2019

Using Adaptive Enterprise Architecture Framework for Defining the Adaptable Identity Ecosystem Architecture

Memoona J. Anwar
University of Technology Sydney, memoona.j.anwar@student.uts.edu.au

Asif Q. Gill
University of Technology Sydney, asif.gill@uts.edu.au

Ghassan Beydoun
University of Technology Sydney, Ghassan.Beydoun@uts.edu.au

Using Adaptive Enterprise Architecture Framework for Defining the Adaptable Identity Ecosystem Architecture

Full paper

Memoona J. Anwar
School of Software
The University of Technology Sydney
Sydney, Australia
Email: memoona.j.anwar@student.uts.edu.au

Asif Q. Gill
School of Software
The University of Technology Sydney
Sydney, Australia
Email: asif.gill@uts.edu.au

Ghassan Beydoun
School of Software
The University of Technology Sydney
Sydney, Australia
Email: ghassan.beydoun@uts.edu.au

Abstract

Digital identity management is often used to handle fraud detection and hence reduce identity thefts. However, using digital identity management presents additional challenges in terms of privacy of the identity owner meanwhile managing the security of the verification. In this paper, drawing on adaptive enterprise architecture (EA) with an ecosystem approach to digital identity, we describe an identity ecosystem (IdE) architecture to handle identity management (IdM) while safeguarding security and privacy. This study is a part of the larger action design research project with our industry partner DZ. We have used adaptive EA as a theoretical lens to define a privacy aware adaptive IdM with a view to improve the Id operations and delivery of services in the public and private sector. The value of the anticipated architecture is in its generic yet comprehensive structure, component orientation and layered approach which aim to enable the contemporary IdM.

Keywords: Identity Ecosystem, Identity Ecosystem Architecture, Identity Management Frameworks, Digital Identity

1 INTRODUCTION

Identity Management Architecture is cogently described by Windley (Windley 2005, p. 134) as *"...a coherent set of standards, policies, certifications and management activities, aimed at providing a context for implementing a digital identity infrastructure that meets the current goals and objectives of the business"*. In simple words, identity (ID) is a data-intensive key that allows to support the authentication stages in an evolving digital ecosystem (DE). Validating the ID of the data subject is a critical job. Current identification methods which are either document-based (ID card, Passport etc.) or knowledge-based (a PIN, A password), both of which can be forgotten, lost, inappropriately shared or stolen resulting in ID theft or abuse. A third identification method is based on physical attributes i.e. biometrics, which is considered as more reliable then document-based and knowledge-based methods. IdM is not a novel approach. For decades, manual collection of private information has been used for multiple purposes e.g. to carry out research on customer behaviours and/or to boost marketing operations (D-Cent 2013). However, with a growing need for higher border control security and the pervasiveness of digital communications (Breebaart et al. 2008), a more consistent and interoperable ID system is needed. All types of ID are based on personal sensitive information and hence carry an inherent risk of misuse. Indeed, electronic forms of ID (or "dematerialized ID") carry even a higher risk. They have a broader scope and produce huge data about individuals, their online patterns, financial position, acquaintances, and hypothetically political and religious opinions (Dixon 2019). They are markedly more sensitive and vulnerable to identity theft. Victims of ID theft can be severely affected. ID fraud's adverse effects are not limited to money only. There are other major impacts such as an emotional toll. Other impacts are harder to assess (Equifax 2015). Imagine an ID thief using your name leading to law enforcement department arresting you. This would be an extremely traumatic incident with long term cost. It affects your profile and history of background checks. This can impact employment prospects and credit worthiness (Johansen 2019). Hence, there is a clear need towards a secure, privacy aware and reliable IdM system. This need led to an increased interest in a privacy aware adaptive Identity Ecosystem (IdE) architecture.

This paper is a part of an action design research (ADR) (Sein et al. 2011; Gill and Chew 2019) which is focused on developing and evaluating an IdE framework for our industry partner DZ (coded name) based on the adaptive Enterprise Architecture (EA) (Gill 2014;2015). This will be an overarching framework consisting of the important layers of a digital ecosystem (DE): Human, Technology, Facility, Environment, Interaction and Privacy. The framework can produce an IdM system that will jointly enable privacy, data, and an ID which is, impartial, and able to recognize the challenges of extremely complicated information environments where digital ID currently functions. The scope of this paper is limited to the critical step of development of an adaptive IdE architecture. The architecture components covered here are by no means exhaustive but will provide architects with a solid foundation for components they must consider before getting started.

2 BACKGROUND

There are many examples of local and national-level ID ecosystems that failed because end-users doubted their privacy and security protocols (Dixon 2019), particularly in ID domain provided by state or government. An example is the disbanded UK National ID Card System. After 8 years of planning, this was abundantly discarded soon after its inauguration, at a substantial cost. Another example is the case of India's Aadhaar, which, despite presenting a most important illustration on the execution of a huge biometric based IdE, teaches vital lessons. World Privacy Forum (WPF) studied the Aadhaar ecosystem broadly including its design and implementation details and drafted a comprehensive report on it (Dixon 2017). One prominent issue the system faced was substantial mission creep that gradually affected end-user's confidence in the system. The Australian government is trying to build two identity schemes, Govpass and Digital ID. Both schemes are not administrated by committed regulations, apart from current legislations for example the insufficient Privacy Act 1988, making Australians susceptible to ID theft (Hanson 2018).

The past 25 years have provided ample lessons around information security and digital IdE vulnerabilities. There are noteworthy analogies in information security regulations endorsed in 89 countries, even when characteristics of the regulation have been modified according to individual country's context (Anwar et al. 2018). Nevertheless, a reference IdE architecture is not normally acknowledged in some environmental and legal contexts. An IdE should be designed very carefully in order to create impactful business understandings that expand service value and viability. Further effort is required towards modelling a privacy aware end-to-end IdE. The challenge is rooted in the absence of a generic and adaptive IdE reference architecture that can help in designing and constructing an IdM

systems using existing solutions and staying adaptive to expected future ones. This paper is a step towards the definition of the complete reference architecture for adaptive IdE with privacy focus. It extends our previous study on evaluation of modelling approaches for digital ecosystem architecture (Anwar and Gill 2019).

IdE architecture is helpful in getting a perception of the way different components of IdE relate to each other. A conceptual model can lead to IdE development that can avoid numerous pitfalls of bad implementations that lead to unreliable and insecure systems as well as lack of interoperability (Anwar and Gill 2019). The existence of an IdE architecture is significant for academia as well as industry, since it provides with a starting point on what to base further research and implementation plans. Extensive investigation has already led to several technical aspects of IdM, but little research has been carried out into how a privacy aware IdM system is designed for a changing organisational environment. Not enough research articles on the description of the end-to-end design of adaptive IdE architecture or its components, were found. For this research we have studied articles on similar architectures, blogs, standards, and tried and tested industry practices that are mentioned and cited as needed. The contemporary industry has several enterprise architecture frameworks that may provide required architecture and components. A lot of research has already been carried out on different aspects of IdM architectures (Jin et al. 2010, Dabrowski and Pacyna 2008 ; Chigani 2007 ; Bussard 2008 ; Kerberos 2005 ; Agarwal et al. 2003 ; Mishra 2005 ; Ray and Schultz 2007; Bauer 2004; Bourass et al. 2014) , but less evidence is found on how an end-to-end IdM solution is designed to be adaptable and privacy aware. None of the architecture focuses on privacy. The models are either attribute centric (Jin et al. 2010), network centric (Dabrowski and Pacyna 2008; Chigani 2007), service centric (Bussard 2008; Kerberos 2005; Agarwal et al. 2003) or user centric (Mishra 2005; Ray and Schultz 2007; Bauer 2004). Some also discuss security (Bourass et al. 2014) but that is with reference to federated digital identities and are not applicable to a generic organisational context e.g. decentralised digital identity. The existing architectures can be used as reference architecture, if they cover every architectural aspect to build a secure IdE. In the search of adaptive IdE reference architecture, enterprise architecture frameworks could be the baseline for the proposed framework development. The definition of IdE used in this study is based on adaptive EA due to its higher relevance with the layers of a digital ecosystem (DE). Adaptive EA discusses the "elements (concepts or properties) of integrated adaptive human (BIPS: business, information, professional, social), technology (ADPI: application, data, platform, infrastructure) and facility (SEHA: spatial, energy, HVAC, ancillary) system or ecosystem (value network of systems) in its secure environment (PESTLE: political, economic, sociological, technological, legal, and environment), relationships (type, strength), and the principles (adaptive design) and evolution "(based on Gill 2014;2015). The layers and components provided by an adaptive EA can be analysed, compared, measured and validated to build the secure architecture required for end-to-end adaptive IdE.

This paper is structured as follows. Sec. 3 outlines the research questions for this study. Sec. 4 highlights the methodology and kernel theories used to develop adaptive IdE architecture. Sec. 5 exposes our reference architecture. Sec. 6 discuss the proposed architecture and its implications. Sec. 7 and 8 present our conclusions and perspectives for future work.

3 RESEARCH QUESTION

DZ (our industry partner) intends to develop an IdE which is adaptable to change and is privacy focussed. DZ wants to offer a strong identity verification solution that can give end users confidence about privacy of their identity. DZ needs a robust IdE that is adaptable and highly secure to mitigate chances of security breaches, ensure data privacy and manage risk. However, the problem is there no such architecture that could help in designing a secure and successful digitisation of end user's identity while adhering to applicable laws and ever-changing companies' vision. To enable a common glossary and to sketch architectural facets for implementation of an effective IdM system, a reference architecture for an adaptive IdE is discussed in this paper. It is intended to be technology independent i.e. it should offer a general scheme for development of secure IdE and preferably covers all key aspects of it. While developing an architecture for frictionless, reusable identity only generic components are added, as one organisation relying on the identity verifications of another organisation may be operating in a completely different risk environment. Privacy and security constraints that restrict the sharing of additional information, such as document identifiers, may also reduce the ability of relying parties to deduce the strength of the original verification (Australian Government 2017). Agreeing on common standards for identity verification checks can mitigate many of these problems and provide significant benefits to both customers and business. Thus, for individual organisational context single architecture component might not be included into this reference architecture or might be surplus. Therefore, the

main research question of this research is: **RQ: How to design an adaptive IdE reference architecture for effectively ensuring privacy and security?**

4 METHODOLOGY

This research is part of an overarching action design research (ADR) (Sein et al. 2011) aimed to develop a model for an end-to-end IdE by using a hybrid modelling approach. ADR is a four-step process: problem definition (PD), Building, Intervention & Evaluation (BIE), Reflection and Learning (RL) and Formalisation of Learning (FL). In this study, we adopt combination of ADR method as described by Sien et al. (2011) and Gill and Chew (2019). ADR allows looping back and forth between BIE and RL (Gill and Chew 2019). Hence, as an initial contribution, this paper proposes an IdE architecture that will provide a basis for further research and development of IdM systems for privacy and security. The proposed IdE architecture is based on DZ vision for IdE, adaptive EA (Gill 2014;2015) kernel theory and industry best practices (see Figure 1). DZ wants to develop an adaptive IdE architecture for developing a secure, efficient, user friendly and reusable IdM system that offers trust, privacy & security, consent, and innovation. Adaptive EA (Gill 2014;2015) provides guidelines that can be used to build the security architecture required for Identity Ecosystem. Adaptive EA can help in implementing the IdM system that can enhance privacy, adjust to individual organisation context and improve the quality of service. Along with adaptive EA, we examined IdE architectures of different IdM systems (ShoCard 2017; Civic 2017; Sovrin 2018; Jumio 2017) to analyse and select industry best practices towards IdE architecture development. These IdM systems were selected because at the time of the study, they were the most cutting-edge and innovative in architecture and/or implementation.

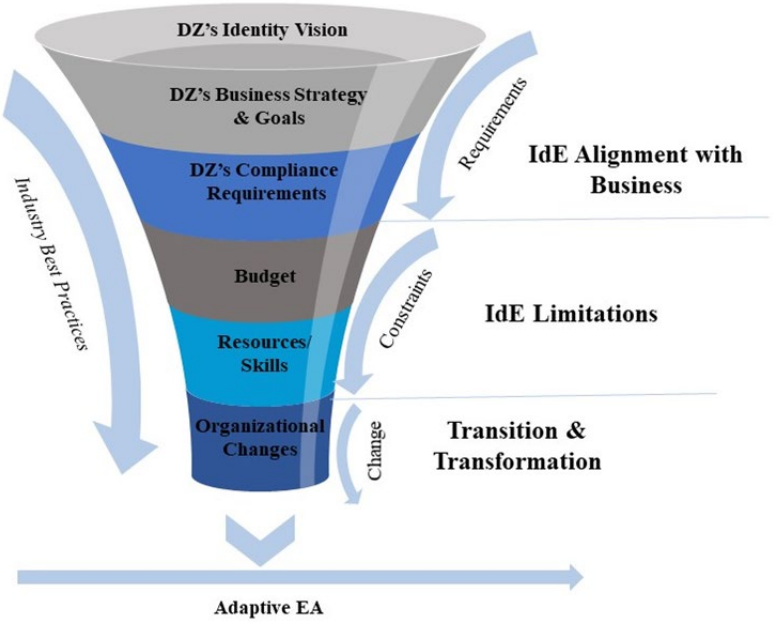

Figure 1: IdE Architecture Drivers (based on DZ vision, adaptive EA and industry best practices)

5 IDENTITY ECOSYSTEM (IDE) ARCHITECTURE

An IdE can be developed and maintained by governments, banks, employers, universities, by persons, and groupings of them, thereof for various objectives. The technologies upon which IdM systems are based, are copious ranging from huge data centres to blockchain to biometrics and more. A well-known example of ID is that of a state-issued ID, characteristically used for many tasks specifically identification. Whilst conventional IdM systems are not vanishing, they are constantly altered. Several IdE have now developed, with more still developing, each engaging unique digital designs and usages. These systems normally intersect and may differ in scope ranging from international to micro-identity systems. Although IdM systems have changed enormously, risks related to conventional and recent purposes of ID will still exist and will diverge based upon any individual technological or organisational context. This is where adaptive EA can iteratively address new data-related problems as they relate to

Col: Requires Row: Used by	Human	Technology	Facility	Environment
Human	Many-to-Many	Many-to-Many	Many-to-Many	Many-to-Many
Technology	Many-to-Many	Many-to-Many	Many-to-Many	Many-to-Many
Facility	Many-to-Many	Many-to-Many	Many-to-Many	Many-to-Many
Environment	Many-to-Many	Many-to-Many	Many-to-Many	Many-to-Many

Table 1. Identity Ecosystem Interactions based on (Gill 2014; 2015)

the creation and use of identity. Hence, the IdE is a human-centric (HUMAN) connected environment (ENVIRONMENT) – a collection of organisational policies, technologies (TECHNOLOGY), processes and approved standards that securely (PRIVACY & SECURITY) enable communications(INTERACTION) ranging from unidentified to fully-authenticated and from lesser to higher worth based upon data stored in secure data centre (FACILITY) (Gill 2014) (The White House 2011). As per this definition, an identity ecosystem consists of four layers (human, technology, facility, environment) and their secure interactions.

The IdE architecture can be developed on the component level e.g. a solution architecture refers to the design of solutions with regards to security, as well as the roles and responsibilities within a business relating to identity and security. Business architecture involves the setup and design of duties, access, and authorisations across business applications. Information architecture dealing with information exposure and security with access management, usage, storage, retrieval, and more. It also involves analysing and interpreting insights to understand the impact of information on a company. Infrastructure architecture involves networks, storage, and computing for platforms such as directory services. However, DZ needs to discern a generalised IdE architecture to realise their goals, aligning with corporate strategy to ensure that the company gets the most out of their IdE. In this study, we adopt an ecosystem approach for architecture development that covers all the layers and components of an IdE. Hence, we critically analysed the requirements of DZ along with reviewing different IdM systems (ShoCard 2017; Civic 2017; Sovrin 2018; Jumio 2017) and proposed an adaptive IdE architecture which is secure and privacy focused. This research is expected to demonstrate that the designs and applications studied, use some generic components that collectively can establish an adaptive IdE architecture. Each layer taken from adaptive EA is divided into components that constitute it (see Table 2). These components are the basic building blocks of proposed IdE architecture. Every IdM system that was included in this research, had an exclusive focus on different aspects of the architecture. Some architectures comprised almost all aspects, while others only included few elements. The architectural components were extracted from literature and design documents to compile a list of the major components in each design. All these elements were then categorised based on the adaptive EA layers (see Table 2). An IdE is composed of four main entities (end users, service providers, attribute provider, relying party) (see Figure 2). End users are the individuals whose personal data is processed to create a digital identity. Service provider issues and manages credentials. The attribute providers are the entities that allow the ID feature to be used for identification purposes. For instance, a credential provided by a bank could have an attribute from a telecom firm or a social network to carry out certain jobs. Lastly, the relying parties are those who will receive the credentials provided in the IdE (see Figure 2). In this study, we have taken the best bits of what others have done and learned from their experience to create a secure IdE which is privacy enabled, secure, interoperable, adaptable, cost effective and easy to use. To achieve all these properties, the proposed architecture is divided into six layers based on adaptive EA.

5.1 Interaction

The Identity Ecosystem supports many types of interactions. According to Gartner, an ecosystem "enables you to interact with customers, partners, adjacent industries – and even your competition." In case of identity management, all entities (end user, service providers, attribute providers and relying party) are continuously interacting with each other and within their own organisation. The interaction layer in adaptive IdE architecture proposed in this study is intended to be compliant with 'privacy by design' principles. The table 1 shows the kind of interactions in adaptive IdE architecture. Each layer interacts with corresponding layers in a many-to-many relationship.Human

The architecture of an IdE fails when not informed by and viewed from human perspective. The human layer has sub-elements such as human performs different roles and involved in the process of ID verification with the IdE. All these varying roles need to be considered when developing an IdE.

Human exchange information and socialise in the process of ID verification. Human layer is supported by many technologies, which could be hosted at different facilities within the external and internal environment of multiple organisations within the overall context of IdE.

5.2 Technology

Technology architecture is about modelling the basic technology elements of and their relationships for the identity ecosystem. It covers the hardware and software applications, platforms and infrastructure technologies that are required to support the IdE. For instance, the software applications for IdE can be web or mobile apps along with their supported platforms (iOS, Android, Windows). Identity verification services are provided based upon personal data that represents individual identity such as ID card, passport, driving licence. The data is stored in secure storage systems and servers implementing encryption at rest and encryption at transit. Modern identity verification solutions leverage a variety of emerging technologies, including computer vision, blockchain, OCR, artificial intelligence, machine learning and biometric-based liveness detection. An ideal IdE needs to utilise the best-of-breed technologies as per requirements into its identity services and solutions. With the ever increasing and changing business needs, the underlying technologies must also evolve.

5.3 Facility

Facility layer includes spatial, energy, HVAC equipment and any other ancillary components required to support the interaction, human and technology layers of the IdE . Securing a facility layer effectively requires that every element within the layer, from data centres and energy equipment to HVAC facility and ancillary (e.g. fire, health & safety), be integrated into an overarching security plan. DZ specialises in the APAC region supplying comprehensive data to meet identity requirements. The identity solution is based on Google cloud and the data centres are also dispersed around Australia, China, Hongkong, India, Indonesia, Malaysia, NZ, Singapore, Philippines and Vietnam. A well-managed facility layer helps IdE function effectively and efficiently. We have developed IdE architecture to consider the physical locations of DZ, the equipment installed at each location the energy facilities, the precautionary arrangements for fire, health & safety and how they can be protected using physical security protocols.

5.4 Environment

Human, technology and facility interactions are executed in an ecosystem environment. Such environment should be secure. In an IdE, the environment supports all basic requirements for components performance and evolution. A system's environment governs the variety of external and internal stimuli upon the system (ISO 2011). The environment also comprises political, economic, social, technological, environmental, legal, and all other influences which can affect the architecture. Politics and relevant national and international polices can potentially have a huge impact on the DZ IdE. The geographic characteristics, standards, traditions and morals of people influences the design of IdM architecture and solutions as well. For example, it might affect the available skills of local staff and their readiness towards working in certain situations. Technological features relate to modernisations in technology that could favourably or un-favourably affect the IdE architecture and its technical viability. Environmental aspects such as increasing awareness of the possible effects of weather changes can also influence the IdE and its operations. It is important to consider the legal requirement for DZ while defining the environment architecture for IdE. IdE needs to have a clear understanding of legal and not-legal elements, in order to provide identity services successfully and ethically. Laws regarding IdE that do not include controls on information protection, security and privacy, and other threats may only direct the formation of a system without providing a complete background for fair and lawful operations of the system. An IdE where this issue has been overlooked, there are everyday issues, such as witnessed in India's Aadhaar IdE. DZ clients require them to comply to ISO 27001 hence, they have their policies designed around it. Government policies, legal and compliance requirements, company's business strategy and its economic standing define the sociotechnical environment for IdE. In summary, DZ operates in a complex and interconnected environment, and must need to consider environment factors when designing and implementing the IdE architecture.

5.5 Privacy

Privacy is cross-layer concerns and is applicable to interaction, human, technology, facility and environment layers and underlying assets or elements of the IdE (Figure 2). In an effort to enhance privacy on different layers of IdE, different practices are used as shown in Table 2.

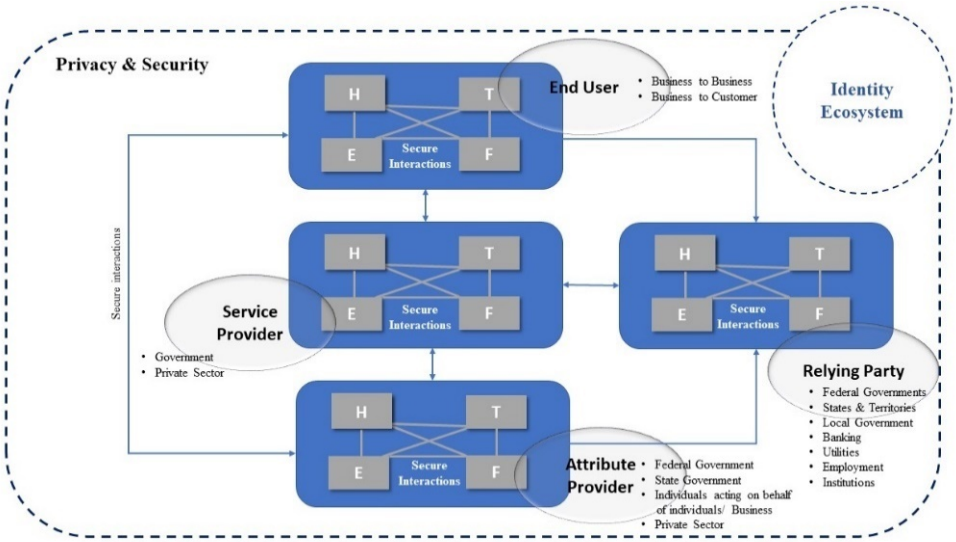

Figure 2: Identity Ecosystem Architecture

Figure 2 shows the main components of an IdE and their internal layers. An end user could directly be a data subject, or a business authorised to hold data subject's personal information. Service providers facilitate end users(individuals/businesses) in process of identity management and verification. In this process, service providers verify the personal information provided by end users with the attributes provided by attribute providers. For example, an end user may claim to be of certain age. In order to prove this, he will provide his dob to service provider who will then verify the information from the issuing authority such as federal government e.g. passport. Relying Party are those who reply on service providers verification about the credentials of the end users issued by attribute providers such as employers, institutions, banks etc. All these interactions have a common security requirement hence the entire series of actions is carried out under privacy and security layer.

6 DISCUSSION AND IMPLICATION

Adaptive EA (Gill 2014;2015) is a comprehensive framework with a very detailed coverage of concepts and layers for IdE. Therefore, Adaptive EA elements and layers are used as a lens and starting point for this study (see Table 2). Further we derived IdE architecture elements by reviewing renowned IdM systems. The list of elements discovered from the designs provides the basis for a generic IdE architecture that can be used for any IdM system. Elements derived from the adaptive EA and industry best practices were aligned to DZ vision for IdE (see Figure 1).

The proposed IdM architecture is composed of four main layers (Human, Technology, Facility and Environment) which are **interacting** with each other via interaction layer inheriting privacy and security from security layer. The **human layer focuses** on business, information, professional and social elements. While designing this IdE architecture, one major thing that came into play was DZ's vision of identity. DZ devised its identity vision based upon its goals and business strategy. The vision was formulated by a group of professional and senior people who had their experience and skills in doing so. The business goal for DZ is to successfully provide identity information (e.g. proof of age) based upon data subject's (Human) identity attributes (Name, dob etc). This entire business process is carried out by professional humans interacting with each other according to the assigned roles and responsibilities in line with their social goals (FAQ, technical support). The **technology layer** includes application, data, platform and infrastructure elements to support DZ's identity vision. The identity services can be provided through any type of application (mobile, web) running on compatible platform (iOS, Android, Windows, MAC etc), supported by infrastructure (cloud, storage etc.), based upon the identity data (passport, driving licence etc). Irrespective of the technology used, an effective IdE must be adaptable, secure, comprehensive, and interoperable to ensure access to multiple institution. The **facility layer** integrates human, business locations and processes within the organisational environment services (ISO 2017). The facility layer of IdE architecture describes what locations are managed by DZ, what type of equipment is used, how energy requirements are fulfilled and how are physical and environmental hazards handled. Hence, facility layer is composed of spatial, energy, HAVC and ancillary components

(e.g. fire, health & safety). Facilities can be an office complex, physical resources at the company or site. The **environment layer** is composed of political, economic, social, technological, environmental and

Layer	**Instance**	**Privacy & Security**
Interaction	Verification process, Data source connections, Identity Network	Secure interactions, Logs and Audit Trails
Human		
Business	Identity Verification (digital onboarding, electronic verification, global screening, due diligence delivery platform, AML/CT Compliance), PEPs and Sanctions, Rule set, attribute providers, consumers and relying parties, Privacy by design & default	IPfication, Authentication and Authorisation, ISMS, Internal/External Audit, Training and Awareness, vulnerability & penetration testing, data collection practices audit, communication, Privacy Impact Assessment, Trusted processing Environment, Watch list checking, Fraud Risk, Marketing and advertising, Age Verification, consent, notice
Information	Identity attributes (name, phone no, dob, address, passport no, SSN, DL etc)	Information Life Cycle (Management), Masking, Tokenisation, Encryption, Hashing, confidentiality and NDA, classification, labelling, attribute minimisation, credential limitation, anonymity, zero knowledge proof
Professional	Internal/External Auditor, Evaluator, Verifier, User, ISMS Manager, Identity Attribute Providers, Accreditation authorities	KYC/AML checks for partners, Compliance certification
Social	FAQ, Technical Support, Operational Support, brochures, culture	Privacy Policy, Employee Screening, Usage notice, Consent
Technology		
Application	Mobile and Web	Device ID, IPfication, mobile device policy, Firewalls
Data	ID card, Passport, Driving Licence, Social Security Number	Data quality, Discovery, classification, labelling, Hashing, Encryption, Provenance, Curation, Archiving, data minimisation, data retention and disposal
Platform	iOS, Android, Windows	Updated patches
Infrastructure	Google Cloud, Network, Storage, Servers (NZ, Singapore, Philippines), identity media, switches, routers	IS Audit, Technical vulnerability management, restriction on software installation, Network Control, Segregation of Network, Risk assessment and treatment
Facility		
Spatial	DZ offices (Australia, NZ, Singapore), Data locations (Australia, China, Hongkong, India, Indonesia, Malaysia, NZ, Singapore, Philippines, Vietnam), GC data centre facility, office layout	Encryption at Rest, Encryption at Transit, physical security
Energy	Generators, UPS system/backup generator, cables,	Physical Security,
HVAC	Air conditioners, heating ventilation, HVAC Equipment	Physical Security, network security, timescale equipment testing, cabling security, equipment maintenance, asset offsite policy
Ancillary	Fire, Health & safety, parking space,	Physical security, emergency exit plan, effective waste disposal
Environment		
Political	Asia Pacific and international privacy laws, cross border transfer of information, proof of data collection	Jurisdiction ethics and laws
Economic	New competitors in market, economic growth, exchange rates, inflation rates, interest rates, disposable income of consumers and unemployment rates	Competitors analysis
Social	Increased privacy awareness, Notice and Consent, Legal and Ethical sources of information, career attitude, safety emphasis, health consciousness, cultural barriers	Training and Awareness, Trust
Technological	Blockchain, biometric, mobile, web, failover services, privacy compliant proof of data storage	Feasibility and Suitability research and development
Environmental	Environment and carbon footprint, Environment Friendly Identity services, climate	Paperless Digital Identity, Corporate social responsibility (CSR)
Legal	AML & CT Compliance, ISO 27001, Cross border transfer of personal information, legislative requirements for data sources	End user compliance obligations, GDPR, ISO 27001

Table 2. Identity Ecosystem Elements based on (Gill 2014; 2015)

legal considerations (Rastogi and Trivedi 2016). Social factors such as the age, income, career choices, safety awareness, privacy awareness and cultural blocks influence the design of IdE architecture. Along with social components, technological factors may affect decision about getting into certain domains, to offer certain service or to outsource operational service. Being informed technology-wise, businesses can be prevented from spending un-necessary money on implementing a technology that would become outdated very soon due to troublesome technological changes elsewhere (B2U 2016). The IdE architecture presented in this research also highlights environmental elements such as raw materials, climate changes, pollution and carbon footprint goals presented by government. In addition, economic features may have a direct or indirect lasting influence on an IdM systems. It determines the buying power of customers and can perhaps modify the demand/supply models in the economy. Accordingly, it also impacts the pricing of products and services. DZ operates globally which makes legal requirements particularly complicated because each government has its own legislations and standards. All the layers of IdE are interdependent and interact with each other to carry out identity functions. For example, if a system fails it is not just a facilities' problem, it could also be a technology related problem. If an electrical failure disrupts your data centre, it raises questions like; how are facilities management systems running? If the fire alarm system is running on a server that fails or hacked or compromised, what happens? If it is virtualized, it may just fail over to another virtual server and continue. To authenticate compactness of the proposed architecture we can look how its components are connected and working together. This is demonstrated in Table-1.

In order to preserve the strong user-focused privacy properties of the IdE, this architecture has a fully dedicated **privacy layer**. The growing privacy requirement is a blend of civil rights and cultural partialities; commercial policies, state, national, regional, and international regulations and laws; as well as input from global entities such as the Organisation for Economic Co-operation and Development (OECD), the United Nations and Internet Corporation for Assigned Names and Numbers (ICANN) (Holt and Malčić 2015). The privacy constraints affect all layers and underlying elements involved in IdM system. Hence, in defining components of privacy layer, we kept our focus on ISO 27001 due to DZs' client's requirements. However, the privacy preserving practices mentioned in Table-2 are generalised and independent of any specific law or standard.

7 CONCLUSION AND FUTURE DIRECTIONS

Although the technical details of several aspects of an IdM architecture are very well explored, very little work is done towards definition and integration of an adaptive IdE architecture. This study proposed such adaptive IdE architecture which is an attempt to fill this small research gap and has several implications. Firstly, it aims to identify all the essential layers & underlying elements for IdE type architecture. Secondly, this architecture presents a notion of adaptability that makes the proposed architecture more agile and flexible to ever-changing privacy and security needs of a business. The future research and development in this area will consider additional IdE development and implementation with the DZ clients. This will generate additional insights, which will be shared with the community in future publications. Finally, this research sets a foundation for further defining a Common Body of Knowledge (CBK) for IdM and thus provide a basis for a consistent curriculum development. It is anticipated that the proposed architecture in this paper will provide a step toward the definition of the adaptive IdE reference architecture and Common Body of Knowledge (CBK) for digital identity and IdM systems.

8 REFERENCES

Agarwal, D., Lorch, M., Thompson, M., and Perry, M. 2003. "A New Security Model for Collaborative Environments,"

Anwar, M., Gill, A. 2019. "A Review of the Seven Modelling Approaches for Digital Ecosystem Architecture," *21st IEEE Conference on Business Informatics*, July 2019

Anwar, M., Gill, A., and Beydoun, G. 2018. "A Review of Information Privacy Laws and Standards for Secure Digital Ecosystems," *29th Australasian Conference on Information Systems,* December,2018

Australian Government. 2017. "Review into Open Banking in Australia," August 2017, (available at https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-IP.pdf ; retrieved July 25, 2019)

B2U. 2016. “PESTEL Analysis (PEST Analysis) EXPLAINED with EXAMPLES,” Industry Analysis, September 16 (available at https://www.business-to-you.com/scanning-the-environment-pestel-analysis/; retrieved August 4, 2019).

Bauer, M. 2004. "Paranoid Penguin: Linux Filesystem Security, Part Ii," *Linux Journal* (2004:127), p. 11.

Bourass, I., Afifi, N., Belhadaoui, H., Ouzzif, M., and Hilali, R. F. 2014. "Towards a New Model of Management and Securing Digital Identities," *2014 International Conference on Next Generation Networks and Services (NGNS)*: IEEE, pp. 308-312

Breebaart, J., Busch, C., Grave, J., and Kindt, E. 2008. "A Reference Architecture for Biometric Template Protection Based on Pseudo Identities," *BIOSIG 2008: Biometrics and Electronic Signatures*

Bujoreanu, L., Mittal, A., and Noor, W.2018. “Demystifying technologies for digital identification.” Voices, February 27, 2018 (available at https://blogs.worldbank.org/voices/demystifying-technologies-digital-identification; retrieved August 7, 2019).

Bussard, L., Di Nitto, E., Nano, A., Nano, O., and Ripa, G. 2008. "An Approach to Identity Management for Service Centric Systems," *European Conference on a Service-Based Internet*: Springer, pp. 254-265.

Chigani, A., Arthur, J. D., and Bohner, S. 2007. "Architecting Network-Centric Software Systems: A Style-Based Beginning," *31st IEEE Software Engineering Workshop (SEW 2007)*: IEEE, pp. 290-299.

Civic. 2017. “Civic Whitepaper,” Civic (available at https://tokensale.civic.com/ CivicTokenSaleWhitePaper.pdf ; retrieved August 3, 2019)

Dabrowski, M., and Pacyna, P. 2008. "Generic and Complete Three-Level Identity Management Model," *2008 Second International Conference on Emerging Security Information, Systems and Technologies*: IEEE, pp. 232-237.

D-Cent. 2013 "Research on Identity Ecosystems"

Dixon, P. 2017. “A Failure to ‘Do No Harm’ – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.,” Technology Science, August 29 (available at https://techscience.org/a/2017082901/; retrieved August 3, 2019).

Dixon, P. 2019. “Digital Identity Ecosystems,” Blog, February 30 (available at https://www.worldprivacyforum.org/2019/02/digital-identity-ecosystems/ ; retrieved August 2, 2019).

Equifax. 2015. “A Lasting Impact: The Emotional Toll of Identity Theft,” February 2015 (available at https://www.equifax.com/assets/PSOL/15-9814_psol_emotionalToll_wp.pdf ; retrieved August 1, 2019).

Evernym. 2018. “Sovrin: A Protocol and Token for SelfSovereign Identity and Decentralized Trust,” January 2018, Sovrin (available at https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf ; retrieved August 3, 2019)

Gill, A. Q. 2014. "Applying Agility and Living Service Systems Thinking to Enterprise Architecture," *International Journal of Intelligent Information Technologies (IJIIT)* (10:1), pp. 1-15.

Gill, A.Q. 2015. “Adaptive Cloud Enterprise Architecture”. World Scientific,2015.

Gill, A.Q., Chew, E. 2018. “Configuration information system architecture: Insights from applied action design research,” *Information & Management*, North-Holland, September 25 (available at https://www.sciencedirect.com/science/article/abs/pii/S0378720617310091; retrieved October 11, 2019)

Hanson, F. 2018. "Preventing Another Australia Card Fail,".

Holt, J., and Malčić, S. 2015. "The Privacy Ecosystem: Regulating Digital Identity in the United States and European Union," *Journal of Information Policy* (5), pp. 155-178.

ISO. 2011. “Systems and software engineering - Architecture description.” (n.d.). ISO/IEC/IEEE 42010: Conceptual Model (available at http://www.iso-architecture.org/ieee-1471/cm/; retrieved August 5, 2019).

ISO. 2017. "ISO 41011:2017." ISO, March 31 (available at https://www.iso.org/standard/68167.html; retrieved July 31, 2019).

Jin, Z., Xu, J., Xu, M., and Zheng, N. 2010. "An Attribute-Oriented Model for Identity Management," *2010 International Conference on e-Education, e-Business, e-Management and e-Learning*: IEEE, pp. 440-444.

Johansen, A. G. (n.d.). "4 Lasting Effects of Identity Theft," LifeLock Official Site, Symantec (available at https://www.lifelock.com/learn-identity-theft-resources-lasting-effects-of-identity-theft.html retrieved August 2, 2019).

Jumio.2017. "Five tips to make sure that customers transact with your app, A Jumio White Paper," (available at https://www.jumio.com/app/uploads/2017/06/apps-wp.pdf ; retrieved August 3, 2019)

Kerberos, M. 2005. "Kerberos: The Network Authentication Protocol." Diakses.

Mishra, P., Maler, E., Cahill, C. P., Hughes, A. J., Beach, M., Metz, B. R., Randall, R., Wisniewski, T., Reid, E. I., and Austel, P. 2005. "Conformance Requirements for the Oasis Security Assertion Markup Language (Saml) V2. 0." OASIS SSTC, March.

Rastogi, N., and Trivedi, M. 2016. "Pestle Technique–a Tool to Identify External Risks in Construction Projects," *International Research Journal of Engineering and Technology (IRJET)* (3:1), pp. 384-388.

Ray, E., and Schultz, E. E. 2007. "An Early Look at Windows Vista Security," *Computer Fraud & Security* (2007:1), pp. 4-7

Sein, M., Henfridsson, O., Purao, S., Rossi, M., and Lindgren, R. 2011. "Action Design Research," *Management Information Systems Quarterly* (35:1), pp. 37-56

ShoCard. 2017. "Identity Management Platform," ShoCard Inc (available at http://shocard.com/wp-content/uploads/2018/01/ShoCard-Whitepaper-Dec13-2.pdf ; retrieved August 3, 2019)

The White House. 2011. "National Strategy for Trusted Identities in Cyberspace (NSTIC)," The White House, Washingtion, Aprill,2011

Windley, P. J. 2005. *Digital Identity: Unmasking Identity Management Architecture (Ima)*. " O'Reilly Media, Inc."

Acknowledgement

This research is supported by "Australian Government Research Training" Program Scholarship. We are also thankful to our industry research partner for their ongoing financial support.