A Review of Identity, Identification and Authentication

Juanita Blue, Joan Condell, Tom Lunney
ISRC,University of Ulster, UK

Abstract

With the continued increase in identity theft and related crime, the topics of Identity, Identification and authentication have become a salient focus for governments, institutions and federal crime units across the globe. A plethora of personal identifying details contribute to the formation of an 'identity'. The construct of an individual's identity is formed from a combination of attributes that may be genetic, assigned, acquired or socially based. Although the concept of 'identity' is somewhat intangible, the concept has morphed in something that is undeniably tangible through the use of identification documentation. Traditionally individuals and organisations depended on traditional paper documentation as a proof of identity, however, with technological advancements, this trend is fast becoming obsolete. Individuals are now required to prove their identity not only in the physical world but also in a cyber context. This review paper explores the areas of identity, identification and authentication, identifying the means by which individuals may be identified, including the modern technologies that are invoked to conduct the process. It also examines emerging technologies that may become standard methods utilized to authenticate purported identities.

1. Introduction

Every individual who is born into the world has an identity. Although identity may be considered intangible, its elements contribute to the formation of an entirely unique and separate entity. The embodiment of this persona emerges from a distinct subset of characteristics that are both inherited at birth and acquired over time. From their birth, individuals possess a unique combination of personal attributes which vary in their method of assignment, some are genetically defined physical identifiers such as ethnicity, height, eye colour. Others are genetically defined familial links such as birthmother, birthfather and sibling relationships. Then there are those that may be circumstantially assigned at or closely following birth, these include birthdate, place of birth, name. This type includes government assigned primary keys such as a National Security Number (NSN), designed to function as a unique identifier as a part of governed identity management. As individuals develop and interact with society they acquire additional attributes that map the path of their lives. These details may include home addresses, education history, employment history, spouses, offspring, extending to assets and medical history.

Accumulation of personal identifiers and formation of an associated identity has become requisite in modern society. The tenure of an identity functions both to protect an individual, allowing them prove and claim various benefits via ownership and rights, it also functions to protect the individuals and organisations they interact with, enforcing accountability, traceability and trust. When individuals identify themselves, they are making a claim of identity based on a variety of the aforementioned attributes. However, these claims alone do not authenticate identity; supportive evidence is required to verify that the identification document and the information contained therein are valid and therefore the identity of the individual is verified [1].

In contemporary times, identity has metamorphosed from something intangible to something that is quite tangible and that can be traced. Verification of identity can be achieved through tangible identity cards and documentation such as birth certificates, passports and driver's licences. Although these documents have been relied upon for many decades and considered to be suffice, technological advancements and improved printing capabilities have undermined the integrity of this type of documentation. Counterfeit identity documents have become increasingly commonplace, subsequently, authentication and verification of identity documentation has become more difficult than ever. To counteract counterfeit documentation, theft resistant authentication mechanisms are built into identity documentation to prove the document is genuine and verify the identity assertions that are made, and to protect the true and legitimate identity [1].

To achieve this end, industry invokes various types of security and verification features within identity. Although these features verify the authenticity of the card itself, they do not verify the identity presented on the card. To do so would require the card to link to a real-time central repository that verifies the individual is authorized to

possess the identity card itself, thus verifying the link between the card and the card-holder.
In recent times there has been a sharp rise in incidents of identity theft, where perpetrators use the identities of others for nefarious purposes and essentially to violate the law. Identity theft is the misuse of another individual's personal information to commit fraud. It generally occurs in two stages; illegally obtaining personal information relating to the identity of an individual and using this information to create a fake identity through false or fraudulent documentation. In a bid to stamp out fraudulent crime, there is increased pressure on individuals to provide evidence that they possess a 'real' identity [2].

Counterfeiting and fake identities have reduced confidence in traditional documentation as a proof of identity, this has created demand for electronic and digital alternatives [2]. Recent government implementations and identity trends have also imcreased the popularity of electronic and digital forms of identification. There has been a catalytic shift toward the utilization of digital identification as a method of authentication both online and off. Innovative identification technology invoked by Estonia has encouraged a futuristic trend where paper documents are no longer relied upon to attest to the identity of an individual. This is in line with the UN directive that every individual shall have a legal identity by 2030.

This review paper explores various aspects of identity authentication and identification verification. This is achieved by initially examining the core construct of identity based on personal attributes, therein also identifying potential new types of personal identifying attributes. This is followed by an examination of methods used to verify identity both manually and in an automated fashion. The paper moves through modern technologies including methods of identity resolution and online identity access management, finally ending with modern implementations of electronic and digital identification, including current innovation and research in that area.

2. Identity and Identification

Identity is a broad term from which society has drawn many meanings. In a philosophical or psychological sense, it describes the unique condition or character to who a person is, including the qualities and beliefs that distinguish them from another. In another context, it describes the condition of being oneself and not another based on personal identifying attributes that largely remain static. It is in this context that the concept of 'proving identity' has grown. For the purposes of this review paper, identity is viewed in the context of the combination of recordable and traceable attributes that distinguish one individual from another. To this end 'identification' is the evidence that may be provided to prove that a purported identity is genuine and thus, to authenticate that identity both in the real and digital worlds.

In the digital context, the terms 'digital identity', 'digital footprint' and 'electronic identification' are used somewhat interchangeably and often convey very different meanings. This may cause confusion regarding the type of characteristics, data or systems that are being referred to. Research was conducted to distinguish between these and associated terms to establish the most widely accepted meaning for each. To clarify the terminology for the purpose of this paper, the meanings are defined in the next subsection.

2.1. True and Fake Identities and Identification

Fake identities present a very real threat to modern digitalised society, presenting the opportunities for criminals and terrorists to commit various types of crime. These types of crime are potentially committed both online and within the physical world. In examining fake/real identities and fake/real identification documentation, it was discovered there were four distinct groups. When combined, they were as follows:

- Fake Identity/Real Document
- Real Identity/Real Document
- Real Identity/Fake Document
- Fake Identity/Fake Document

As demonstrated by successful incidents of cybercrime and fraud, the biggest threats reside where the identity is fake, as tracing these individuals is considerably more cumbersome than tracing real identities displayed upon a fake document. Additionally, the core threat lies in the accessibility and acquisition of fake identities, not the verification documentation that is produced thereafter.

An investigation into the origin and creation of fake identities indicated that typically fake identities are not entirely fabricated, they are generally duplicated real identities (possibly altered slightly). This is based on the premise that it is far more difficult to obtain traditional identification documentation with an entirely fabricated Identity that lacks verifiable personal attributes such as national security numbers (NSNs).

It should be noted that traditional identification documentation alone does not verify a true identity as there is always a risk of document tampering. Although security features are incorporated into identification documents and these features verify

the authenticity of the document itself, they do not verify the identity presented on the card, the overtly displayed identity remains potentially fake and/or stolen.

2.2. Digital Identity

Twenty-five years ago, in 1993, a cartoonist named Peter Steiner created a cartoon for The New Yorker magazine that claimed "On the internet, nobody knows you are a dog". This popular image gave great insight and pre-empted a futuristic and very real challenge that is faced globally today. In theory, a digital identity can be whatever you want it to be [3].

Figure 1: Peter Steiner's infamous New Yorker magazine cartoon

A digital identity as a single definition is globally debated. However, it is largely accepted as the online persona of a subject. The use of the term 'persona' describes the changeable and often capricious nature in which a subject can represent themselves online. Individuals may have multiple digital identities for their various accounts including email, personal finances or social media. Digital identity as a legal identity in terms of digital signatures and certificates further complicates the terminology. Furthermore, remotely proving that an individual is who they purport themselves to be is fraught with opportunities for attackers to impersonate individuals.

In cases where accessing 'low-risk' digital services, proof of identity is of lesser importance, however when accessing 'high-risk' services, an appropriate level of confidence is required to establish that the digital proxy is a legitimate link to the real-life subject. This further develops the term 'digital identity' to refer to the unique representation of a subject engaged in an online transaction [4]. However, it may be considered that a digital identity is always unique in the context of a specific digital service, but this does not mean that the specific service needs to uniquely identify the subject in all contexts. This implies that accessing the digital service, the subject's real-life identity may not be known. For this reason, a digital identity may or may not be associated with a subject's real-world identity and may also be associated with various organisations through electronic records, identity access management (IAM), digital signatures & certificates and under many other online conditions.
The term 'identity proofing' is used to describe the process of establishing that a subject accessing digital services are who they claim to be. Digital authentication is the term used to describe the process that establishes that a subject attempting to access a digital service is in control of a valid authenticator associated with that subject's digital identity.

2.3. Digital Footprint

As described in the previous section, individuals now possess a "real world identity" and one or more "digital identities", defined by their interaction and access to online services and accounts. The term 'digital footprint' is often used interchangeably with 'digital identity', however there are notable differences between the two.

A digital footprint represents an individual's online presence and provides evidence of their digital and real-world identities. It logs the trail and artifacts left behind by individuals interacting in a digital setting. Digital footprints are persistent and link the past with the present, regardless of transitions and changes in an individual's life. It requires multiple participants as it intertwines with external and official entities and it is bolstered by electronic records, email notifications, digital receipts, the lives of others and the metadata that forms components of the digital footprint used to trace and record every online move [2].

2.4. Electronic Identification (e-Identification)

As an element of 'e-Government', this type of identification, although digitalised, largely refers to electronic records that contain data relating to citizens of a nation. As well as allowing online access and authentication for government services, this type of digital record is linked to a physical document containing a chip that verifies the identity of the document holder. For this reason, e-ID in all its forms is typically considered two-factor

authentication, where a subject 'has' something and 'knows' a password to authenticate their identity. Thus, this technology is a combination of traditional identification documentation and IAM.

3. Identity Records and Management

According to a report released by The United Nations, the current world population sits at approximately 7.2 billion. With an average increase of 200,000 per day, this is projected to increase by 1 billion over the next twelve years and reach 9.6 billion by 2050. In dealing with such vast numbers of individuals, governments attempt to apply schemes that aid them in differentiating between individuals. This allows them to categorise, identify and if necessary, pinpoint specific people for a range of legal and humanitarian reasons. In achieving this end, the world's citizens are each defined by a unique set of personal identifiers that are subsequently stored in various types of identity management systems. Where identities may be mistakenly duplicated, identity resolution techniques are invoked to identify where two separate records link to the same real-world individual. This section discusses types of personal identifiers, identity record management and identity resolution techniques.

3.1. Personal Identifiers

An individual's true identity is comprised of two basic components, a personal identity represented by standard identifiers and also a social identity. An individual's personal identity is acquired from birth and includes identifiers such as name and date of birth; officially assigned identifiers such as a national security number (NSN); current physical descriptions such as height and weight and also biometric data such as fingerprints. A social identity is a person's biographical history, gathered over their lifetime, describing the social context of their life experience. Social contextual information refers to the 'reputation' that an individual has built up over time, this is inclusive of employment history, credit history, friendship networks and familial relationships. These attributes have been found to be effective when identities are reconciled as they are difficult to manipulate [2].

3.1.1. Biometric Identifiers. The term 'biometric' refers to a process where an individual's biological traits are measured and statistically analysed to prove identity. This may include physical characteristics such as fingerprints, iris/retina patterns and hand geometry or behavioural characteristics such as voice, handwriting and gait. The premise of using physical or behavioural data in identification is fundamentally based on the concept that every individual is unique and therefore may be identified by their unique individual traits. Acquisition may be accomplished using scanner/reader devices, some of which are more physically intrusive than others depending on the type of data being harvested. Following acquisition, the analogue signal is digitalised and stored in an authentication database. In recent years, biometric security technologies have advanced to allow for almost instantaneous identification.

Technologies that are currently commercially available possess several tangible benefits; the costs have been greatly reduced, the devices are small and overall they are relatively easy to integrate. Biometric identification tools are considered to be convenient and more secure than alternative methods such as passwords, therefore fulfilling the need for strong authentication. This has resulted in an increased employment of biometric security technology by governments, financial institutions and other organisations. Thus, a scenario has been shaped where individuals are now compelled to provide their biological information for standard identification purposes. The mandatory provision of personal biometric information however raises many legal, ethical and social issues in relation to the data's acquisition, purpose and storage.

3.1.2. Social Identifiers. Social identity theories consider both the psychological and sociological aspects of an individual's existence. An individual's social identity and their interaction with the world and its occupants is defined by the psychological view. Interpersonal relationships that are role-based between "social actors" such as teacher-student and employer-employee are emphasized by the sociological view. Combining these views allows for a more comprehensive understanding of social identity. Research conducted in the area of identity by Wang et al. has indicated that the use of additional non-standard attributes that relate to an individual's social behaviour may contribute to the authentication or refutation of identities when attempting to identify unique individuals who have shared or replicated attributes [5].

Traditionally, standard personal identity attributes in record management systems were used to differentiate between individuals. However, data quality may affect these attributes [5]. Biometric data is potentially more reliable as an identifier, however due to high cost and confidentiality issues, this information is often unavailable. The United Kingdom Home Office conducted a study on identity fraud [6] suggested that crimes involving identity typically involved records where traditional personal identifiers were illegally used or altered. In deviating from the utilization of traditional identifiers, an individual's social context should possess attributes that authenticate their undeniable

identity. Recent studies have recognized the value of social context data such as relationships and social behaviours in identity resolution. For example, Köpcke and Rahm devised a categorical scheme that considered attribute-value-matchers that rely only on attributes that are descriptive and contextual matching to examine data gathered from social interaction links [7].

The trend toward digitalised existence and increasing popularity of social media platforms such as Facebook, Twitter and Instagram have certainly facilitated a shift toward utilising both standard personal identifiers in addition to social contextual information to differentiate between individuals who share attributes such as name, date of birth and residential area among others.

3.2. Identity Records & Management Systems

Technology has ameliorated how identities are recorded and proven with organisations relying more heavily on electronic records to execute the same [2]. ISO/IEC 24760-1 defines identity as "set of attributes related to an entity". The information contained in a digital record allows for assessment and authentication of individuals interacting with organisations often without the involvement of human operators [8].

Government records are defined as recorded information in any form, created or received in the conduct of government business and kept as evidence of activities and transactions. This definition emphasizes the purpose, rather than the physical form or recording medium. The definition includes traditional paper records and records in all other forms, including electronic.

Records management has traditionally referred to an organisation's policies and procedures for managing file systems and disposing of records once they are no longer needed. In recent years, attention has shifted to the need to create reliable records in electronic form, and 'records management' is understood more broadly to mean the overall management of records from their initial creation to final disposition.

The sheer volume and complexity of modern records is apparent to anyone who uses them. Government employees at all levels have first-hand experience of the importance of good records management, whether they create or handle records in their work, depend on finding the records they need quickly, wonder how long their records should be kept, or are required to make decisions that affect the way business-critical records will be created and maintained.

Current implementations utilizing electronic records provide for convenience. However, entry processes that lack precision, verification and validation have caused fake, duplicate and erroneous records to become commonplace in identity record management systems. Subsequently, many identity schema lack the integrity to properly verify and authenticate identities [2].

3.3. Identity Resolution

Identity resolution is a process of semantic reconciliation that determines whether a single identity is the same when being described differently. The goal of identity resolution is to detect identity records that are co-referent to the same real-word individual. Database and Statistics researchers have proposed a plethora of techniques to implement forms of identity resolution. Traditionally, these techniques rely on key attributes such as identification numbers, names and date-of-birth to detect matches between records. These common attributes act as simple describers of an individual, most individuals possess them and they are available in most record management systems [5]. However, the same identity attributes also vary in terms of availability and reliability across heterogeneous systems. Due to erroneous and absent data entry, the accuracy of these attributes cannot be relied upon [5] and thus, they do not present a reliable source of information against which identity authentication can be performed. This simplifies the task for criminals and terrorists who wish to conceal their true identities and prevent themselves from being traced.

Identity resolution can be invoked to determine whether a single identity has been duplicated when described by variant personal identifiers in separate records, with the aim to detect identity records that refer to a single individual as depicted in Figure 2. In a bid to improve the accuracy of identifying duplicate and potentially fake identities, recently proposed resolution techniques have considered the use of additional attributes that may also contribute to the authentication or refutation of identities. When social contextual information is reconciled along with traditional description attributes, new avenues of evidence are created for identity matching.

Varied attribute types and methods for record matching result in various success rates when operating as a means for detecting duplicate and potentially fake identities in heterogeneous identity management systems. Assorted identity attributes provide valuable assurances when conducting computational identity resolution, especially when considering both personal identity attributes and social identity attributes. Current matching techniques include pairwise matching, transitive closure and collective clustering.

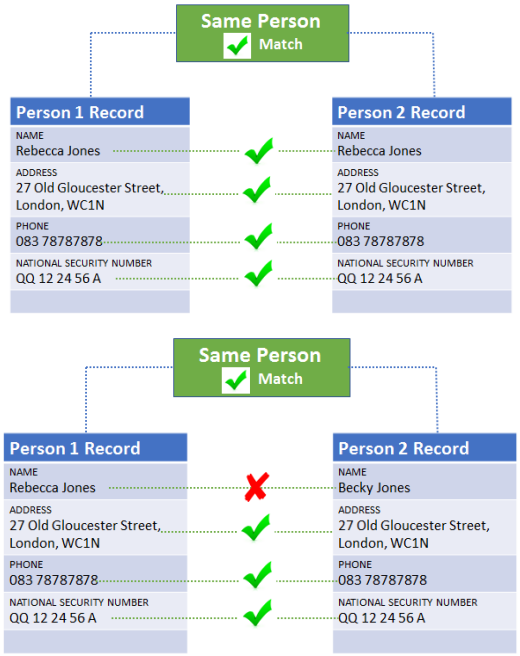

Figure 2: Identity Resolution of Identical and Non-Identical Duplicate Records

4. Identification Documentation and Authentication

Trends in identification documentation have metamorphosed over time, in each stage paying homage to the available resources and technology. This has led to many variations and styles of accepted documentation that may be used to verify an identity. This section examines various implementations of identification documentation. These examples range from traditional paper documents to electronic implementations such as eIDs, ePassports and eBorders, to more recent digital implementations that include computer system Identity Access Management (IAM), Identity-as-a-Service, digital signatures and digital certificates.

4.1.Traditional Paper Identification Documentation

Currently, governments, financial institutions and other official organisations rely heavily on an individual's ability to produce physical paper documentation that can verify their purported identity. This is based on primary resources that were available from the latter half of nineteenth century, right through to current day implementations. Paper identification documentation may range from birth certificates, driver's licences and passports to other documentation that is 'difficult' to obtain such as education and health records, land title deeds and evidence of utility accounts. Depending on the type of documentation an individual possesses, they may be required to produce further 'proof' that they possess a valid identity.

Prior to advancements in printing capability and availability, identification documents were largely handwritten and verified by an authoritative individual who represented an official organisation. In the current age these types of documents would not be considered reliable without further supporting evidence of identity. Following the industrial era documents have largely become printed, displaying overt identifiers such as name and date of birth and even photos of an individual and to further protect the authenticity of paper documentation, security mechanisms have been invoked, examples of which are provided in Table 1.

Security Level	Attributes	Examples
Level 1: Overt	• Basic requirement • Lowest level security • Visual verification via discernible features • Overtly printed features • Characterised by method of production • Physical additives to card substrate and laminate	• Visible watermarks • Holograms • Fine printing • Fibres • Security laminates • Overt biographic data • Embossed ridges
Level 2: Covert	• Compliment level 1 features • Not readily perceivable • Requires basic specialist tools to capture, register and authenticate data (lighting, magnification)	• Smart chips • Contactless chips • Magnetic Stripes • Radio Frequency ID • UV Ink • Microprinting
Level 3: Forensic	• Optimum security • Complex & Specialized • Visually perceivable data combined with secret data • Requires specialist forensic tools to capture, register and authenticate data (unique algorithms) • Optimal schemes link to a real-time digital central repository	• Steganography • Barcodes • Qode • QR Code • Nexcode • SecureText™

Table 1. Identity Document Security Levels

4.2.E-Government and Electronic Identification Documentation

A prevalent trend in the last two decades has seen a shift toward 'electronic government' or 'e-government. Globally, governments have recognised improved benefits and efficacy in project management, cost reduction, risk sharing, improvement of service quality, and enhanced technological innovation in utlilizing digital infrastructure and pursuing e-government initiatives. Through this growing phenomenon, examples of e-government implementations include eIDentification, ePassports and eBorders as mechanisms of governance enacted in e-government policies. This section provides an overview of these aforementioned implementations.

4.2.1. Electronic Identification (e-ID). Electronic identification (e-ID) provides a key example of the development of shared digital infrastructures. This type of digital solution provides proof of identity for citizens to conveniently authenticate their identity when accessing benefits or services provided by government authorities, financial institutions and

other organisations. Aside from online authentication and login, these systems may also involve the use of digital signatures used to 'sign' electronic documents.

Typically, this type of identification document operates as two-factor authentication as users are provided with a physical identity card that can be used for online and offline authentication. An electronic identification is an example of smartcard technology that includes overtly displayed personal identifiers and also possesses an embedded RFID microchip that stores personal identifiers relating to the individual. This information may include images and biometric information such as fingerprints.

This type of government implemented eID system has been implemented by a plethora of countries across Europe, South America, Asia and the Middle-East. According to the EU electronic identification and trust services electronic identification and trust services (eIDAS) Regulation, described as a pan-European login system, all organizations delivering public digital services in an EU member state shall accept electronic identification from all EU member states from September 29, 2018 [9]. E-IDs have been evaluated from many perspectives, including technological decision [10], trust and public value [11], surveillance [12], and security [13]. Another set of studies by Melin et al. [14] found that there are significant challenges involved in managing e-ID, mainly due to contextual, technological integration, and governance issues in these projects.

4.2.2. Electronic Passports (e-Passports) and e-Borders. An e-Passport, also known as a biometric passport, is a traditional paper document that displays overt personal identifiers relating to an individual and also contains an embedded electronic microprocessor chip. The embedded chip stores personal identifiers that may be used to further authenticate the identity of the passport holder. This form of electronic identification is based on smartcard technology where the personal identifiers stored on the chip allow authorities to authenticate the document by ensuring that the information that is overtly displayed matches that which is covert [15]. Authentication is achieved by public key infrastructure (PKI) [16], decreasing the ease by which the document can be tampered with. As of June 2018, more than 150 countries issue electronic passports of this type.

Most countries provided their own implementation of e-Passports, however e-Passport security must conform to the international public standards of the International Civil Aviation Organisation (ICAO) which cover confidentiality, integrity and authenticity of the passport's data [16]. Currently the standard biometrics used for e-Passports are finger prints, facial recognition and iris recognition as defined by the ICAO's Document ICAO-9303 and verification of biometric features are conducted at e-Borders [16]. This has encouraged international airports to facilitate e-Borders as 'automatic border control gates' capable of verifying biometrics without the need for human intervention. However, in the interests of future-proofing and robustness, new trends in travel documents shall include the introduction of tamper-proof polycarbonate pages which dramatically reduce the risk of document fraud. This type of substrate will be introduced in the 2019 British passport. There is also an expectation that travel documentation will become further digitalised and data from the e-Passport may be stored in the user's smart phone. New technology conceived by the ICAO New Technologies Working Group called Logical Data Structure Version 2 (LDS2) will introduce digital e-Passports with the capability to both read and write [16]. This will facilitate the e-Passport's accompanying application to store e-Visas and also entry/exit stamps that will support efficient immigration control. Technology has already advanced for users to use boarding passes stored in digital format in their smartphones as an alternative to paper format. Currently there are more than 1,000 million e-Passports in circulation, subsequently e-Borders and smart airports are emerging and developing at a faster pace.

4.3. Digital Authentication & Documentation

As described in Section 2, a digital identity may encompass multiple identities depending on the service that is being interacted with. In addition, these various digital identities may or may not link to or contain evidence of a subject's real-world identity [4]. This section explores the mechanisms by which individuals are able to authenticate their identity in the case of online transactions or digital system interactions. It explores the methods by which users my access a digital system, authentication to other users and also provide verification of their own identity when transmitting digital documents.

4.3.1. Identity Access Management. Digital Identity Access Management Systems (IAMs) refer to databases containing electronic records that allow users to access various types of organisational and online systems. These may be used by government organisations for official records or by business enterprises for employee records or authentication and access purposes. Authentication for these purposes is usually achieved via a username and password and may not necessarily link to the individual's real-world identity by way of personal identifiers. Instead it is a means by which users may verify that they have access to specific systems and online accounts. This area of identity authentication

is largely commercially developed by market leaders such as IBM and Microsoft, although many smaller companies offer identity and access management solutions.

A study conducted in 2015 estimates that the IAM market will increase from US$8.09 Billion in 2016 to US14.82 Billion by 2021. Major drivers in this area include compliance, process inefficiency and changes in technology trends. Another major driver is the increase in security breaches for global organisations; stolen employee credentials is the largest cause of breach incidents and it is predicted the global business cost will rise to US$2 trillion by 2019 [17]. This is inclusive of cloud-based options such as Identity-as-a-Service (IDaaS).

4.3.2. Identity as a Service. IDaaS refers to Identity and Access Management Services that are offered as part of cloud or Software-as-a-Service subscription-based products. This type of IAM solution contrasts with traditional solutions that operate entirely on-premises, self-managed and delivered through software or hardware means. Largely these solutions rely heavily on existing technology such as Active Directory (AD) and Lightweight Directory Access Protocol (LDAP).

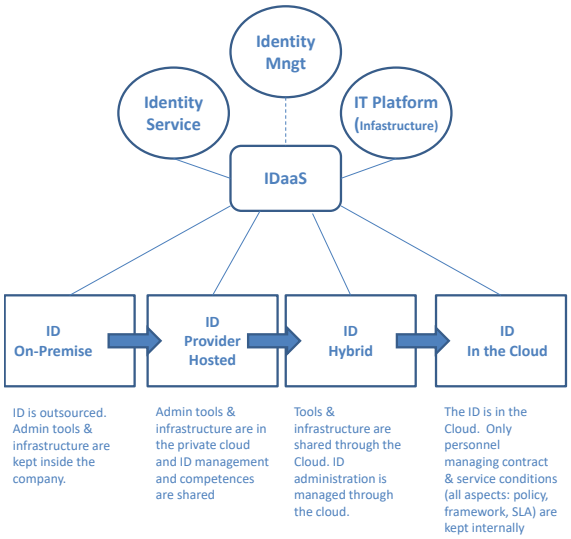

Figure 3. Identity as a Service

This is another competitive area in which market leaders and small technology companies compete. There are Hybrid solutions available from market leaders such as Amazon and Microsoft who provide a combined approach where cloud-based directories link with on-premises IAM systems.

4.3.3. Digital Signatures. Digital signatures are often confused with digital certificates, although they offer entirely different assurances, this form of digital identification is a mathematical technique used to validate the integrity and authenticity of a digital document. It may be viewed as equivalent to a handwritten signature or official seal, whereby offering assurance that digital documents have not been tampered with. It indicates details such as document origin, identity, status and informed consent of the signer. In many countries, including the United States, digital signatures hold the same legal clout as a handwritten signature.

The technique is based on public key cryptography such as RSA that links a private and public key. Solutions for a digital signature create a one-way hash that is subsequently encrypted using the private key. The included data, the encrypted hash and the hashing algorithm create the digital signature. The value of the hash is unique to the hashed data and any change in that data will result in a different hashed value. When the signature is decrypted using the public key and the hashes match, it verifies that the data has not been tampered with. These solutions are also part of a competitive market where market leaders and smaller technology organisations compete.

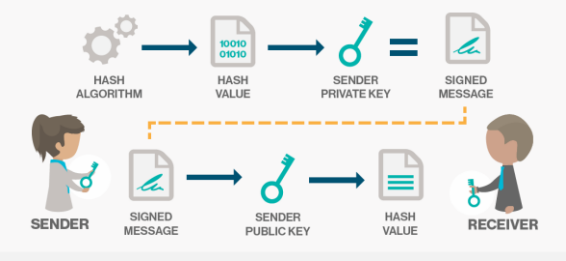

Figure 4. Digital Signatures

4.3.4. Digital Certificates. Digital Certificates are used for secure information transmission over the internet, acting as a type of digital passport for individuals and organisations. The technology relies upon public key infrastructure (PKI) and provides identifying information about the sending party. The security lies in forgery resistance, as the certificates can be verified with their trusted issuing third parties. The certificates contain details including the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key and the digital signature of the certificate issuing authority to allow the recipient to verify its authenticity. Typically, certificates are proven genuine and valid though a digital signature belonging to a root certificate of a trusted authority. Operating systems and browsers form lists of trusted certificate authorities' root certificates so they may more simply verify subsequent certificates.

The use of these certificates in combination with SSL encryption ensures authentication of the website that users are connecting to; information privacy during the communication cannot be viewed by unauthorised parties and information integrity ensures that the information accessed has not been

altered. This is another area where large and small technology companies compete.

5. Emerging Identification and Authentication Trends

As discussed in previous sections, there has been a major shift from traditional paper documentation (non-electronic) as proof of identity and also an increased need for identity authentication in online transactions. This has increased the need for electronic records required to support e-Government initiatives related to identity and has also improved the popularity of utilisation of off-premises cloud services such as IDaaS. The high prevalence of market leaders offering IDaaS has increased the popularity of this type of IAM and authentication.

5.1. Identity on the Blockchain

Another emergence is the use of blockchain for identity. Many organisations are now offering the utilisation of distributed ledger technology based upon the blockchain data structure as a new approach to identity management [18]. This has given rise to technology that may potentially up-end the current dominant approaches to storing and accessing digital identities in identity management [19]. As a characteristic of distributed ledger technology, this may successfully enhance the security, decentralisation, transparency and user control associated with transactions which include identity information. The landscape of Identity on the blockchain is currently being shaped by three main organisations, uPort [20], ShoCard and Sovrin [18]. This type of technology is intended to operate as an innovative approach to IAM, rather than replacing traditional paper documentation with a truly digital substitute.

5.1.1. uPort. This open source decentralised identity framework aims to provide identity management for decentralised applications on the Ethereum distributed ledger and also for more traditional applications such as online banking and email. Its structure is hinged on Ethereum smart contracts that provide a decentralised record of data movement. Identity is stored within two smart contracts defined as ‘user’ and ‘proxy’ templates. To utilise this application, users create an asymmetric key pair via a mobile application. This transaction is recorded on the Ethereum distributed ledger as a reference to the public key linked to the ‘controller’ template. The ‘proxy’ template contains a reference to the address of the ‘controller’ template. Once this is complete, only the controller template can invoke the functions of the proxy. The address of the proxy stores a unique uPort identifier. uPort securely maps identity attributes to a particular uPort identifier that is part of a registry of uPort identities. Any entity can query the register, but only the owner may modify the associated attributes. Files on the register are retrieved via their cryptographic hash.

5.1.2. Sovrin. This open source decentralised identity network is hinged upon a permissioned distributed ledger, meaning that although it is public, only permissioned nodes may take part in consensus protocols. These nodes are operated by trusted institutions such as banks, universities and governments. Governance of the operation is overseen by the Sovrin Foundation, a not-for-profit group via a legal agreement called the Sovrin Trust Framework. A user may generate a scaled number of required to contextual separate identities. Each identifier is controlled by a unique asymmetric key pair. The user themselves manages the identifiers via a decentralised identifier specification that stores the identifier itself, a cryptographic public key and associated metadata that allow transactions with that specific identifier to occur. The ledger contains the transactions associated with specific identifiers and is distributed among the permissioned nodes.

5.1.3. Shocard. This application uses distributed ledger technology to fuse a personal identifier with a traditional paper document such as a passport or driver licence and additional identity attributes within a cryptographic hash stored within Bitcoin transactions. This form of identity on the blockchain is used for manual verification of identity as well as online transactions. The Bitcoin element is used for timestamping of the signed cryptographic hashes that store the user’personal identifiers. The scheme incorporates a central server that acts as an exchange service for the encrypted identity data between a user and the reliant party. The mobile application creates an asymmetric key pair for each user and uses the camera to scan the traditional paper document. The scan and the associated data are then encrypted and stored on the device. The signed hash is then embedded into a Bitcoin transaction so that the date may be validated. The generated Bitcoin transaction number is utilised as the user’s ShoCardID and is stored in the mobile device as a pointer to the ShoCard verified seal.

5.2. Online Identity Verification and Trust

There has been a demonstrated requirement for individuals interacting in an online environment to not only prove their identity, but also prove their ‘trustworthiness’. This has encouraged a trend toward solutions that are capable of analysing attributes from a subject’s online interaction and produce a score indicating how trustworthy they are. As an example, *Trooly*, assesses the trustworthiness

and measure of 'real' information contained within a digital footprint. This company was acquired by AirBnB to assess the trustworthiness of individuals offering their properties for letting via an online service. However, this service does not provide a digital identification document.

Another alternative is a service called Hooyu that confirms identity in real time. When a user receives a request to prove identity via email or SMS, Hooyu sends the requesting party a confirmation report that confirms that the details they provided are correct. This is achieved by the user supplying Hooyu with a selfie image, an image of a traditional paper document and also their online credentials. The primary use for this service is personal financial transactions with individuals offering services online such as private temporary property rentals and the purchase of used goods.

6. Conclusion

This paper has offered a review of the history of identity, identification and authentication with a particular focus on modern implementations, current trends and emerging technology. As demonstrated, the requirement for proving one's identity has been present for many thousands of years and the methods by which this is achieved pays homage to the resources and technology that are available at the time. It has also been demonstrated that although 'identity' is an ambiguous and amorphous term that refers to something intangible, through documentation of unique personal identifiers, it is something that becomes quite tangible.

The research conducted has followed the development of identity, including the attributes and traits that are considered to contribute to it. These include standard personal identifiers such as name and date of birth, biometrics such as fingerprints and also social behavioural data such as relationships. The constructs of real and fake identities has been examined, indicating the risks associated with fake identities and how they are obtained and also pinpointed through identity resolution.

Increases in population and transient migration have necessitated a shift toward electronic and digitalised records that accompany electronic documentation such as e-IDs, e-Passports and e-Borders. This major move toward global digitalisation has come to exploit the use of the aforementioned personal identifiers and new biometric technologies. These technologies may still be considered two-factor authentication as they include a document containing a smart chip and an electronic record that is linked to a username and password.

Increased utilisation of online services has also necessitated a requirement for individuals to prove their real-world and digital identities through technologies such as IAM, IDaaS, digital signatures and digital certificates offering innovative approaches through ever growing and improving cloud service solutions.

Finally, emerging identity trends have shown an interest in providing measures of trust in a user. Further future-proofing technologies aim to utilise novel and innovative blockchain technologies to store identities, however these are for the purpose of IAMs and online transactions, not as a replacement for traditional paper documentation.

The clear message demonstrated through this research is that the trend is certainly leaning toward 'tangible' identification being phased out and replaced by a substitute 'intangible' digital representative. However, a true 'digital identification' alternative that proves a real-world identity without traditional paper documentation has not evolved as yet.

References

[1] J. Blue, J. Condell, (2017), 'Identity Document Authentication using Steganographic Techniques: The Challenges of Noise', Ulster University, 28th Irish Systems and Signals Conference, Killarney, Ireland.

[2] J. Blue, J. Condell, (2018), 'Identity Document Authentication using Steganographic Techniques: The Challenges of Noise', Ulster University, 28th Irish Systems and Signals Conference, Killarney, Ireland.

[3] M. Cavna, (2013), '"NOBODY KNOWS YOU'RE A DOG': As iconic Internet cartoon turns 20, creator Peter Steiner knows the joke rings as relevant as ever', The Washington Post, (online) https://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600 -f98d-11e2-8e84-c56731a202fb_blog.html?noredirect=on&utm_term=.1838265bcd92.

[4] National Institute for Standards and Technology, (2017), 'Digital Identity Guidelines', NIST Special Publication 800-63-3, June, 2017.

[5] G.A. Wang, H.C. Chen, J..J. Xu and H. Atabakhsh, (2006), 'Automatically detecting criminal identity deception: an adaptive detection algorithm', IEEE Transport Systems Management, Part A-Systems Humans 36, pp. 988–999.

[6] United Kingdom Home Office, (2002), 'Identity Fraud: A Study', (online) http:// www.homeoffice.gov.uk/cpd/id_fraud-report.pdf.

[7] H. Köpcke and E. Rahm, (2010), 'Frameworks for entity matching: a comparison'. Data and Knowledge Engineering, Elsevier, Volume 69, Issue 2, page 197–210.

[8] International organization for Standardization, (2011), 'Information technology -- Security techniques -- A

framework for identity management -- Part 1: Terminology and concepts', ISO/IEC 24760-1.

[9] European Parliament, (2018), 'Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC'.

[10] E.A. Whitley and I.R. Hosein, (2008), 'Doing the politics of technological decision making: due process and the debate about identity cards in the U.K.', European Journal of Information Systems, Volume 17, Issue 6, pp. 668–677.

[11] P. Seltsikas and R.M. O'Keefe, (2010), 'Expectations and outcomes in electronic identity management: the role of trust and public value' European Journal of Information Systems, Volume 19, Issue 1, pp. 93–103.

[12] D. Lyon, (2009), 'Identifying citizens: ID cards as surveillance' Polity Press, Cambridge, UK.

[13] E. Wihlborg, (2013), 'Secure electronic identification (eID) in the intersection of politics and technology', International Journal of Electronic Governance, Volume 6, Issue 2, pp. 143–151.

[14] U. Melin, K. Axelsson, and F. Söderström, (2016), 'Managing the development of e-ID in a public e-service context: Challenges and path dependencies from a life-cycle perspective', Emerald Insight, Transforming Government: People, Process and Policy, Volume 10, Issue 1, pp. 72–98.

[15] J.H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk and R.W. Schreur, (2006), 'Crossing Borders: Security and Privacy Issues of the European e-Passport', IWSEC 2006: Advances in Information and Computer Security, pp. 152-167.

[16] International Civil Aviation Organisation (ICAO), (2015), 'Machine Readable Travel Documents', Document 9303, Seventh Edition.

[17] Identity Management Institute, 2018), 'Identity and access management market analysis', (online) https://www.identitymanagementinstitute.org/identity-and-access-management-market-analysis/.

[18] Andrew Tobin and Drummond Reed, (2017), 'The Inevitable Rise of Self-Sovereign Identity', The Sovrin Foundation, September.

[19] U. Melin, K. Axelsson, and F. Söderström, (2016), 'Managing the development of e-ID in a public e-service context: Challenges and path dependencies from a life-cycle perspective', Emerald Insight, Transforming Government: People, Process and Policy, Volume 10, Issue 1, pp. 72–98.

[20] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena, (2017) 'uPort: A Platform for Self-Sovereign Identity'.

.