain, Qatar and Saudi Arabia have passed general laws on personal data protection. All countries have recognised the right to privacy to some degree and specifically guarantee privacy of communication.

However, government surveillance is at best weakly regulated and at worst allows for extensive surveillance powers. Countries that have some provisions against surveillance, such as Bahrain and Qatar, have broad exemptions to permit government surveillance and others, such as Saudi Arabia and the UAE, do not specify what constitutes lawful surveillance.

COUNTRY	DOES THE CONSTITUTION ENSHRINE THE RIGHT T O PRIVACY?	DOES THE COUNTRY HAVE DATA PROTECTION LAWS?	DOES THE COUNTRY HAVE REGULATIONS CURTAILING GOVERNMENT SURVEILLANCE?
BAHRAIN	Bahrain's constitution as amended in 2012[91] guarantees privacy of postal, telegraphic and telephonic communications.[92] Article 25 provides for the Right to privacy in dwellings.	Law No. (30) of 2018 with Respect to Personal Data Protection Law. [93]	Only vague and broad provisions that do not detail how government surveillance, which is rampant in the country, is curtailed in practice. Article 26 of the Constitution as amended in 2012, protects against the disclosure of private communications and states, "No communications shall be censored nor the contents thereof revealed except in cases of necessity prescribed by the law and in accordance with the procedures and guarantees stated therein." Additionally, provisions of the Personal Data Protection Law do not apply to "national security–related data processing undertaken by the MOI, the NSA, the Defense Ministry, and other security services."[94]

EXISTING REGULATORY FRAMEWORKS

COUNTRY	DOES THE CONSTITUTION ENSHRINE THE RIGHT T O PRIVACY?	DOES THE COUNTRY HAVE DATA PROTECTION LAWS?	DOES THE COUNTRY HAVE REGULATIONS CURTAILING GOVERNMENT SURVEILLANCE?
KUWAIT	Not expressly but through the freedom and secrecy of communications right enshrined in Article 39 and the inviolability of home enshrined in Article 38 of the 1962 Constitution.[95]	No	No express law limiting governmental surveillance.
OMAN	Recent recognition of the right to private life in Article 36 of the new constitution[96] – a right that was not previously recognised in such a manner in Oman.[97]	No	Only vague and broad provisions that do not detail how government surveillance is curtailed in practice. Article 36 of the Basic Law guarantees that "it is not permitted to monitor or inspect or reveal" the content of communication except where authorized by law. The Cyber Crime Law criminalizes accessing electronic information or softwares without authorization.[98] A cyber defense system established by decree No. 64 of 2020 system "gives absolute control to the Internal Security Service over communication networks and information systems in the country." [99]

EXISTING REGULATORY FRAMEWORKS

COUNTRY	DOES THE CONSTITUTION ENSHRINE THE RIGHT T O PRIVACY?	DOES THE COUNTRY HAVE DATA PROTECTION LAWS?	DOES THE COUNTRY HAVE REGULATIONS CURTAILING GOVERNMENT SURVEILLANCE?
QATAR	Article 37 of Constitution: "The sanctity of the individual's privacy shall be inviolable, and therefore interference in a person's privacy, family affairs, home or correspondence, or any other act of interference that may demean or defame a person, shall not be allowed, save as permitted by the provisions stipulated in the Law." [100]	Data Protection Law No. 13 (2016) (offers safeguards for the individuals concerned with how their ID-related information is being processed electronically in the recent digital scheme). [101]	No. 2006 Telecommunications law, under Chapter 15 states that "power of monitoring and enforcement," with the permission of the Attorney General and the Chairman of the Board, "may require service providers or others to provide information necessary for exercising its powers, and the information shall be furnished in the form, manner, and time as the government specifies."[102]
SAUDI ARABIA	Article 37 of the Basic Law of Governance of 1992 as amended in 2013 provides for a right to "physical" privacy by stating that "dwellings are inviolable."[103] Article 40 guarantees the right to privacy of telephone, postal and other means of communication. [104]	Personal Data Protection Law (PDPL) implemented by Royal Decree M/19 of 9/2/1443H (16 September 2021) approving Resolution No. 98 dated 7/2/1443H (14 September 2021). [105]	Only vague and broad provisions that do not detail how government surveillance, which is rampant in the country, is curtailed in practice. [106] Article 40 of the Basic Law of Governance 1992 also guarantees "there will be no surveillance or eavesdropping, except in cases provided by the Law." This is supplemented by article nine of Telecommunications Act 2001. [107] Article 3 of the Anti-Cyber Crime Law of 2007, imposes a fine and one year prison sentence for unlawful surveillance. [108]

EXISTING REGULATORY FRAMEWORKS

COUNTRY	DOES THE CONSTITUTION ENSHRINE THE RIGHT T O PRIVACY?	DOES THE COUNTRY HAVE DATA PROTECTION LAWS?	DOES THE COUNTRY HAVE REGULATIONS CURTAILING GOVERNMENT SURVEILLANCE?
UAE	Article 31 of the Constitution "provides for the right to freedom and secrecy of communication by post, telegraph, or other means of communication under law."[109]	No	Only vague and broad provisions that do not detail how government surveillance, which is widespread in the country,[110] is curtailed in practice. Article 378 of the Penal Code makes surveillance, unless authorized by law or without the consent of the individual, punishable by up to seven years. [111] Article 2 of the Cybercrime law criminalizes accessing information that is unlawful, "without authorization or in excess of authorization." [112]

TABLE 6: LEGISLATION CONCERNING PRIVACY AND DATA PROTECTION AND CURTAILING GOVERNMENT SURVEILLANCE IN THE GCC.

OVERVIEW OF DIGITAL ID IN THE GULF

Legislation on cybercrime and cybersecurity

In the same way that data protection and privacy provide safeguards that help mitigate the existing security and privacy risks in digital ID systems, cybercrime and cybersecurity constitute an essential pillar of the legal framework for digital ID's safe implementation.

While cybercrime legislation is primarily concerned with prescribing punishments for crimes committed through and against computer networks and systems, cybersecurity focuses on protection and defense of these networks and systems.

In the context of digital ID, cybercrime legislation would help protect against crimes such as:

- The unauthorized access to ID systems or other databases holding personal data of ID holders
- The unauthorized monitoring/surveillance of ID systems or other databases holding personal data or unauthorized use of personal data
- The unauthorized alteration of data collected or stored as part of ID systems or other databases holding personal data
- The unauthorized interference with ID systems or other databases holding personal data of ID holders

Cybersecurity frameworks on the other hand, would help identify ID systems as critical infrastructure, provide for mechanisms to report cybersecurity incidents and breaches, allow the establishment of computer emergency response teams to investigate breaches, and help set standards for information technology security of government systems and databases.

In the GCC, as shown by the below table, all countries have adopted laws to govern cybercrimes which highlights the importance given by these governments to protecting their information systems and networks. Similarly, all of them have set in place national cybersecurity strategies among which, Oman has developed one considered particularly robust.[113]

OVERVIEW OF DIGITAL ID IN THE GULF

COUNTRY	DOES THE COUNTRY HAVE CYBERCRIME LEGISLATION?	DOES THE COUNTRY HAVE A CYBERSECURITY STRATEGY?
BAHRAIN	Law No. 60 of 2014 regarding information technology crimes. [114]	According to the eGovernment portal (bahrain.bh), "the National Cybersecurity Centre is working with the Information & eGovernment Authority (iGA) and other government entities on a National Cybersecurity Strategy, which is expected to be announced soon. The strategy will help combat and mitigate cybersecurity threats, protecting the Kingdom's interests in cyberspace."[115]
KUWAIT	Cyber Crime Law No. 63 of 2015. [116]	National Cybersecurity Strategy by the Central Agency for Information Technology.[117]
OMAN	Royal Decree No 12/2011 Issuing the Cyber Crime Law. [118]	Oman was cited by the International Telecommunication Unions (ITU) and ABI Research as one of the "best prepared" countries in the world to prevent cyber attacks thanks to its High Level Cyber Security Strategy and Master Plan, and Comprehensive Roadmap.[119]
QATAR	Law No.14 of 2014 Issuing the Law on Combating Cyber Crime. [120]	In 2014, Qatar adopted a National Cybersecurity Strategy, which its objectives include "Safeguard[ing] the national critical information infrastructure" and "Establish[ing] a legal and regulatory framework to enable a safe and vibrant cyberspace".[121]

OVERVIEW OF DIGITAL ID IN THE GULF

COUNTRY	DOES THE COUNTRY HAVE CYBERCRIME LEGISLATION?	DOES THE COUNTRY HAVE A CYBERSECURITY STRATEGY?
SAUDI ARABIA	Anti-Cyber Crime Law (Royal Decree No M/17). [122]	The National Cybersecurity Strategy was developed to achieve "a safe and reliable Saudi cyberspace that enables growth and prosperity." [123]
UAE	Federal Decree-Law No. 5 of 2012 on Combating Cybercrimes (Cybercrime Law). [124]	The National Cybersecurity Strategy 2019 includes five pillars and goals: "implementing a comprehensive legal and regulatory framework," "enabling a vibrant cybersecurity ecosystem," "establishing a robust 'National Cyber Incident Response Plan'," "protecting critical assets," and "mobilising the whole ecosystem through local and global partnerships." [125]

TABLE 7: CYBERCRIME LEGISLATION AND CYBERSECURITY STRATEGIES IN THE GCC.

CHAPTER 4

DATA PROTECTION, INDEPENDENT OVERSIGHT AND ACCESS TO REMEDY

DATA PROTECTION, INDEPENDENT OVERSIGHT AND ACCESS TO REMEDY

As explained in the previous section, most countries have comprehensive legal frameworks regulating most aspects related to Digital ID. However, these legal frameworks are falling short in certain areas, particularly when it comes to protection of personal data and ensuring strong independent oversight of the digital ID system and data.

DATA PROTECTION LAWS: VAGUE LANGUAGE AND BROAD EXEMPTIONS

Not all GCC countries have adopted data protection laws, and when these laws do exist—in the case of Bahrain, Qatar and Saudi Arabia—vague language and broad exemptions for public authorities's processing of personal data coupled with the region's poor human rights track record and massive surveillance leaves the data in the digital ID system at risk of government surveillance.

In Qatar, Article 18 of the Data Protection Law states that: "The Competent Authority may decide to process some Personal Data, without abiding by the provisions of Articles (4), (9), (15) and (17) hereof, for achieving any of the following purposes:
1.Protecting national and public security.

2.Protecting international relations of the state.

3.Protecting the economic or financial interests of the state.

4.Preventing any criminal offense, or gathering information thereon or investigating therein."[126]

The articles establish conditions for the processing of personal data. They require data controllers to obtain consent of individuals before processing their data (Article 4) and to inform data subjects of "lawful purposes" and "comprehensive and accurate description of the processing activities and the levels of disclosure" before they start processing their data (Article 9).

These exemptions to the law in the name of "national and public security," "international relations of the State," "economic or financial interests of the State," or even "preventing any criminal offense, or gathering information thereon or investigating therein," allows authorities to process personal data without abiding by the provisions of the Data Protection Law. These exemptions are broad, vague, and could be manipulated by any government against the privacy of its people.

The exemption in 4) is especially dangerous since it allows data processing in "prevention," which therefore could lead to massive surveillance.

In Bahrain, the scope of the Personal Data Protection Law (Law No 30 of 2018) is also limited when it comes to data processing by public authorities.[127] Article 1(4) of chapter 1 exempts "processing operations concerning public security handled by the Ministry of Defense, Ministry of Interior, National Guard, National Security Service, or other security body in the Kingdom" from abiding by the law's provisions. Similar to Qatar, the provisions of the law do not apply for the processing of data concerning "public security" handled by any security body in the Kingdom of Bahrain. This exemption is extremely dangerous as it allows security bodies to process data without abiding by any provisions that guarantee the rights of data subjects such as processing "for specific, explicit and legitimate purpose," (Article 3) and obtaining the data subject's consent (Article 4).

In Saudi Arabia, the new PDPL, states that "data processing does not necessarily require the data subject's consent" if the processing would result in a "clear benefit" and attempting to contact the data subject would have been "impossible or impractical," "if it is required by law or a prior agreement to which the data subject is a party, or if the controller is a public entity and the processing is required for security or judicial purposes." In these cases, consent is not required.[128]

DATA PROTECTION, INDEPENDENT OVERSIGHT AND ACCESS TO REMEDY

LACK OF STRONG INDEPENDENT OVERSIGHT

Digital ID programs in the Gulf region provide many facilities for its users including administrative services, healthcare, electoral services, e-wallets, e-signatures, travel documents, etc. Providing so many services also means collecting massive amounts of data and biometric information from users.

Overseeing these ID systems is an important step towards protecting users, their data and their human rights. The countries analyzed all lack strong and independent oversight over data collection and protection of privacy. Two main issues have been identified, the first is the lack of independent oversight over the data (for example, to ensure minimal collection and disclosure and whether users are able to appropriately control the collection, use and disclosure of their data), and the second is the lack of independent oversight over the identification system to ensure fairness and prevent exclusion. These shortcomings can have major repercussions on personal data protection and human rights.

Because the ID system is managed by a governmental entity, this gap creates significant risks of potential abuse and misuse of the system and the data of its users.

In Oman, The Directorate General of Civil Status of the Royal Oman Police is responsible for the national ID system. It issues ID cards and maintains population registers.[129] Researchers were not able to locate evidence of any type of oversight over the ID system or the data. Oman does not have a comprehensive data protection law or a data protection authority.

Kuwait does not have any data protection law either. The ID data is stored and accessed by the Public Agency for Civil Information. The oversight over its Digital ID program is lacking and no independent authority is tasked with overseeing the national ID system.

In Qatar, the The General Directorate of Information Systems at the interior ministry is tasked with "develop[ping] the information technology at the ministry" [130] and lists among its accomplishments the "Qatari Smart ID Card system."[131] There is a Human Rights Department at the Ministry of Interior, but it is unclear if it performs any oversight of the ID system.[132]

A number of countries have some kind of limited oversight of electronic transactions. In the UAE, under the 2006 Federal Law on Electronic Commerce and Transactions, the Certification Services Controller oversees "certification services particularly in relation to the licensing, approval, monitoring and overseeing of the activities of Certification Service Providers." Similarly, in Kuwait, the Electronic Transactions Law establishes a body "to supervise the issuance of licenses necessary for carrying out electronic authentication and electronic signature services and other services in the field of electronic transactions and information."[133] In Qatar, under the Electronic Transactions Law, the Supreme Council of Information and Communication Technology (ictQATAR) sets requirements for electronic transactions and signatures. It is tasked with a number of oversight powers such as "oversee[ing] the provision, use and development of electronic transactions and commerce means;" and "set[ting] the appropriate criteria and standards to protect the consumers that use electronic transactions or electronic commerce services."[134]

Other countries in the Gulf do have personal data protection legislations but task government entities to do the data-related oversight.

DATA PROTECTION, INDEPENDENT OVERSIGHT AND ACCESS TO REMEDY

In Bahrain, Article 30 of the Personal Data Protection Law establishes a Personal Data Protection Authority which "shall undertake all assigned duties and granted powers necessary to protect personal data," including "overseeing and inspecting Data Controllers' activities with respect to processing of personal data...," "receiving reports and complaints concerning breach of provisions of this Law," and investigating them.[135] The authority, however, lacks independence. Its duties and powers are assumed by the Ministry of Justice, Islamic Affairs and Waqf under Royal Decree No. (78) of 2019 on the Administrative Entity to Assume the Duties and Powers of Personal Data Protection Authority. The Minister of Justice oversees the authority's work.[136]

In Qatar, the Compliance and Data Protection (CDP) department at the Ministry of Transport and Communications (MOTC) is tasked with "implement[ing] the Personal Data Privacy Protection Law. Its responsibilities include "investigating complaints and violations relating to data privacy protection."[137]

ACCESS TO REMEDY

ID systems, particularly digital ones, may give rise to errors in information, misuses of the data, mistreatment by agents, and other undue burdens that may be imposed on ID users and holders. It is, therefore, crucial for an ID system to include relevant means to both (i) anticipate and (ii) remedy these grievances. Users of ID systems should indeed be able to file complaints, demand access and rectify any errors in the system that impact them or their right to identity.

Types of redress mechanisms can vary from online complaints to offline, whether in writing or by phone etc.[138] Several of the GCC countries have in place redressal mechanisms.

Saudi Arabia's Unified National Platform,[139] for instance, allows users to access the information shared, obtain it, and correct it by sending an email request at a specified address. There is also a judicial review mechanism by the Supreme Judicial Council and relevant information about access to such review is available on the platform's website. [140] Users can file complaints electronically on the Council's external portal.

In Oman, a specific page is made available on Oman.om for citizens to report and file complaints about "any electronic service provided by government institutions."[141] The portal is managed by the Ministry of Technology and Telecommunications.

In the UAE, The UAE Pass also has a support page and a phone number allowing users to submit complaints and suggestions.[142] The government of Dubai has also put in place an e-complaint system that allows users to provide their feedback and complaints over a wide-range of services such as passports and identity cards, entry and residence permits etc. It is unclear, however, if an alternative offline mechanism exists.[143]

However, in the absence of relevant data protection authorities in most GCC countries, the scope of grievance redressal mechanisms for ID systems remains limited. Even where data protection supervisory entities exist, such as in Qatar or Bahrain, the fact that they are hosted by ministries such as the Ministry of ICT in Qatar's case, and the Ministry of Justice in Bahrain, does not allow for independent oversight and adjudication of grievances.

PRIVACY AND SECURITY

Identification systems in the Gulf collect a range of data on users, including ID numbers, biometric data (such as fingerprints, facial recognition and iris scans), contact details, residential addresses, employment and education details, and health-related information like blood type and disability status.

The table below summarizes the types of data collected for issuance of ID cards and for registration in the digital ID system, demonstrating how identification systems in the Gulf do not always minimize data collection. For example, foreign residents in Kuwait need to submit copies of the civil IDs of other residents living in the same address as well as other documents and data to obtain an ID card. In Oman, foreign residents are also required to submit more data and documents, including health related data ("original and copies of the Manpower form after medical examination").

For registration purposes, Digital ID systems collect at least ID numbers and phone numbers. Additional information such as date of birth (Bahrain), email address (Kuwait and UAE), nationality (Bahrain) and passport number (Kuwait) are required for foreign residents. For identity verification, the UAE Pass collects face ID biometrics. However, this is optional and users who do not want to use face ID verification can visit a nearby kiosk with their Emirates ID. In Kuwait, submitting a selfie for identity verification is required.

PRIVACY AND SECURITY

COUNTRY	DATA COLLECTED FOR ISSUANCE OF ID CARD	DATA COLLECTED FOR REGISTRATION IN THE DIGITAL ID SYSTEM
BAHRAIN	Old ID card (if existing), passport data (a copy of the passport), proof of residence for non-Bahrainis, declaration of citizenship or valid passport for Bahrainis, blood type, employment/education details, address and fingerprints. [144]	Citizens and residents need to register with their ID and phone numbers and submit data such as date of birth, and for GCC citizens, provide their nationality, gender and full name. Submitting an email address is optional. [145]
KUWAIT	For first time issuance[146]citizens need to submit a birth certificate, photos, fingerprints, address details and nationality certificate. Expatriates[147] need to submit passport data, photos, fingerprints, blood type certificate, a lease contract, and copies of civil IDs of other residents living in the same address. For GCC citizens,[148] birth certificate data, photos, blood type certificates, lease contract, passport data, fingerprints, marriage contract "if issued in Kuwait or if the wife has Kuwaiti nationality," and a certificate from an educational institution for those attending school or college is required.	Civil number, card serial number or mobile ID serial number, passport number for non-Kuwaitis, email, mobile phone number and a photo (a selfie) for identity verification. [149]
OMAN	For first time issuance: not enough information is available as to which data is collected to issue the ID card for citizens and foreign residents, however, the required documents offer a clue as to some	To activate the service, a phone number and an ID is needed.[152] It is unclear if any other data is collected for this purpose.

PRIVACY AND SECURITY

COUNTRY	DATA COLLECTED FOR ISSUANCE OF ID CARD	DATA COLLECTED FOR REGISTRATION IN THE DIGITAL ID SYSTEM
OMAN	*of the data collected. This includes passport data (copy of passport) or birth certificate and parents' ID and passport data, if the applicant does not have a passport.[150] Additional documents are required from foreign residents, but it is not exactly clear what type of data these documents contain. For example, foreign residents need to submit "original and copies of the Manpower form after medical examination" and "a letter from the employer" for government employees.[151]*	
QATAR	*For Qataris, they need to submit a form containing their full name, detailed home and work addresses, personal and work phone numbers, and job title.[153] They also need to submit two pictures, a copy of their passport in addition to the original document, proof of their blood type, copies of their parents' personal ID cards and approval of the guardian (when needed). For GCC nationals, they need to submit additional documents such as a copy of marital contracts (only for women) and a copy of personal ID card or family card. For residents, they need to submit data and documents to obtain the right of residence before they can get a personal ID card (Iqama). This usually depends on the*	*To access the National Authentication System (Tawtheeq),[155] which acts as a national identity provider for all online government services, a QiD data and a mobile phone number is collected.*

PRIVACY AND SECURITY

COUNTRY	DATA COLLECTED FOR ISSUANCE OF ID CARD	DATA COLLECTED FOR REGISTRATION IN THE DIGITAL ID SYSTEM
QATAR	purpose of residence, the most common of which is work. This is usually handled by the employer. [154]	
SAUDI ARABIA	Electronic identification by the applicant's parents, a statement of legacy disposition and the original deed of limitation of inheritance (if the father is deceased), school identification or a copy of the latest academic qualifications, birth certificate, a photo, applicant form, the family record and a copy of the mother's ID (if the parents are divorced). [156]	To sign in to the system, users need to first register with the Absher app (the ministry of interior online portal) by providing their ID number, mobile phone number, and email address,[157] or via the National Single Sign-On Initiative.[158]

PRIVACY AND SECURITY

COUNTRY	DATA COLLECTED FOR ISSUANCE OF ID CARD	DATA COLLECTED FOR REGISTRATION IN THE DIGITAL ID SYSTEM
UAE	*Data collected for issuance of Emirates ID: According to an official Emirates ID "renewal form" of an anonymized resident, we were able to gather that the following information is collected for ID renewals (likely, similar information is collected for ID issuance):* - *Mobile number* - *Name* - *Date of birth* - *Gender* - *Nationality* - *Unified number (which is different from the ID number)* - *Passport number* - *Passport expiry* - *Residency number* - *Residency expiry* - *IDN number (since it is a renewal form not a registration form)*	*Emirates ID number, mobile phone number and email address.[159] Face ID biometrics are also collected for verification purposes,[160] but this is optional. Users who do not want to use face verification can visit a nearby kiosk with their Emirates ID.*

TABLE 8: DATA COLLECTED BY GGC GOVERNMENTS TO ISSUE ID CARDS AND TO REGISTER CITIZENS AND RESIDENTS IN THEIR DIGITAL ID SYSTEMS.

PRIVACY AND SECURITY

Although some information is provided concerning the types of data collected for registration in the digital ID system, there is a lack of transparency about the types of data collected in the course of the use of these systems.

In addition to the data collected, further data is stored on the ID card's chip. Some of this data is sensitive such as digital certificates to enable authentication to the digital ID system and DNA data (in the case of Bahrain). In some cases, regulations contain vague language that fail to minimize the amount of data collected and stored on the card's chip. In Bahrain, Law No. (46) of 2006 regarding identity cards specifies (in Article 2) that the identity cards have a multi-purpose chip that stores personal information belonging to people including iris scan, fingerprints, blood type, DNA data and "any other information or data."[161] In other cases, there were no policies or regulations specifying the amount and types of data collected and stored on the chip (Qatar).

COUNTRY	DATA THAT APPEARS ON THE ID CARD	DATA STORED ON THE CARD'S CHIP
BAHRAIN	*Name, ID number, nationality, expiry date, place and date of birth, blood type, gender, signature, driving license type and date of first issue, eyesight and disability.* [162]	*Name in Arabic and English, personal Central Population Registry (CPR) number, date of birth, card expiry date, photo and signature images, contact details (email and phone numbers), address, occupation, employer data, sponsor data (for foreign residents), driving license data, passport data, residence data for foreign residents) and blood group,*`[163] *iris scan, fingerprints, blood type, DNA data and "any other information or data."*[164]

PRIVACY AND SECURITY

COUNTRY	DATA THAT APPEARS ON THE ID CARD	DATA STORED ON THE CARD'S CHIP
KUWAIT	Civil ID number, full name, date of birth, gender, nationality, expiry date, detailed address, phone number, blood type, and occupation and sponsor for foreign residents.[165]	According to Thales, the card's microprocessor "can host a large amount of data" and it "securely stores digital certificates, enabling the use of electronic authentication and digital signatures." It is unclear what other data is stored on it.[166]
OMAN	Name, Facial ID, ID number, date of birth, place of birth, signature, address, in addition to job and nationality for foreign residents, and driving license data on the back of the card. [167]	Marital status, level of education, passport number and the picture and fingerprint of the card holder.[168] According to Thales, "Oman's citizens and residents' credentials are securely stored on the cards, including name, address, digital color photo, and fingerprints."[169] It is unclear what other data is stored on the card's microchip.
QATAR	Biometric data (fingerprint, iris scan, facial recognition), ID number, photo, quaternary name (including the name of tribe or family), place and date of birth, nationality (if any), validity, permanent address (address of tribe and family), current place of residence and blood type. For foreign residents, the card further includes profession, name and address of the sponsor, and the residency permit number.[170]	According to Thales, "in addition to the personal data available in usual identity documents, the microprocessor also stores the person's fingerprint."[171] It is unclear what other information is stored on it.

PRIVACY AND SECURITY

COUNTRY	DATA THAT APPEARS ON THE ID CARD	DATA STORED ON THE CARD'S CHIP
SAUDI ARABIA	Personal details such as name, date and place of birth, photo,[172] in addition to nationality, job and employer for foriegn residents working in the kingdom.[173]	Personal and biometric data, including demographic background, photograph, fingerprints and Hajj records.[174]
UAE	ID number, name, nationality, date of birth, sex, date of validity, card number and signature. It includes additional information for UAE residents such as employer or family sponsor and job title details, and a field for "population group".[175]	Basic data, photo, biometrics and fingerprints.[176]

TABLE 9: TYPES OF DATA VISIBLE ON ID CARDS AND STORED ON THE CHIPS.

SECURITY AND USER RIGHTS

The level and sensitivity of the data collected under digital ID systems, as explained above, can entail serious risks to privacy, if the processing occurs without robust measures aimed at ensuring the security of the system, protection of the data, and the necessary individual rights for users of the digital ID program that would provide them with some level of control over their personal information.

Generally, Gulf countries implement a number of features and measures to secure data in the (digital) ID system. When it comes to the actual ID, Bahrain[177] and Qatar[178] are implementing a match-on-card technology, which allows the data to be securely stored on the card. Digital ID programs in the region largely rely on a national Public Key Infrastructure (PKI), a system of processes, policies, hardware, software and procedures needed to create, manage, distribute,

use, store and revoke digital IDs. PKI allows users to encrypt data, digitally sign documents, and authenticate themselves using certificates (which Digital IDs are based on).

PRIVACY AND SECURITY

Another key feature is secure and strong authentication. For example, Bahrain's eKey Single-Sign-On System (an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials (usually a username and a password), offers two levels of eKeys: Standard eKey, which requires only the personal ID number and a password to access a limited number of services, and the Advanced eKey, which "ensures the highest level of security and allows access to all eServices including highly confidential eServices requiring the verification of the user's smart card and biometrics (fingerprint)."[179]

According to the UAE Pass website, the Pass "relies on a national PKI that utilizes industry standard signing certificates. Secure storage of the keys is done through SE/TEE on the mobile and through cloud based HSM." [180] This means that the Pass uses safe and highly secure encryption keys within the device by using SE/TEE which will guarantee that the code and data on the phone are protected with respect to confidentiality and integrity, and when communicating through cloud by using HSM which is used to generate encryption keys on the cloud.

The institutional policies and measures in place to protect the privacy and data of card holders and the system's users (such as measures to limit and monitor access to the data or policies to handle data breaches) lack transparency. This is despite the fact that a number of countries have personal data protection laws that require data controllers to put in place such measures and policies.

For example, the Qatari Personal Data Protection Law requires data controllers to develop "internal systems for the effective management of Personal Data, and report any breach of measures aiming at the protection thereof," in addition to "conducting comprehensive audits and reviews on the compliance extent with Personal Data protection requirement," among other policies and measures. According to the Personal Data Protection Law in Bahrain (Article 8), "the Data Controller shall implement appropriate technical and organizational measures to guarantee protection of data against accidental or unauthorized destruction, accidental loss, as well as against alteration or disclosure of, access to and any other unauthorized forms of processing." It is unclear what organizational measures are specifically implemented in relation to the ID systems in both countries.

Additionally, users of digital ID systems in the Gulf have limited options to control their data. In Bahrain, under the Personal Data Protection Law, data subjects have some level of control over their data. This includes the right to object to processing of data that may result in material or moral damage (Article 21) and to decisions made based on automated processing (Article 22), and the right to "rectify, block or erase the personal data relating to him when the processing of such data is in breach of the provisions of this Law, in particular if the data is inaccurate, incomplete, outdated or if its processing is illegal." However, it is unclear to what extent these rights are guaranteed for users of the eKey Single-Sign-On System and what other options to control their data are available to them.

In Qatar, citizens and residents registered on the Hukoomi portal can access some of their data such as electricity and water bills, "details on the real estate owned by the user" and "details associated with the commercial registration and commercial license." It is unclear what other data is available for users to access and what other rights they have over the data. In addition, the Personal Data Protection Law requires controllers to use "appropriate technologies to enable individuals to exercise their rights to directly access, review and correct their respective Personal Data." It is unclear how this is implemented in the digital ID system.

In the UAE, users of the UAE Pass can only update their email addresses and mobile phone numbers.

PRIVACY AND SECURITY

In order to update "outdated" or "incorrect" information, they need to contact the Federal Authority for Identity and Citizenship and update their Emirates ID card.[181] It is unclear what other ownership and access rights are available to users and to what extent. Article 12 of the Federal Law No (9) of the Year 2006 stipulates that "each individual may obtain a symbolic copy of the personal data related thereto, or to the predecessors, successors or spouses thereof."[182] It is unclear what is meant by "symbolic data" and the level of data individuals can obtain.

CHAPTER 6

MARGINALIZED GROUPS AND THE RIGHT TO NONDISCRIMINATION

MARGINALIZED GROUPS AND THE RIGHT TO NONDISCRIMINATION

While digital ID can help ensure a higher proportion of IDs in a country, lack of internet penetration and access to technologies such as smartphones can pose real obstacles to inclusion of vulnerable groups (particularly populations with low technology literacy).

The Gulf region is considered to have some of the highest internet penetration rates in the Middle East and North Africa. By way of example, the penetration rate for the United Arab Emirates was 91 percent for 2018 and for Saudi Arabia 73 percent in the same year.[183] In comparison, Egypt had a penetration rate of 43 percent during the same time period. This likely means that digitizing ID systems in the Gulf countries is in line with the population's access to the internet and may not, in-and-of-itself, be a factor of discrimination.

More generally, however, ID systems can often lead to lack of inclusion and increased discrimination against certain vulnerable groups (such as women, children, refugees). Legal and policy frameworks pertaining to legal identification can be discriminatory through the requirements and procedures imposed to register, obtain, and use identification documents as well as through the collection of data that appears on identification documents and reinforces discrimination.

GENDER-BASED DISCRIMINATION

An analysis of provisions related to civil registration systems and, more particularly, birth registration in some Gulf countries highlights gender discrimination issues when it comes to women's right to register their children.[184]

For example, in Kuwait, under the Birth and Death Registration Law (No. 36/1969) art. 3), registering the birth of children is primarily the responsibility of their fathers. Similarly, in Oman, registering the birth of children is first the responsibility of fathers followed by a number of other individuals before finally falling on mothers. Saudi law prioritizes health facilities over fathers, and mothers can only register the birth of their children if both are unavailable. Under Bahraini, Qatari and Emirati law, preference is similarly given to the father for child registration and it is unclear whether mothers have the right to register their children. [185]

Other types of gender-based discrimination occurs when certain Gulf countries render ID mandatory for male children but not for females. For instance, both Saudi[186] and Omani ID [187] laws mandate a male child to obtain a personal identification document at a certain age while making the same identification optional for girls and based on approval of their guardians.

Such gender discrimination not only violates international norms prohibiting discrimination on the basis of gender but, more importantly, deprives children from the possibility of obtaining identification documents that often rely on information provided in birth certificates and, thus, denies them the right to access certain vital services that may only be available upon presenting such documents.

As mentioned above, digitization can reinforce existing discriminatory practices. This is the case for instance, in Saudi Arabia, where gender discrimination is widespread on different levels. Women in the country are subject to male guardianship to exercise some important rights, such as the right to travel. With the Absher application permitting e-government services, male guardians are able to exercise control over women even more than before. They can grant or deny permission for

MARGINALIZED GROUPS AND THE RIGHT TO NONDISCRIMINATION

women and children to travel abroad and obtain a passport under a subsection of the application called "dependent services." The Absher application portal also allows the male guardian to suspend a previously issued travel permission, and "displays a travel log function that allows male guardians to view all the trips in and out of Saudi Arabia that their female dependents make, showing destination countries and dates of travel." [188]

STATELESSNESS AND RESIDENCY REQUIREMENTS

Additionally, in their efforts to digitize identification systems and documentation, the Gulf countries mapped by our research show that vulnerable groups such as stateless persons and refugees are not part of the categories of persons eligible for enrolling in ID systems and obtaining identification documents. Although non-nationals can be part of the eligible groups for enrolling and obtaining identification documents, such eligibility relies on a residency permit, which excludes those who do not qualify as residents. Hence, benefits such as healthcare and financial services that are contingent upon having an ID cannot be accessed by those who do not fall under the resident or national categories.

Indeed, most of the Gulf countries have residency as a core requirement for identification:

In the UAE, Emirates IDs[189]are only issued to nationals and non-nationals who are residents. In Qatar, ID is obtainable for Qataris and Qatar residents.[190] The same is relevant for Kuwait, KSA, Oman and Bahrain. [191]

By zooming-in on the Kuwaiti example, one can note that a part of the population they call the bidoon[192] (i.e: the without or, in other words, those without a nationality) are completely marginalized from daily life by being deprived of legal documentation that identifies them. Indeed, by requiring a residency, Kuwait denies the bidoons civil identification that would allow them services such as renting real estate, opening a bank account, enrolling in private universities, holding legal employment, receiving birth certificates etc.

The residency requirement is also clearly apparent in the UAE through the close nexus between residency, labor, and ID.[193] In fact, male children born to foreign workers and residents who reach adulthood cannot stay in the country unless they obtain a residency permit, which is only possible through an employment or student visa. Therefore, by making the issuance of an Emirates ID contingent on being a UAE resident, which can only happen through employment, the UAE is indirectly imposing a barrier to entry for the most vulnerable: non-working populations.

THE NEGATIVE IMPACT OF BIOMETRICS ON PERSONS WITH DISABILITIES

Discrimination can also be prompted by the technology chosen by governments for their ID systems. When countries, such as the GCC countries, decide to rely on certain types of biometrics such as fingerprints or irises for the enrollment and use of ID systems, they indirectly discriminate against certain people. Indeed, manual laborers with worn fingerprints, the elderly, and persons with disabilities may have difficulty enrolling in or using ID systems that rely on fingerprints and a lack of an alternative option can lead to exclusion.

MARGINALIZED GROUPS AND THE RIGHT TO NONDISCRIMINATION

One way of providing an alternative is by carving out exceptions in the legal requirements and processes for digital ID, just as Bahrain did in its decision No. 16 of 2011 (amending the national ID law of 2006), where it exempted persons with disabilities from providing their biometrics to obtain a national ID card.[194]

CONCLUSION AND RECOMMENDATIONS

Our mapping of GCC countries' ID landscape reveals an increased effort on digitization in the field with reliance on various technologies, including the use of biometric for authentication. This is naturally aligned with the region's focus on digitizing the economy and leveraging ID as a core pillar of the digital transformation journey.

All GCC countries have implemented digital ID programs, with the first program implemented in Bahrain in 2007, and the latest ones implemented in Kuwait and Saudi Arabia in 2020. While all countries have put in place legislation addressing different aspects which enable a strong environment for Digital ID including data protection, electronic transactions and e-commerce, cybercrime and cybersecurity, these legal frameworks are falling short in many areas, most notably lack of robust and overarching laws for protecting data and users privacy as well as a lack of independent oversight for how personal data is being processed, which ultimately undermines trust in the ID system.

The wide-range of personal data collected by ID systems, including sensitive information, require strong security measures and policies to ensure its protection. While some Gulf countries adopt certain technical measures and features to secure data in the (digital) ID system, users have limited options to control their data and lack access to remedy in case their human rights are violated or impacted by the system. Finally, identification systems in the Gulf fail to take into consideration the needs of and impacts on marginalized populations, which can further exacerbate inequalities and discrmination against women, migrants, stateless people and those living with disabilities.

CONCLUSION AND RECOMMENDATIONS

RECOMMENDATIONS TO GCC GOVERNMENTS

- **Strengthen legal protection for digital ID.** Most notably by (i) adopting robust and overarching data protection laws (Kuwait, Oman and UAE), and (ii) for countries that have personal data protection-related legislation, reduce the scope of legal exemptions related to "national security" imperatives, that give room to unregulated processing of data conducted by government agencies and rampant government surveillance. Additionally, include legal provisions that provide for grievance redress mechanisms that enable users to file complaints or legal disputes when a digital ID system interferes with their human rights, particualry their rights to privacy and non-discrimination. When those complaints are not initially solved in favor of users, the latter should be able to appeal to an independent authority such as an independent judicial authority or oversight body.

- **Establish and enforce independent and strong oversight over the digital ID system.** Oversight can be conducted by a digital ID system oversight body or by separate authorities overseeing the data (such as a data protection authority) and the identification system. It should include oversight over the privacy and security of data and identification systems.

- **Adopt a privacy by design approach in the digital ID system.** This entails not only the adoption of the technical standards and features (such as encryption of data and strong multi-factor authentication), but also providing users with tools and platforms that give them control over their own data, such as options to limit collection and sharing of their data. Data collection and disclosure should also be minimized.

- **Eliminate all forms of discrmination in identification systems and ensure inclusion of marginalized groups.** This is key to ensure that inequalities and discmrination are not exacerbated by digital ID. GCC governments should particularly address gender discrimination, and discrimination against migrants, refugees, stateless people and those living with disabilities. Assessments, including public consultations involving these groups, should be done throughout the implementation of a digital ID system. Inclusion can also be achieved through amendments of existing ID-related legislation that indirectly discriminates against a certain group of people, in order to provide for exceptions that erase such discrimination (as done by Bahrain's recent amendments to the law on national ID cards).

REFERENCES

1 Sophie Smith, ''Digital Transformation in the GCC,'' The Euro-Gulf Information Centre, https://www.egic.info/digital-transformation-in-the-gcc.

2 ''E-Government Survey 2020. Digital Government in the Decade of Action for Sustainable Development,'' United Nations Department of Economic and Social Affairs, https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf.

3 "Digital Government," UN Department of Economic and Social Affairs, https://publicadministration.un.org/en/ict4d.

4 ''Practitioner's Guide. Glossary,'' The World Bank ID4D, https://id4d.worldbank.org/guide/glossary.

5 ''e-Governance,'' e-Estonia, https://e-estonia.com/solutions/e-governance/i-voting/.

6 ''Practitioner's Guide. Glossary,'' The World Bank ID4D, https://id4d.worldbank.org/guide/glossary#:~:text=Digital%20identification%20(ID)%20system,Public%2DPrivate%20Cooperation%20report.

7 Goal 16, United Nations, https://sdgs.un.org/goals/goal16.

8 "Principles on identification for sustainable development: toward the digital age," World Bank, ID4D, https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf.

9 ID4D, The World Bank, https://id4d.worldbank.org/.

10 ''Catalog of Technical Standards for Digital Identification Systems,'' The World Bank ID4D, https://id4d.worldbank.org/technical-standards.

11 "Principles on identification for sustainable development: toward the digital age," World Bank, ID4D, https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf.

12 ''Catalog of Technical Standards for Digital Identification Systems,'' World Bank, ID4D, https://id4d.worldbank.org/technical-standards.

13 '' Practitioner's Guide. Digital Certificates and PKI,'' World Bank, ID4D, https://id4d.worldbank.org/guide/digital-certificates-and-pki

14 ''Practitioner's Guide. Platforms for personal oversight,'' World Bank, ID4D, https://id4d.worldbank.org/guide/platforms-personal-oversight.

15 ''Practitioner's Guide. Tamper-proof logs,' World Bank, ID4D,' https://id4d.worldbank.org/guide/tamper-proof-logs.

16''Australia's digital ID system will soon get an oversight body,'' TOTT News, October 11, 2021, https://tottnews.com/2021/10/11/australia-digital-id-oversight-body/.

17 "Principles on identification for sustainable development: toward the digital age," World Bank, ID4D, https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf.

18 ''Practitioner's Guide. Platforms for personal oversight,'' World Bank, ID4D, https://id4d.worldbank.org/guide/platforms-personal-oversight

REFERENCES

19 ''Understanding the Lived Effects of Digital ID A Multi-Country Study,'' The Engine Room, January 2020, https://digitalid.theengineroom.org/assets/pdfs/200310_TER_Digital_ID_Report+Annexes_English_Interactive_Edit3.pdf.

20 "Principles on identification for sustainable development: toward the digital age," World Bank, ID4D, https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf.

21''PACI Kuwait Launches Kuwait Mobile ID App,'' KWT Today, April 14, 2020, https://kwttoday.com/paci-kuwait-launches-kuwait-mobile-id-app/.

22 'Saudi Arabia to officially launch unified services portal in 2020,'' Argaam, October 8, 2019, https://www.argaam.com/en/article/articledetail/id/1319570.

23 "What is the National Profile," Saudi National Portal for Government Services (SNPGS), https://www.my.gov.sa/wps/portal/snp/content/ssoinfo.

24 "Service Channels," SNPGS, https://www.my.gov.sa/wps/portal/snp/content/servicechannels.

25 "Frequently Asked Questions," (SNPGS) https://www.my.gov.sa/wps/portal/snp/content/help#header2_1

26 "National Portal," bahrain.bh, https://www.bahrain.bh/wps/portal/!ut/p/a0/hY7BCoJAFAB_ZS97fk8lsaNEGF6EIrK9yCYP3VbfurZKnx9S944DMzCgoAbFejWdDsaxHjZWaXOqMI3iLC6z5JpgXqWH8_6IUYE7uBBD-U-q4W6e3qscVOs40DtATZ1bJzcHPTTEEns3kkS_mNaKwbB9SdQPtwSxeTTzSBwk8u9LfEuYbHH7AHO7BRI!/#:~:text=The%20Portal%20has%20been%20launched,execute%20the%20comprehensive%20eGovernment%20programs.

27Lakshmi Kothaneth, "Activate TAM Card for Digital Sign," Oman Observer, March 29,2017 https://www.omanobserver.om/article/85056/Main/activate-tam-card-for-digital-sign.

28''e Government Strategy Summary 2007-2010,'' Kingdom of Bahrain. https://www.bahrain.bh/wps/wcm/connect/790f3079-7389-46b0-bb55-5d5ea5d2dccb/eGovernment+Strategy+2007-2010.pdf?MOD=AJPERES.

29 "Log In," bahrain.bh https://services.bahrain.bh/wps/portal/!ut/p/a1/04_Sj9CPykssy0xPLMnMz0vMAfGjzOItLNydDY0sjLwMfHyMDBwDHE0tAkMtjAz8jYEKIoEKnN0dPUzMfQwMDEyAwp4uTh4u5pa-Bgae5sTpN8ABHA0I6Q9OzdMP148CK8PnCrACPNYU5IZGVHimKwIA06s50w!!/dl5/d5/L2dBISEvZ0FBIS9nQSEh/.

30 "Electronic Identity," Omanuna, https://omanportal.gov.om/wps/portal/index/sso

31''National ID cards in Qatar : from ID to digital government,'' Thales, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/qatar-i.

32 ''Smart Dubai and TRA Launch National Digital Identity,'' October 17, 2018, https://www.smartdubai.ae/newsroom/news/2018/10/17/smart-dubai-and-tra-launch-national-digital-identity/.

33''The UAE Pass app,'' The United Arab Emirates's Government portal, https://u.ae/en/about-the-uae/digital-uae/the-uae-pass-app.

34 ''Thales Completes Acquisition of Gemalto to Become a Global Leader in Digital Identity and Security,'' Thales, https://www.thalesgroup.com/en/portugal/press_release/thales-completes-acquisition-gemalto-become-global-leader-digital-identity.

REFERENCES

35 "Gemalto Provides Kingdom of Bahrain with Additional One Million New-Generation e-ID Cards," Secure Technology Alliance, January 21, 2009, https://www.securetechalliance.org/gemalto-provides-kingdom-of-bahrain-with-additional-one-million-new-generation-e-id-cards/.

36 "Identity documents & Solutions," Thales, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity.

37 "National ID cards in Qatar : from ID to digital government," Thales, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/qatar-i.

38 "Government of Bahrain's Digital Transformation Journey," bahrain,bh, https://www.bahrain.bh/wps/portal/!ut/p/a1/pZLLbsIwEEV_JSyy-DJ7E5EF3KaK0iEcFpSXeICcYJyixQ2Kg_H0NqFIrlUJV78Y6d3zvjBFBc0QE3WWcqkwKmh9r4i0ex-DZTuD0AzzDEI69zqTdBbsHrgairwBg3D0C_rP_2na8AG7TgzPs2E8trR8OAcLgfjJ4eegA9PA1_RsiiCRClSpFEeNyV8pK0XzBhAk5FctMcKOknNUmxDStaCZqY5nxTDOGplklCiaUsZbbSrDDsVmZZEsUuSwAF9u-5QbMtVoe9a14Bdhqe57vOtRLwI4_zV844dXwUybOAa6M8AT8NqMzcNlHpI36F53oDtM_Ju_fsNdsvdmQUG9HCsXeFZr_fz36WZ7L-PQxo1DEOOClVGzFKlY1t5W-TpUq6zsTTNjv900uJc9ZM5GFCT9JUllrX99JVBazWRHgg9XvrkYji8RuvhuEjcYHtsAH6g!!/dl5/d5/L2dBISEvZ0FBIS9nQSEh/.

39 "Committees contributing to the development of ICT and digital transformation in the Kingdom of Bahrain," bahrain.bh, https://www.bahrain.bh/wps/portal/!ut/p/a0/hcrBCoJAEAD-Qr_E8systdpQIw4tQRNteZJFBNnVGaxI_X_qCjg8eBPAQOK6pj5qE4_hzcO2lQWdsYesiv-dYNu50PZ7RVHiAGzHU_5KHZ3otSyghdMJKm4KnXtZZ3hrHljjDL1u0JsNOpimpEn1gHqrHDivtAQk!/.

40 Information and eGovernment Authority, https://www.iga.gov.bh/en/.

41 Public Authority for Civil Information, https://www.paci.gov.kw/Home.aspx.

42 "Directorate General of Civil Status," Royal Oman Police, https://www.rop.gov.om/english/dg_cs.html.

43 "National ID Programme. A first in the Region, Digital Oman, http://digitaloman.com/indexbf54.html.

44 National Digital Certification Center, https://oman.om/tam/.

45 "ictQATAR to Enhance Consumer Protection," Ministry of Transport and Communications, https://www.motc.gov.qa/en/news-events/news/ictqatar-enhance-consumer-protection.

46 "National ID cards in Qatar : from ID to digital government," Thales, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/qatar-i.

47 "National Authentication System (Tawtheeq)," Hukoomi, https://hukoomi.gov.qa/en/digital-project/national-authentication-system-tawtheeq.

REFERENCES

48 "General Directorate of Information. Introduction," Qatari Ministry of Interior, Systemshttps://portal.moi.gov.qa-/wps/portal/MOIInternet/de-partmentcommittees/gainformationsystems/!ut/p/a1/tVJNU9swEP0tHHx0tLJjR-5NDQzOB7g0YcC-MLIjO2IsyZHUAPn1FSmcCqXMtDrt7jy9fft2UYVuUaXYXnTMCa1Y_5xX6d1lBhRnBSyKaXbmQ7pYF_m3aIUTDyg9YEbJOMeAFyQHAnS1nq-_FtMIAH_0_wZVqGqUG9wWlQ-N7EUdCuW4UdyFXAVgWbjhAzNOcuUaLaVwjvMAOq64YT3bSKGEdeaoWLdCtdrIY2KfrOPSBtDgjBB4bjQ0YoPKZFPzOk0mYRyTLBw340lYk7oNCWAec5y2BEe_hHnt8_x0BvEKFufLNPajLS-m0fQKgCQvgD_NfgTAO48CmqOq63V9NLqkqo5JhyrDW264Gf0wvrx1brBfAghg0MaxfiS1GHV6P9qxAB4G-1oP4KKYzV6MC-ANy-xbPbbaOnT7GzUq_Von7-4tx2j1STs_lJz8Y8Is-jTh_C9OXdzvdhX1B6u904_euf97sYO8liROv-eHJb8JWU0gTob9YUnpyclP8DzFNg!!/?1dmy&urile=wcm%3apath%3a%2Fwcmlib-internet-en%2Fsa-departmentcommittee%2Fgeneraladministrationofinformationsystems%2Fc17320

49 "General Directorate of Information. Accomplishments," Qatari Ministry of Interior, https://portal.moi.gov.qa/wps/-portal/MOIInternet/department-committees/gainformationsystems/!ut/p/a1/tVJNU9swFPwtHHx09PwV272pgcH5AJcmDFgXRrZlR4wlOZIaIL--IoVToZSZVie9N6vVvn2LCLpFRNI976nlStLhuSbTu8sccJCXsCxn-Zm74uWmLL6F6yBxgMoB5jiLiwCCZVZABni9WWy-IrMQIPjo_Q0iiDTSjnaLqodGDLz2ubRMS2Z9Jj0w1G_ZSLUVTNpGCcGtZcyDnkmm6UBbwSU3Vh8Vq47LTmlxLMyTsUwYD5owDJ-VIDI2vEVV0sR5HNDIr1me-nFHE7_u0tyP07gNUkjrJG9_CXPaF8XpHKI1LM9X08iNtrqYhbMrgCx5Afxp9iMA3jkY0AKRflD10egKyzrKekQ065hmevJDu_bW2tF88cCDUWlLh4lQfNKr_WRHPXgYzWvfg4tyPn8xzoM3LDNv_bFVxqLb36hR5daavru3IkDrT9r5AWH6jwnz8NOEi7-IOr_f7Qh2gVXO6Ufn3P9N7CiuRRZNvxeHFbvxaZ1BIlz7wwrjk5OfNcRXzg!!/?1dmy&urile=wcm%3apath%3a%2Fwcmlib-internet-en%2Fsa-departmentcommittee%2Fgeneraladministrationofinformationsystems%2Fc19880

50 "Innovating Beyond the Horizon to Build the Future of Digital Government," Digital Government Authority, https://dga.gov.sa/en/

51 Council Resolution No. (418) dated 25/7/1442 AH), Bureau of Experts at the Council of Ministers, https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/cb98b088-6d6f-41a7-8633-acfc00b6db02/1.

52 "Frequently Asked Questions," SNPGS, https://www.my.gov.sa/wps/portal/snp/content/help#header2_1

53 "Identity Authentication Management," iam.gov.sa, https://www.iam.gov.sa/authservice//userauthservice?lang=en.

54 "Agency Services: Ministerial Agency of Civil Affairs," my.gov.sa, https://www.my.gov.sa/wps/portal/snp/agencies/relatedservices/AC182.

55 "National Information Center," SNPGS, https://www.my.gov.sa/wps/portal/snp/agencies/agencyDetails/AC344.

56 "Legal References," TDRA, https://tdra.gov.ae/en/Pages/legal-references.

57 "About TDRA," tdra.gov.ae, https://tdra.gov.ae/en/About.

58 "Smart Dubai and TRA Launch National Digital Identity," October 17, 2018, https://www.smartdubai.ae/news-room/news/2018/10/17/smart-dubai-and-tra-launch-national-digital-identity/.

59 "UAE Pass User Guide," mohap.gov.ae, https://www.mohap.gov.ae/Documents/Banner/UAEPASS_User_Guide_1.0.pdf.

REFERENCES

60 “Leading the Digital Future of Abu Dhabi,” Abu Dhabi Digital Authority, https://www.adda.gov.ae/

61 “Smart Dubai and TRA Launch National Digital Identity,” Digital Dubai, 17 October, 2018, https://www.digitaldubai.ae/newsroom/news/2018/10/17/smart-dubai-and-tra-launch-national-digital-identity.

62 ‘’Mandatory National IDs and Biometric Databases,’’ Electronic Frontier Foundation, https://www.eff.org/issues/national-ids.

63 ‘’Exclusion and identity: life without ID,’’ Privacy International, December 14, 2018, https://privacyinternational.org/long-read/2544/exclusion-and-identity-life-without-id.

64 ‘’A smart national ID card for Saudi Arabia,’’ Thales, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/saudi-arabia.

65 Bahrain, Law No. 46 of 2006 concerning the identity card, Issued August 2, 2006 (Official Gazette No. 95, August 2, 2006) https://bahrain.bh/wps/wcm/connect/0a45826e-8aed-4537-9b4d-3df6b0746e92/%D9%82%D8%A7%D9%86%D9%88%D9%86+%D8%B1%D9%82%D9%85+%2846%29+%D9%84%D8%B3%D9%86%D8%A9+2006+%D8%A8%D8%B4%D8%A7%D9%94%D9%86+%D8%A8%D8%B7%D8%A7%D9%82%D8%A9+%D8%A7%D9%84%D9%87%D9%88%D9%8A%D8%A9.pdf?MOD=AJPERES.

66 “Identity Card Services,” Information and eGovernment Authority, https://www.iga.gov.bh/en/category/identity-card-services.

67 “How to Apply for a Civil ID in Kuwait,” Kuwait OFW, https://kuwaitofw.com/how-to-apply-civil-id/.

68 “Issuance of identity card (ID) for the first time,” Royal Oman Police, https://www.rop.gov.om/english/omani_id.html#:~:text=Every%20Omani%20citizen%20who%20is,on%20their%20legal%20guardian's%20consent.

69 Qatar, Decree Law No.5 of 1965 regarding Identity Cards, Issued on 20 September, 1965, (Official Gazette No. 4, January 1, 1965),https://www.almeezan.qa/LawView.aspx?opt&LawID=4001&language=ar.

70 “Issuing a National Identity Card,” SNPGS, https://www.my.gov.sa/wps/portal/snp/servicesDirectory/servicedetails/9511.

71 “Emirates ID,”The UAE Government Portal, https://u.ae/en/information-and-services/visa-and-emirates-id/emirates-id.

72 Law No. 46 of 2006 regarding the identity card, https://bahrain.bh/wps/wcm/connect/0a45826e-8aed-4537-9b4d-3df6b0746e92/قانون+رقم+%2846%29+لسنة+2006+بشأن+قاطبة+الهوية.pdf?MOD=AJPERES.

73 Resolution No. 16 of 2011 amending some provisions of Resolution No. (1) of 2007 regarding the executive regulations of Law No. 46 of 2006 on the identity card, https://www.bahrain.bh/wps/wcm/connect/2026d9e0-afc7-4964-b1e3-e7470438e4c4/%D9%82%D8%B1%D8%A7%D8%B1+%D8%B1%D9%82%D9%85+%2816%29+%D9%84%D8%B3%D9%86%D8%A9+2011+%D8%A8%D8%AA%D8%B9%D8%AF%D9%8A%D9%84+%D8%A8%D8%B9%D8%B6+%D8%A7%D9%94%D8%AD%D9%83%D8%A7%D9%85+%D8%A7%D9%84%D9%82%D8%B1%D8%A7%D8%B1+%D8%B1%D9%82%D9%85+%281%29+%D9%84%D8%B3%D9%86%D8%A9+2007+%D8%A8%D8%B4%D8%A7%D9%94%D9%86+%D8%A7%D9%84%D9%84%D8%A7%D9%8A%D9%94%D8%AD%D8%A9+%D8%A7%D9%84%D8%AA%D9%86%D9%81%D9%8A%D8%B0%D9%8A%D8%A9+%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86+%D8%A8%D8%B7%D8%A7%D9%82%D8%A9+%D8%A7%D9%84%D9%87%D9%88%D9%8A%D8%A9+%D8%B1%D9%82%D9%85+%2846%29+%D9%84%D8%B3%D9%86%D8%A9+2006.pdf?MOD=AJPERES

REFERENCES

74 Law No. 32 of 1982 regarding the civil information system, law.almohami.com, 29 April 2017, https://law.almohami.com/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%B1%D9%82%D9%85-32-%D9%84%D8%B3%D9%86%D8%A9-1982-%D9%81%D9%8A-%D8%B4%D8%A3%D9%86-%D9%86%D8%B8%D8%A7%D9%85-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA/?__cf_chl_managed_tk__=pmd_plNSjmNq_WNZBr0cjl30IfZVc13HtqjDGlwsGErLXyM-1634637362-0-gqNtZGzNBBCjcnBszQi9

75 PACI decision No.1 of 2012 dated 8 April 2012 regarding the civil ID card equipped with an electronic chip for Non-Kuwaitis, eastlaws.com, http://sub.eastlaws.com/GeneralSearch/Home/ArticlesTDetails?MasterID=1665318.

76 "Ministerial decision invoking the electronic civil ID card in all government and private transactions," 7 July 2020, PACI on Twitter, https://twitter.com/pacikwt/status/1280582036751777792

77 "Civil Status Law (amended)," Qanoon, https://qanoon.om/p/1999/l1999066/#_ftnref1

78 Decree Law No 5 of 1965 regarding personal ID cards, almeezan.qz, https://www.almeezan.qa/LawView.aspx?opt&LawID=4001&language=ar.

79 "National ID," Saudi Ministry of Interior, https://www.moi.gov.sa/wps/portal/!ut/p/z1/rZJNc4IwEIb_ih48OIkI5eOY6Vih1elUS5FcmABB0kpQJ0r77xscewTasTllZ959d5_dRRRtEJXsLLZMiVqynY5jaicQWJZvWObTMyYzIPbDwlt5YAQGoOgiuJ8T33IWAO5ifgcB8cOV94IxEIzob_Kh4xEYyn9DFNFMqr0qUVzVYpSLhskJtN-yrvgoq6XiUk2gjSZw5NvT7kJ30STySjoSeZLzgp12KuGyNd1nIkcx9IKObQArt9IUex5LTacoUp47GXOx7f4AdHdI-_nWutrjEKVeg3g_HCjRrC3Pp0Kb_4ONWtyeBpbmVdC35iHOWM_J6Szh60s4C96gUNbHSh_e-g8r8AfdzRvcB6yNG6z3VRhWLv6azqPpx8ptXotyWyXLWUPG428vUQmH/dz/d5/L2dBISEvZ0FBIS9nQSEh/.

80 UAE, Federal Law No. 9 on the Population Register and Identity Card, Issued on May 7, 2005 https://www.lexmena.com/law/en_fed~2006-05-07_00009_2020-05-30/.

81 The Executive Regulations of the Federal Law No. (9) of the Year 2015 on the Population Register and the ID Card, ica.gov.ae, Systemhttps://ica.gov.ae/wp-content/uploads/2020/09/The-Executive-Regulations-of-the-Federal-Decree-Law-No.-9-of-2006-regarding-the-Population-Register-System-and-the-Emirates-ID-Card.pdf.

82 Federal Decree-Law No. (2) of the Year 2004 on Establishment of the Federal Authority for Identity and Citizenship https://www.lexmena.com/law/en_fed~2004-09-29_00002_2020-05-30/

83 Decree-Law No. (54) of 2018 issuing the Law on Electronic Communications and Transactions, bahrain.bh, https://www.bahrain.bh/wps/wcm/connect/be6c6387-ae70-44ad-8755-1986fb2eedd2/%D9%85%D8%B1%D8%B3%D9%88%D9%85+%D8%A8%D9%82%D8%A7%D9%86%D9%88%D9%86+%D8%B1%D9%82%D9%85+54+%D9%84%D8%B3%D9%86%D8%A9+2018+%D8%A8%D8%A7%D9%95%D8%B5%D8%AF%D8%A7%D8%B1+%D9%82%D8%A7%D9%86%D9%88%D9%86+%D8%A7%D9%84%D8%AE%D8%B7%D8%A7%D8%A8%D8%A7%D8%AA+%D9%88%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%85%D9%84%D8%A7%D8%AA+%D8%A7%D9%84%D8%A7%D9%95%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9.pdf?MOD=AJPERES.

REFERENCES

84 Law No. 20 of 2014 on Electronic Transactions, Cyrilla, https://cyrilla.org/pt/entity/doplobfh504wtlwnilh-ht1emi?page=1.

85 Laurent Levac, "Kuwait: Law regarding Electronic Transactions in force - introduction of a concept akin to data privacy," December 11, 2015, https://www.globalcompliancenews.com/2015/12/11/kuwait-law-regarding-electronic-transactions-in-force-introduction-of-a-concept-akin-to-data-privacy/.

86 Omani Electronic Transactions Law, Cyrilla, https://cyrilla.org/en/document/sqzb6t2h6jgwa04rjgqup7gb9?page=1.

87 Qatar: Decree Law No.(16) of 2010 on the Promulgation of the Electronic Commerce and Transactions Law issued on August 19, 2010 https://www.motc.gov.qa/sites/default/files/documents/e-Commerce_Law_EN.pdf.

88 "Saudi Arabia E-Commerce Law of 2019," Clyde & Co, https://www.clydeco.com/clyde/media/fileslibrary/J470323_KSA_E-commerce_Law_Interactive_-_Update_0919_FV2.pdf.

89 Electronic Transactions law, Kingdom of Saudi Arabia, https://www.mcit.gov.sa/sites/default/-files/la_003_e_e-transactions_act.pdf.

90 "Federal Law No. (1) of 2006 Concerning Electronic Transactions & Commerce," https://ded.ae/DED_Files/-Files/%D8%A7%D9%84%D9%82%D9%88%D8%A7%D9%86%D9%8A%D9%86%20%D9%88%D8%A7%D9%84%D8%AA%D8%B4%D8%B1%D9%8A%D8%B9%D8%A7%D8%AA%20PDF/Federal%20Law%20No.%20(1)%20of%202006%20Concerning%20Electronic%20Transactions%20&%20Commerce.pdf

91 "Bahrain's Constitution of 2002 with Amendments through 2012," Constitute Project, April 18, 2026, http://extwprlegs1.fao.org/docs/pdf/bah117079.pdf.

92 "The Internet in the Mideast and North Africa: Free Expression and Censorship. Bahrain," Human Rights Watch, June 1999, https://www.hrw.org/legacy/advocacy/internet/mena/bahrain.htm.

93 Law No. (30) of 2018 with Respect to Personal Data Protection Law, https://bahrainbusinesslaws.com/laws/Personal-Data-Protection-Law.

94 "Freedom on the Net 2021. Bahrain," Freedom House, https://freedomhouse.org/country/bahrain/freedom-net/2021.

95 Kuwait Constitution, Refworld, https://www.refworld.org/docid/3ae6b4dab.html.

96 Royal Decree No. 6.2021 Issuing the Basic Law of the State, Qanoon, https://qanoon.om/p/2021/rd2021006/.

97 Riyadh Al-Balushi, "Privacy is Finally a Constitutional Right in Oman," riyadh.om, https://riyadh.om/2021/privacy-is-finally-a-constitutional-right-in-oman/.

98 Royal Decree No 12/2011 Issuing the Cyber Crime Law, https://www.qcert.org/sites/default/files/public/documents/om-ecrime-issuing_the_cyber_crime_law-eng-2011.pdf.

99 Gulf Center for Human Rights, "A new 'cyber defence' system in Oman raises human rights concerns," Global Voices Advox, September 18, 2020, https://advox.globalvoices.org/2020/09/18/a-new-cyber-defence-system-in-oman-raises-human-rights-concerns/.

100 The Permanent Constitution of the State of Qatar 0 / 2004, https://www.refworld.org/pdfid/542973e30.pdf.

REFERENCES

101 Law No.13 of 2016 Personal Data Privacy Protection, Compliance and Data Protection Department , https://compliance.qcert.org/en/library/privacy.

102 "Internet Filtering in Qatar," Open Net Initiative, 2009, https://opennet.net/sites/opennet.net/files/ONI_Qatar_2009.pdf.

103 "Saudi Arabia's Constitution of 1992 with Amendments through 2013," Constitute Project, August 26, 2021, https://www.constituteproject.org/constitution/Saudi_Arabia_2013.pdf?lang=en#:~:text=The%20State%20shall%20guarantee%20the,the%20confiscatee%20is%20fairly%20compensated.&text=Collective%20confiscation%20of%20properties%20shall%20be%20prohibited.

104 Basic Law of Governance, https://www.saudiembassy.net/basic-law-governance.

105 "Saudi Arabia issues Personal Data Protection Law," Clyde & Co, https://www.clydeco.com/en/insights/2021/09/saudi-arabia-issues-personal-data-protection-law.

106 "Freedom on the Net 2021. Saudi Arabia," Freedom on the Net, https://freedomhouse.org/country/saudi-arabia/freedom-net/2021.

107 Telecommunications Law, https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA%20_001_E_%20Telecom%20Act%20English.pdf.

108 Anti-cybercrime law, https://tahseen.ae/media/2656/ksa-anti-cybercrime-law-english.pdf.

109 "UAE - Data Protection Overview," Data Guidance, October 2021, https://www.dataguidance.com/notes/uae-data-protection-overview#:~:text=Article%2031%20of%20the%20Constitution,means%20of%20communication%20under%20law.

110 "Freedom on the Net Report 2021. United Arab Emirates," Freedom House, https://freedomhouse.org/country/united-arab-emirates/freedom-net/2021#footnote1_844a29h.

11 1 Federal Law No. 3 Issued on 8/12/1987 Corresponding to 17/4/1408 H. CONCERNING THE PENAL CODE: https://elaws.moj.gov.ae/UAE-MOJ_LC-En/00_PENALTIES%20AND%20CRIMINAL%20MEASURES/UAE-LC-En_1987-12-08_00003_Kait.html?val=EL1.

112 Federal Decree-Law no. (5) of 2012 Issued on 25 Ramadan 1433 AH Corresponding to 13 August 2012 AD ON COMBATING CYBERCRIMES: https://wipolex.wipo.int/en/text/316909.

113 "Oman third best prepared in world to thwart cyber attacks," ITU, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Oman-third-best-prepared-in-world-to-thwart-cyber-attacks.aspx.

114 Law No. 60 of 2014 regarding information technology: crimes.https://www.bahrain.bh/wps/wcm/connect/4555732a-0813-4944-8bdc-4adbb64b6d9a/%D9%82%D8%A7%D9%86%D9%88%D9%86+%D8%B1%D9%82%D9%85+%2860%29+%D9%84%D8%B3%D9%86%D8%A9+2014+%D8%A8%D8%B4%D8%A7%D9%94%D9%86+%D8%AC%D8%B1%D8%A7%D9%8A%D9%94%D9%85+%D8%AA%D9%82%D9%86%D9%8A%D8%A9+%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA.pdf?MOD=AJPERES.

REFERENCES

115 "The National Cybersecurity Strategy," bahrain.bh, https://bahrain.bh/wps/portal/!ut/p/a1/lZJdb4IwGIV_ixdc-Qt-2QHF3zDg348eic5PemBYQWLAgVt3-_apmyZbMj_WuzXPennNaxNEccSV2RSZ0USlRHvbcXzyOwcckIP2AziiEY78zaXcB98AzQPQTAEq7B4A9s9c28QO4TQ9k2MFPrtEPhwBhcD8ZvDx0AHr0mv4NccRjpWudoyjNql1dNVqUi1RZsFUECLZgs5UxPnB1XCQocsUyIUnCbCZxYruex2xJCLZdIwGLKZaJ5377OrPCq7mmqTp5u9LOEbgU_wSc9xEZo-ysEzNh-s_k_RuerHhfr3loiq-UTj80ml9s3kzMykoev1MUKkmDDPEmXaZN2jjbxhznWtebOwss2O_3jhR5IwrlyNyCvyR5tTFX_iZRvZrNVgH9tPvd5Whkc-mVu0HYan0BQoFE1g!!/dl5/d5/L2dBISEvZ0FBIS9nQSEh/.

116 Law No.63 of 2105 on combating cybercrime: https://www.moi.gov.kw/main/content/docs/cybercrime/ar/law-establishing-cyber-crime-dept.pdf.

117 "Kuwait Cybersecurity Policy," United Nations Institute for Disarmament Research Cyber Policy Portal, February 2021, https://unidir.org/cpp/en/state-pdf-export/eyJjb3VudHJ5X2dyb3VwX2lkIjoiNzEifQ (download link).

118 Royal Decree No 12/2011 Issuing the Cyber Crime Law: https://www.qcert.org/sites/default/files/public/documents/om-ecrime-issuing_the_cyber_crime_law-eng-2011.pdf.

119 "Oman third best prepared in world to thwart cyber attacks," ITU, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Oman-third-best-prepared-in-world-to-thwart-cyber-attacks.aspx.

120 Law No.14 of 2014 Issuing the Law on Combating Cyber Crime, https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/100242/120183/F1232109237/100242.pdf.

121 "Qatar National Cyber Security Strategy," Ministry of Transport and Communications, May 2014, https://www.motc.gov.qa/sites/default/files/national_cyber_security_strategy.pdf.

122 https://www.wipo.int/edocs/lexdocs/laws/en/sa/sa047en.pdf.

123 "National Strategy for Cyber Security," National Cybersecurity Authority, https://nca.gov.sa/pages/strategic.html.

124 Federal Decree-law No. (20) of 2018 ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AND FINANCING OF ILLEGAL ORGANISATIONS: https://www.mof.gov.ae/en/lawsAndPolitics/govLaws/Documents/EN%20Final%20AML%20Law-%20Reviewed%20MS%2021-11-2018.pdf.

125 "National Cybersecurity strategy 2019," United Arab Emirates' Government Portal, https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/national-cybersecurity-strategy-2019.

126 Law No.13 of 2016 Personal Data Privacy Protection: https://compliance.qcert.org/en/library/privacy

127 Law No. (30) of 2018 with Respect to Personal Data Protection Law: https://bahrainbusinesslaws.com/laws/Personal-Data-Protection-Law.

128 "Saudi Arabia Issues Personal Data Protection Law," Clyde & Co, September 26, 2021 ,https://www.clydeco.com/en/insights/2021/09/saudi-arabia-issues-personal-data-protection-law

129 "Directorate General of Civil Status," Royal Oman Police, https://www.rop.gov.om/english/dg_cs.html.

REFERENCES

130 "General Directorate of Information. Introduction," Qatari Ministry of Interior, Systemshttps://portal.moi.gov.qa-/wps/portal/MOIInternet/de-partmentcommittees/gainformationsystems/!ut/p/a1/tVJNU9swEP0tHHx0tLJjR-5NDQzOB7g0YcC-MLIjO2IsyZHUAPn1FSmcCqXMtDrt7jy9fft2UYVuUaXYXnTMCa1Y_5xX6d1lBhRnBSyKaXbmQ7pYF_m3aIUTDyg9YEbJOMeAFyQHAnS1nq-_FtMIAH_0_wZVqGqUG9wWlQ-N7EUdCuW4UdyFXAVgWbjhAzNOcuUaLaVwjvMAOq64YT3bSKGEdeaoWLdCtdrIY2KfrOPSBtDgjBB4bjQ0YoPKZFPzOk0mYRyTLBw340lYk7oNCWAec5y2BEe_hHnt8_x0BvEKFufLNPajLS-m0fQKgCQvgD_NfgTAO48CmqOq63V9NLqkqo5JhyrDW264Gf0wvrx1brBfAghg0MaxfiS1GHV6P9qxAB4G-1oP4KKYzV6MC-ANy-xbPbbaOnT7GzUq_Von7-4tx2j1STs_lJz8Y8Is-jTh_C9OXdzvdhX1B6u904_euf97sYO8liROv-eHJb8JWU0gTob9YUnpyclP8DzFNg!!/?1dmy&urile=wcm%3apath%3a%2Fwcmlib-internet-en%2Fsa-departmentcommittee%2Fgeneraladministrationofinformationsystems%2Fc17320.

131 "General Directorate of Information. Accomplishments," Qatari Ministry of Interior, https://portal.moi.gov.qa/wps/-portal/MOIInternet/department-committees/gainformationsystems/!ut/p/a1/tVJNU9swFPwtHHx09PwV272pgcH5AJcmDFgXRrZlR4wlOZIaIL--IoVToZSZVie9N6vVvn2LCLpFRNI976nlStLhuSbTu8sccJCXsCxn-Zm74uWmLL6F6yBxgMoB5jiLiwCCZVZABni9WWy-lrMQIPjo_Q0iiDTSjnaLqodGDLz2ubRMS2Z9Jj0w1G_ZSLUVTNpGCcGtZcyDnkmm6UBbwSU3Vh8Vq47LTmlxLMyTsUwYD5owDJ-VIDI2vEVV0sR5HNDIr1me-nFHE7_u0tyP07gNUkjrJG9_CXPaF8XpHKl1LM9X08iNtrqYhbMrgCx5Afxp9iMA3jkY0AKRflD10egKyzrKekQ065hmevJDu_bW2tF88cCDUWlLh4lQfNKr_WRHPXgYzWvfg4tyPn8xzoM3LDNv_bFVxqLb36hR5daavru3IkDrT9r5AWH6jwnz8NOEi7-lOr_f7Qh2gVXO6Ufn3P9N7CiuRRZNvxeHFbvxaZ1BlIz7wwrjk5OfNcRXzg!!/?1dmy&urile=wcm%3apath%3a%2Fwcmlib-internet-en%2Fsa-departmentcommittee%2Fgeneraladministrationofinformationsystems%2Fc19880

132 " Human Rights Department," Ministry of Interior, https://portal.moi.gov.qa/wps/portal/MOIInternet/department-committees/humanrights/!ut/p/a1/rZJNb9swDIZ_jY6O6I849m5ONsyO07lrMrT2ZZBsxhZgSZ6spkB_fdWgRQ_rxwpMJ4l49ZJ8SNrQG9oodhI9s0IrNj6-m_j3jxQyP62grDbpN3fNykOVXwb7auUEtRMUWRLlPvhlkkMC2f6wPayrTQDgf_T_mja0aZWd7EDru1aOgntCWTQKrccMgZl5HU7MWInKtlpKYS0igR4VGjayTgolZmvOFevjiL0LHo9MmJnAcCuZMqIf7PxiQoCxoI1if-kBBp0XQdx6PFhxjyNy3kGaYgqPdU2t6Gj9T-pzH67Vbf61gHAP5fddHDoSu4tNsPkJkCyfBO-hOgvgjZMB3dKmHzU_z6XOFA-TnjYGj2jQLG6NCw_WTvMXAgQmbSwbF1KLRa9Piz-MwN00P8cJXFRF8cSZwCuE59dyDHq29OYva1q7LVi9OeYopPtP4nzfsIz-t6H_acPth5u9ps1aC-W400n-kkkYX-X3O7z2GE8gXE6n--IBqQ0bfA!!/?1dmy&urile=wcm%3apath%3a%2Fwcmlib-internet-ar%2Fsa-departmentcommittee%2Fgeneraladministrationoflegalaffairs%2Fhumanrightsdepartment%2Fc25832

133 Law No. 20 of 2014 on Electronic Transactions: https://cyrilla.org/pt/entity/doplobfh504wtlwnilhht1emi?page=11

134 Qatar, Decree Law No 16 of 2010 Promulgating the Electronic Transactions and Commerce Law, Issued on August 9, 2010, (Official Gazette No. 9 September 28, 2010) https://almeezan.qa/LawView.aspx?opt&LawID=2678&language=en

REFERENCES

135 Law No. 30 of 2018 Issuing the Personal Data Protection Law, iga.gov.bh, https://www.iga.gov.bh/Media/Pdf-Section/Other-Legislations/30-2018.pdf

136 Decree No. (78) of 2019 Administrative Entity to Assume the Duties and Powers of Personal Data Protection Authority: http://www.pdp.gov.bh/en/royal-decree.html.

137 "Compliance and Data Protection Department," CDP, https://compliance.qcert.org/en.

138 "Practitioner's Guide. Grievance redress," The World Bank ID4D, https://id4d.worldbank.org/guide/grievance-redress.

139 "About National Platform GOV.SA," my.gov.sa, https://www.my.gov.sa/wps/portal/snp/aboutPortal/!ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfljo8zivQIsTAwdDQz9_d29TAwCnQ1DjUy9wgwMLEz1g1Pz9AuyHRUBI89e_A!!/.

140 "Electronic Complaint. Supreme Judicial Council," my.gov.sa, https://www.my.gov.sa/wps/portal/snp/servicesDirectory/servicedetails/14169/!ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfljo8zivQIsTAwdDQz9LQwNzQwCnS0tXPwMvYwN3A30g1Pz9L30o_ArAppiVOTr7JuuH1WQWJKhm5mXlq8fYWhiaGapX5DtHg4A6Oygxw!!/.

141 "Contact us," Oman.om, https://www.oman.om/wps/portal/index/cr/housing/reportingviolations/!ut/p/a1/hc_LDoIwEAXQr2HLDEUR3VWJD1QqPqEbg6ZWEqAGUPx80bjR-JjdnZybzACHAHgWXWIZlbHKouSeubVlvmEZQ4Zj5q0MpENc-qzbJ4w1axDWAL8MxX_9hchgA_wXs-fGE5g4QGTt0bRH500kLvG6fssjuMJ3MF5OKRJz3XfbE8t0nMYT_DjUBS4TtXs8HdJsZ9oSeC4OIhe5fs7r9bEsT0VHQw2rqtKlUjIR-l6lGn6qHFVRQvAq4ZQG11E8Szd2QW99TWRo/dl5/d5/L0lKQSEvUUt3SS80RUkhL2Vu/.

142 "Support," UAE Pass, https://selfcare.uaepass.ae/support.

143 "Electronic Complaint System" Government of Dubai, https://www.gdrfad.gov.ae/en/i-need/electronic-complaint-system.

144 Resolution No. (1) of 2007 on the executive regulations of Law No. 46 of 2006 regarding the identity card relates

145 Bahrain, Law No. 46 of 2006 concerning the identity card, Issued August 2, 2006 (Official Gazette No. 95, August 2, 2006) https://bahrain.bh/wps/wcm/connect/0a45826e-8aed-4537-9b4d-3df6b0746e92/%D9%82%D8%A7%D9%86%D9%88%D9%86+%D8%B1%D9%82%D9%85+%2846%29+%D9%84%D8%B3%D9%86%D8%A9+2006+%D8%A8%D8%B4%D8%A7%D9%94%D9%86+%D8%A8%D8%B7%D8%A7%D9%82%D8%A9+%D8%A7%D9%84%D9%87%D9%88%D9%8A%D8%A9.pdf?MOD=AJPERES.

146 "First Time Registration of Individuals," Kuwait Government Online, https://www.e.gov.kw/sites/kgoenglish/Pages/-Services/PACI/KuRegistrationForTheFirstTime.aspx.

147 "First Time Registration of Expatriates," Kuwait Government Online, https://www.e.gov.kw/sites/kgoenglish/Pages/Services/PACI/RegistrationOfNKForTtheFirstTime.aspx.

REFERENCES

148 “Registration of Gulf Cooperation Council Citizens,” Kuwait Government Online, https://www.e.gov.kw/sites/kgoenglish/Pages/Services/PACI/RegistrationCitizensOfTtheGulfForTheFirst.aspx.

149 “How to Install Kuwait Mobile ID App, and How to Enroll Your Mobile ID in the App,” Public Authority for Civil Information,https://hawyti.paci.gov.kw/English/Install.aspx.

150 “Issuance of Identity Card (ID) for the first time,” Royal Oman Police, https://www.rop.gov.om/english/omani_id.html.

151 “First Time Issuance of Residence Card,” Royal Oman Police, https://www.rop.gov.om/english/resident_id.html.

152 “Mobile PKI,” National Digital Certification Center, https://oman.om/tam/.

153 Passport or ID Application, The State of Qatar, https://portal.moi.gov.qa/wps/wcm/connect/0d846899-a95c-4a48-b0b8-edc1331a8fac/Passport+or+ID+Card+Application.pdf?MOD=AJPERES.

154 ‘‘Residence Work and Permits,’’ Hukoomi, https://hukoomi.gov.qa/en/article/residence-and-work-permits.

155 ‘‘National Authentication System,’’ Hukoomi, https://hukoomi.gov.qa/en/digital-project/national-authentication-system-tawtheeq.

156 “Issuing a National Identity Card,” SNPGS, https://www.my.gov.sa/wps/portal/snp/servicesDirectory/servicedetails/9511/.

157 ‘‘Registration procedure. User data,’’ Absher, https://www.absher.sa/wps/portal/individuals/static/register/!ut/p/z1/04_iUlDg4tKPAFJABjKBwtGPykssy0xPLMnMz0vM0Y_Qj4wyizd1DnD2tPA1NnQPCDU3MHIzN_FyNvN2D7Mw0ffSj8KvIDixSL8gO1ARAGHlE-o.

158 “National Portal,” SPNGS, https://www.my.gov.sa/wps/portal/snp/content/NationalProfile.

159 “FAQ,” UAE Pass, https://selfcare.uaepass.ae/faq.

160 UAE Pass: https://selfcare.uaepass.ae./

161

162 ‘‘Civil Registers in the Kingdom of Bahrain,’’ Presentation by the General Directorate of Statistics, Identity and the Population Register, Available on unstats.un.org, 2018, https://unstats.un.org/unsd/demographic-social/meetings/2018/crvs-ws-tunis/docs/Session05-Bahrain.pptx (Note: download link).

163 Ibid

164 Bahrain, Law No. 46 of 2006 concerning the identity card, Issued August 2, 2006 (Official Gazette No. 95, August 2, 2006) https://bahrain.bh/wps/wcm/connect/0a45826e-8aed-4537-9b4d-3df6b0746e92/%D9%82%D8%A7%D9%86%D9%88%D9%86+%D8%B1%D9%82%D9%85+%2846%29+%D9%84%D8%B3%D9%86%D8%A9+2006+%D8%A8%D8%B4%D8%A7%D9%94%D9%86+%D8%A8%D8%B7%D8%A7%D9%82%D8%A9+%D8%A7%D9%84%D9%87%D9%88%D9%8A%D8%A9.pdf?MOD=AJPERES

165 “Residence Permit Stickers Replaced with Civil Identification Cards for Entry and Exit” Fragomen, April 1, 2019, https://www.fragomen.com/insights/residence-permit-stickers-replaced-with-civil-identification-cards-for-entry-and-exit.html.

REFERENCES

166 "Civil ID in Kuwait: the Key to Digital Government," Thales, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/kuwait.

167 Oman Observer, "ROP Launches New Version of ID and Resident Cards," Twitter, November 20, 2016, https://twitter.com/OmanObserver/status/800176914958864384/photo/1.

168 "National ID Programme A First in the Region," Digital Oman, http://digitaloman.com/indexbf54.html

169 "Oman National ID Card," Thales Groups, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/oman

170 Qatar, Law No. 37 of 2005 Amending Certain Provisions of Decree-Law No. 5 of 1965 on Identity Cards, Issued on September 28, 2005, (Official Gazette No.1, February 16, 2006) https://www.almeezan.qa/LawView.aspx?opt&LawID=2590&language=en.

171 "National ID cards in Qatar : from ID to digital government," Thales, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/qatar-id

172 "Saudi Arabian identity card," Wikipedia, https://en.wikipedia.org/wiki/Saudi_Arabian_identity_card.

173 Arab News, "Saudi Arabia: Free Three-Month Extension Of Resident ID Cards For Expats," Eurasia Review, https://www.eurasiareview.com/04042020-saudi-arabia-free-three-month-extension-of-resident-id-cards-for-expats/.

174 Jumana Khamis, "Electronic ID Key to Saudi Arabia's Digital Transformation, Arab News, https://www.arabnews.com/node/1765151/saudi-arabia.

175 "ICA Launches Emirates ID Card New Generation," ICA, https://ica.gov.ae/en/media-center/ica-launches-emirates-id-card-new-generation/.

176 "All you need to know about Emirates ID (2021 guide)," Edarabia, https://www.edarabia.com/all-you-need-know-emirates-id/

177 "New national ID card for Kingdom of Bahrain," Thales, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/bahrain

178 "National ID cards in Qatar : from ID to digital government," Thales, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/qatar-id

179 "About eKey," eKey Bahrain, https://www.ekey.bh/bnaf-usermgmt/pages/C-mFI8n72L_6J8-2KlZHag/C-m02.

180 "FAQs," UAE Pass, https://selfcare.uaepass.ae/faq.

181 "FAQs" UAE Pass, https://selfcare.uaepass.ae/faq.

182 UAE, Federal Law No. 9 on the Population Register and Identity Card, Issued on May 7, 2005 https://www.lexmena.com/law/en_fed~2006-05-07_00009_2020-05-30/.

183 "Internet usage in MENA - statistics & facts," Statista Research Department, December 17, 2020, https://www.statista.com/topics/5550/internet-usage-in-mena/.

184 Betsy L. Fisher, "Gender Discrimination and Statelessness in the Gulf Cooperation Council States," Michigan Journal of Gender * Law, Volume 23 (Issue 2), https://docs.google.com/document/d/1qjlqSTApc2iY7zTdNd9M7PbnW2Uhn9kdW6kQgYh7rFM/edit#

REFERENCES

185 Ibid.

186 Hala Aldosari. ''Family Identification Documents for Saudi Women: An Identity Dilemma,'' The Arab Gulf States Institute in Washington, March 2, 2016, https://agsiw.org/family-identification-documents-for-saudi-women-an-identity-dilemma/.

187 ''Issuance of identity card (ID) for the first time,'' Royal Oman Police, https://www.rop.gov.om/english/omani_id.html#:~:text=Every-%20Omani%20citizen%20who%20is,on%20their%20legal%20guardian%27s%20consent.

188 ''Saudi Arabia's Absher App: Controlling Women's Travel While Offering Government Services,'' Human Rights Watch, May 6, 2019, https://www.hrw.org/news/2019/05/06/saudi-arabias-absh-er-app-controlling-womens-travel-while-offering-government.

189 ''Emirates ID,'' The United Arab Emirates' Government portal, https://u.ae/en/information-and-services/visa-and-emirates-id/emirates-id.

190 Decree-Law No.5 of 1965 regarding Personal ID Cards: https://www.almeezan.qa/LawView.aspx?opt&LawID=4001&language=ar

191 Khaled A. Abdulkarim, "Crystallizing a Discourse of "Khalijiness": Exclusion and Citizenship in the Arab Gulf States" 15 May 2017. CUREJ: College Undergraduate Research Electronic Journal, University of Pennsylvania, https://repository.upenn.edu/curej/211.

192 Ibid.

193 Ibid.

194 Decision No.16 of 2011 amending some provisions of Decisions No.1 of 2007 regarding the executive regulations of Law No. 46 of 2006 on the identity card: https://www.iga.gov.bh/Media/Pdf-Section/Digital/16-2011.pdf.