IDENTITY AND AUTHENTICATION

ITU-T FOCUS GROUP ON DIGITAL FINANCIAL SERVICES

International Telecommunication Union

ITU-T

FG-DFS

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(01/2017)

ITU-T Focus Group Digital Financial Services

Identity and Authentication

Focus Group Technical Report

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. TSAG set up the ITU-T Focus Group Digital Financial Services (FG DFS) at its meeting in June 2014. TSAG is the parent group of FG DFS.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

Identity and Authentication

About this Report

This report has been prepared by Consult Hyperion on behalf of the International Telecommunication Union (ITU) to identify and evaluate ID and authentication systems, both private and state-led for their use and impact on DFS and financial inclusion.

If you would like to provide any additional information, please contact Vijay Mauree at tsbfgdfs@itu.int

Table of Contents

List of Tables

List of Figures

Executive summary

This Technical Report to the ITU-T Focus Group on Digital Financial Services (DFS) presents an overview of the current and projected state of digital identity and authentication, as it applies to the DFS sector. It is intended to be read in the context of Recommendations ITU-T X.1252, ITU-T X.1253, and ITU-T X.1254, which address the wider issues around the management of identity in data networks.

The broader context is the adoption by world leaders on 25th September 2015 of the UN's 17 sustainable development goals (SDGs) of the 2030 "Agenda for Sustainable Development", of which Clause 16 states: "Promote just, peaceful and inclusive societies", which is further amplified with the clause: *"By 2030, provide legal identity for all, including birth registration"*. In the light of broader moves around the world to electronic/digital transactions, particularly in the DFS sector, it is inevitable that the best method of achieving this is through the creation and use of digital identities, through a variety of means. For this reason, the paper briefly explores the relationship between legal and digital identities.

The nature of digital identities is explored in this report, as well as a core definition of their usage presented, based on three phases:

- **Identity proofing** - the process of establishing the legal identity of an entity presenting him/herself for registration. At the successful conclusion of this phase, a digital identity is created and associated with the person.
- **Authentication** - the process (undertaken when the person *asserts* an attribute of their identity) of validating the assertion of an attribute associated with a previously established identity.
- **Authorisation** - the process of determining the degree of access to a service that may be provided on the basis of a previously asserted and successfully authenticated identity.

This includes provision for partial assertion; so an individual does not need to assert every attribute of their identity. For example, an individual might assert their name, and not their address or any other attribute – or perhaps that he or she is over 18 years of age, without being required to provide his or her name.

The paper then describes different types of digital identities, from the **foundational** identity, usually created as part of a national identity scheme, and is typically based on the formal establishment of identity through the examination of qualifying (breeder) documents such as birth records, marriage certificates, and social security documents. This can then be used in the creation of **derived** digital identities, such as a **transactional** identity which might be created during registration for DFS services, and used for customer authentication during DFS transactions, and for other service access as determined by the DFS operator.

After an overview of the importance of the level of assurance (LoA) associated with a digital identity, this paper briefly introduces the various forms of identity architecture that are being explored worldwide. These are explored in more detail in Appendix A.

In addition to architectures, a further complication is the class of digital identity used – either static or dynamic. A static digital identity is derived from the foundational identity and is one that is typically issued by a national identity scheme, or historically, by a bank. Its initial high LoA degrades over time (attributes such as address may change, for example), raising a requirement to re-check periodically – for example, the financial regulator in South Africa requires that banks' customers re-assert their address at least annually. An alternative that is being explored is the dynamic identity, which is initially self-asserted (as in a Facebook ID, for example) with a very low LoA, which can be developed over time – for example, by visiting a service provider and presenting supporting documents (like a passport) in order to gain access to an additional service. This approach can dramatically reduce friction around onboarding, though it does need careful management.

The technologies around digital identity are explored, specifically around the identity proofing, authentication, and authorisation stages of the lifecycle. In general, a specific focus is on authentication technologies; particularly around personal identification numbers (PINs) and biometrics. The reasons for moving away from PINs are explored, and the difficulties of moving to biometrics are highlighted as a set of technologies that are easy to use badly (often giving a sense of security that isn't really there), and difficult to use well.

These inputs are then used as inputs to an analysis of the use of digital identities in the DFS sector, considering first the 'traditional' approach with a customer who has a foundational identity document set. The paper cautions against relying entirely on the foundation identity for DFS transaction authentication, highlighting the consequent performance issues, and suggests the use of derived transactional digital identities for this purpose. With regard to customers without the necessary identity documentation, a way forward based on the use of dynamic digital identities is suggested, with the type of service that can be delivered linked directly to the LoA that can be achieved over time. It is recognized that further work is needed in this regard.

A number of examples of the use of digital identities with DFS services are explored, including a general example of the use of a foundational digital identity with the Groupe Speciale Mobile Association's (GSMA) mobile connect framework, and specific examples from Pakistan, South Africa, India, and Nigeria. The impact of digital identity on DFS in general, and on the barriers to adoption, are explored from the perspectives of the commercial models (increasing the potential customer base, reducing the cost of regulatory compliance, and creating a framework for the development of additional revenue streams), social and cultural issues (specifically including privacy concerns, balanced by the potential to enhance financial inclusion), and the regulatory impact (including the potential for increasing support for the FATF Risk-Based Approach, and the need for developments in the area of liability).

Finally, a number of recommendations are made:

Recommendation 1 At the time of registration, a DFS operator should create a digital identity for its customers, for use in both DFS transactions and (where relevant) in identity assertion with external service providers.

Recommendation 2 Where a customer is unable to provide a foundational document of digital identity, consider the issuance of a dynamic, self-asserted digital identity, which may be 'stepped up' over time and as required.

Recommendation 3 Regulators should standardize digital identity registration, and ensure interoperability between DFS operators and service providers relying on the digital identity.

Recommendation 4 DFS operators should build in customer privacy measures, compliant with national legislation either current or anticipated.

These recommendations are expanded on in the body of the document.

1 Introduction

1.1 Context

This paper presents a summary of the considerations around the development and use of identity and authentication services in digital financial services (DFS), with a specific emphasis on digital identities (also known as electronic identities, or eIDs).

This document should be read with reference to the following ITU Recommendations, which address the wider issues around the management of identity in data networks:

Recommendation ITU-T X.1252: "Baseline identity management terms and definitions"

Recommendation ITU-T X.1253: "Security guidelines for identity management systems"

Recommendation ITU-T X.1254: "Entity authentication assurance framework"

1.2 The UN and the 17 sustainable development goals (SDG)

Significant impetus to the development and deployment of digital identity systems and services has recently come from their adoption at a UN Summit on 25th September 2015 by world leaders of the 17 SDGs of the 2030 Agenda for Sustainable Development[1]. The SDGs build on the foundations of the millennium development goals (MDGs).

The 17 SDGs came into force on 1st January 2016, and signatory countries are expected to take ownership and establish a national framework for achieving the 17 Goals over the next 15 years.

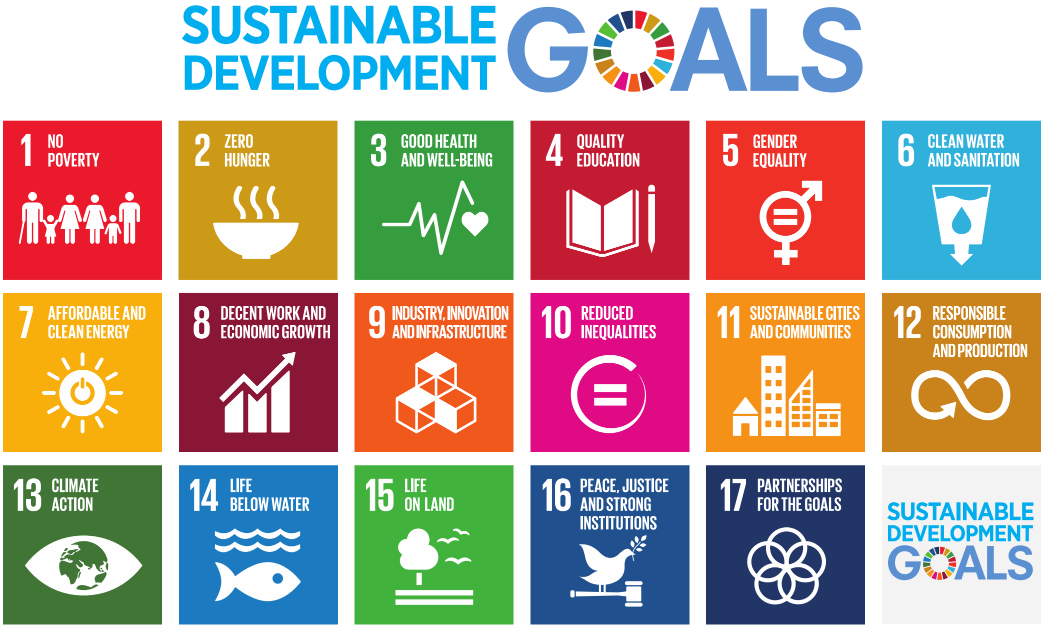
SUSTAINABLE DEVELOPMENT GOALS
1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS
SUSTAINABLE DEVELOPMENT GOALS

Figure 1 – The UN's sustainable development goals

Each of these goals has a number of clauses. Of particular relevance to this report is SDG Goal 16: "Promote just, peaceful and inclusive societies", and specifically the clause: *"By 2030, provide legal identity for all, including birth registration"*.

[1] http://www.un.org/sustainabledevelopment/

The implications of this goal; the embodiment of a legal identity as a digital identity; and the implications for DFA and financial inclusion, are the subjects of this paper.

1.3 Legal identity, digital identity, and DFS

Across the industrialised world, the issuance of birth certificates and the registration of deaths are generally well-established, formal processes. These typically follow a similar pattern, in which attending midwives or other medical staff issue a 'birth notification' document to the mother (and typically also notify the registration authorities, together with any information about the mother that they hold). The parents are then required to present themselves to the public registration authorities within a set time period of perhaps one or two months, in order to formally register the birth, including notification of parental relationships and home address. It is this registration that is at the root of legal identity.

However, there are complications in many emerging economies, due to non-issuance of birth certificates; for example, according to a UNICEF report on Nigeria (2007):

> *"….in urban areas, approximately 50 percent of births are registered, while in rural areas, only about 21 percent are registered (UN July 2007). Low registration rates in Nigeria have been attributed to a number of factors, including lack of awareness of current legislation and of the importance of birth registration, limited number of registration centres, limited financial resources and a lack of effective registration infrastructures".*

In many cases, there are strong correlations between communities that are already at the fringes of society and those who lack proper birth registration. This creates a wide range of issues[2], ranging from non-issuance of national identity cards - to problems with immigration into Western countries such as the United States, and of course financial exclusion.

But the problem in many cases is not necessarily limited to registration difficulties. There are often issues with the accuracy of information held on birth certificates, due to the prevalence of multiple languages and the representation of those languages in written form. For example, in Kenya, which has a relatively well organised system in which medical facilities provide a birth notification card, followed by birth registration at the local town hall (other arrangements are in place for births that take place outside medical facilities), there are occasions when discrepancies occur. For example, a parent's identity card might have a different spelling of the parent's family name from the child's family name on the birth certificate. This can give rise to problems in later life with the claiming of inheritances from parents, the issuance of identity and voters' cards, and, of course, passports and international travel. Even data such as birth dates and marriage certificates may be problematic and many registries have special investigation teams for issues like allegations of bigamy, proposed corrections to the records (including revised paternity details), etc.

It is in response to these issues, and perhaps in some cases with fulfilment of the commitment to the SDGs in mind, that many countries without comprehensive registrars of their citizens are seeking to create formal national identity programs. These programs typically involve a number of steps to register citizens, including at a minimum:

- formal identification of the citizen, through a range of country-specific means;
- the creation and issuance of an electronic or digital identity, held in a central database or on an identity card held by the citizen.

In addition, the capture or creation of a means of authenticating the citizen (that is, that the person presenting themselves with a digital identity is the person to whom the digital identity was originally

[2] http://blogs.lse.ac.uk/humanrights/2015/05/28/questions-of-legal-identity-in-the-post-2015-development-agenda/

issued) forms a part of the registration process, and may include biometrics, PINs, and other authentication technologies.

Independently of state-issued digital identities, there is a need to identify and authenticate customers for access to DFS. This is typically achieved through the creation of a digital identity, but in order to satisfy national financial regulations and international know your customer (KYC) obligations, it is necessary to undertake a number of validation steps at the time of registration – ideally this is based on a national identity service, preferably one that allows presentment and validation of a government-issued digital identity. However, an emerging option is to have self-asserted identity attributes validated at a later stage by a governmental or non-governmental organization.

Where no such national identity service exists, registration of customers for DFS is necessarily more complex. This paper considers the issues in this area and makes a number of recommendations.

2 What is digital identity?

Robust identification systems are crucial for inclusive and prosperous economic and societal growth. Yet in the developing world over 2 billion people lack formal means of identification[3]. Historically, paper-based systems and physical documentation such as national identity cards and birth certificates have been issued in order to allow individuals to interact with government organisations during official transactions. However, the use of these types of mechanisms is often flawed, with a lack of ubiquity and ease of counterfeit being commonplace. According to a 2007 UNICEF report, as many as 70 per cent of the five million children born annually in Nigeria at that time were not being registered at birth[4] - notwithstanding improvements that may have been made over the intervening nine years, those people unregistered at birth face being economically disadvantaged for life, if steps are not taken to address their circumstances.

Advances in identification technologies have provided the opportunity to migrate paper-based systems to digital identity mechanisms. The utilisation of identity via digital means or "digital identity" has the potential to enable a wide range of potential benefits and to address many of the issues around financial inclusion.

2.1 Core definition

Articulation of the term "digital identity" can be found in various forms, though typically centred on the same theme. The ITU definition of digital identity is provided in Recommendation ITU-T X.1252. Within the scope of this paper, we use the term digital identity to define the various mechanisms of asserting and verifying personal data attributes in the context of digital services and transactions. At a high level, it can be described as a composite of three processes: Identification, authentication, and authorisation. The logical relationship between these processes is illustrated in Figure 2.

Identification, authentication and authorisation are defined as follows:

- **Identity proofing** (as defined in ITU-T X.1254; often less accurately termed "identification"): This is the process of identifying an individual or organisation (as defined in ITU-T X.1252), and formally *establishing* the veracity of that identity. It may involve examining "breeder documents" such as passports and birth certificates, consulting alternative sources of data to corroborate the identity being claimed, and potentially collecting biometric data from the individual.

[3] http://pubdocs.worldbank.org/en/205641443451046211/ID4D-IntegrationAproachStudyComplete.pdf

[4] http://www.unicef.org/nigeria/children_1930.html

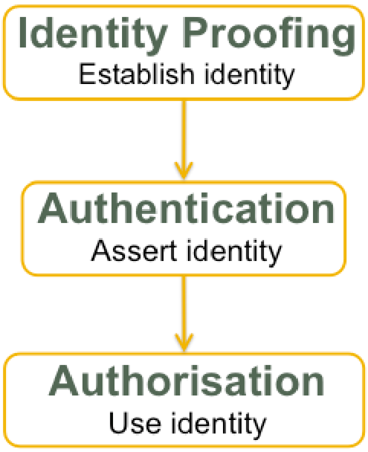

Figure 2 – Digital identity high level process

- **Authentication (**as defined in ITU-T X.1252**)**: This is the process of *validating the assertion* of an attribute associated with an identity previously established during identification. Typically, this involves presenting or using an authentication credential (that was bound to the identity during identification) to demonstrate that the individual (or organisation) owns, and is in control of the digital identity being asserted.
- **Authorisation**: This is the process of *determining* what actions may be performed or services accessed/provided on the basis of the asserted and authenticated identity.

2.1.1 Partial assertion

For government and financial services, the set of identity attributes that need to be established and asserted is usually fixed, including, for example, name, address, and date of birth. There are many services where such a fixed set of attributes is not required. For example, access to age-restricted services may only require determining that the individual is over 18, and personalisation of a retail service may only strictly require information about product preferences (although often retailers are keen to acquire significantly more data).

The ability to assert only the data that is necessary to enable the transaction is referred to as "minimal disclosure". Privacy-respecting digital identity systems often place a great deal of focus on this requirement. More generally, with the increasingly diverse range of digital services that individuals use, there is a growing need for individuals (and the devices they own) to be able to share specific items of data within differing levels of assurance requirements, relevant to the context and shared under their control.

2.2 Derived digital identities

Iteration of the process outlined in Figure 2 can be performed to derive different classifications of digital identity. The identities created during these iterations may be for specific transactional purposes or use within certain domains such as banking or healthcare. Typically, a core or "foundational" identity – usually governmental, and intended to be used for multiple purposes – is used to establish credentials for a derivative digital identity, described as either "functional" or "transactional", which in turn is intended to be used in the context of a particular service. The different classifications identified are:

- **Foundational**: A core digital identity (such as the Aadhaar programme[5] in India), usually created as part of a national identity scheme or similar, which is based on the formal establishment of identity through the examination of qualifying (breeder) documents such as birth records, marriage certificates, and social security documents. Such a digital identity typically enables a wide variety of government services, and sometimes extends further.
- **Functional**: A digital identity (such as the voter registration programme[6] in Ghana) which is created to address the specific needs of an individual sector, such as healthcare.
- **Transactional**: A digital identity (such as the Consult Hyperion Token Administration Platform (TAP) programme[7] in Nigeria), which is intended to ease the conduct of financial or other transactions (either face to face or across the Internet) across multiple sectors.

A state-issued eID acts as a strong, reliable foundational identity. However, there are a number of additional use cases that require more flexible or extensible identities, and the functional or transactional identities, derived as they are from the foundational state-issued eID, can fulfil this role.

2.3 Level of assurance

Level of assurance is a measure of the quality of a digital identity, based on: (1) the quality of the steps taken to verify the claimed attributes; and (2) the robustness of the authentication credentials established. It provides assurance that the identity was correctly assigned, and that the entity asserting a particular identity is the entity to which that identity was assigned.

As defined by ISO/IEC 29115, there are 4 LoAs:

- **LoA 1**: Minimal confidence in the asserted identity of the entity, but enough confidence that the entity is the same over consecutive authentication events. LoA 1 is used when minimum risk is associated with erroneous authentication. There is no specific requirement for the authentication mechanism used; only that it provides some minimal assurance.
- **LoA 2**: Some confidence in the asserted identity of the entity. LoA 2 is used when moderate risk is associated with erroneous authentication. Successful authentication will be dependent upon the entity proving, through a secure authentication protocol, that the entity has control of an agreed credential. LoA 2 implementations often make use of second factor authentication (2FA), such as demonstrating access to a registered mobile phone.
- **LoA 3**: High confidence in an asserted identity of the entity. LoA 3 is used where a substantial risk is associated with erroneous authentication. Identity proofing procedures shall be dependent upon verification of identity information. An LoA 3 implementation might for example extend 2FA implementations, by requiring the entry of a PIN into a registered mobile phone.
- **LoA 4**: Very high confidence in an asserted identity of the entity. This LoA is used when a high risk is associated with erroneous authentication. LoA 4 provides the highest level of entity authentication assurance defined by this standard. LoA 4 is similar to LoA 3, but it adds the requirements of in-person identity proofing.

The trust that is placed in a digital identity by a system or service should be based on the LoA associated with it. However, that trust is exclusively within that system/service and across the federations participating within that system/service.

[5] https://fxb.harvard.edu/indias-aadhaar-program-a-legitimate-trade-off-between-social-protection-and-privacy/

[6] https://eisa.org.za/wep/gharegistration.htm

[7] http://www.chyp.com/token-administration-platform-tap-e-goods-delivery/

2.4 Digital identity architectures

Deployments of digital identity systems in countries around the world, including emerging markets, have been met with varying levels of success. We have identified a number of high level architectures of the systems deployed in these countries (both current and planned) and analysed their associated characteristics as relevant to applications within DFS. The high level architectural models identified are:

- monolithic identity provider (IDP) architecture,
- federated Internet IDP architecture,
- state-issued eID architecture,
- brokered IDP architecture,
- brokered credential service provider architecture,
- personal IDP architecture,
- no IDP architecture.

The ordering of the subsections embodies a hierarchy of consumer control and privacy. This ranges from consumers having relatively low levels of control over how their data is used in the monolithic IDP model to ultimate control in the no IDP architecture.

The intricacies of these architectures are presented in Appendix A.

2.5 Types of digital identity

2.5.1 Conventional / static

Conventional approaches to digital identity have generally revolved around the creation of a static digital identity, hosted in a token such as a smart card. This approach is taken in the rollout of many national eID schemes and in conventional KYC processes.

State eIDs are normally issued in order to provide access to government services. They can also serve as official documents providing access to other services, such as KYC for financial services. As a consequence, these identities are high value, and could potentially be used to enable fraud, if compromised, and so become targets for attack.

The majority of state eID systems start off with the issuance of a smart card. This is a static technology that does not integrate well with Internet-based services, due to the need for an additional, trusted interface device: A card reader (though this need can be obviated through the use of a contactless smart card and near field communication (NFC)-capable smart phone, but this is not currently a mass market solution). Similarly, for PC-based online access, it has been necessary to provide the user with an expensive reader in order to use the smart card. Consequently, eIDs are often not integrated as widely into third party services as had been intended.

Identifiers may or may not be linkable. Austria's[8] Citizen Card is an example of best practice in this regard, as the card carries multiple sector-specific identities, derived from the government-issued identity number and individually cryptographically protected. This greatly enhances privacy, as it prevents the matching of individuals across their use of multiple services, whilst also enabling the simple revocation and replacement of encrypted identifiers in case of fraud.

In contrast, "smart" identifiers, where the identifier includes personal information (such as the UK driving licence number which includes part of the citizen's name and date of birth), clearly enable

[8] http://www.buergerkarte.at

both disclosure of personal information and linkability. So, there are clear privacy issues with smart numbers, particularly if a person's date of birth is used as part of the security checks for other services.

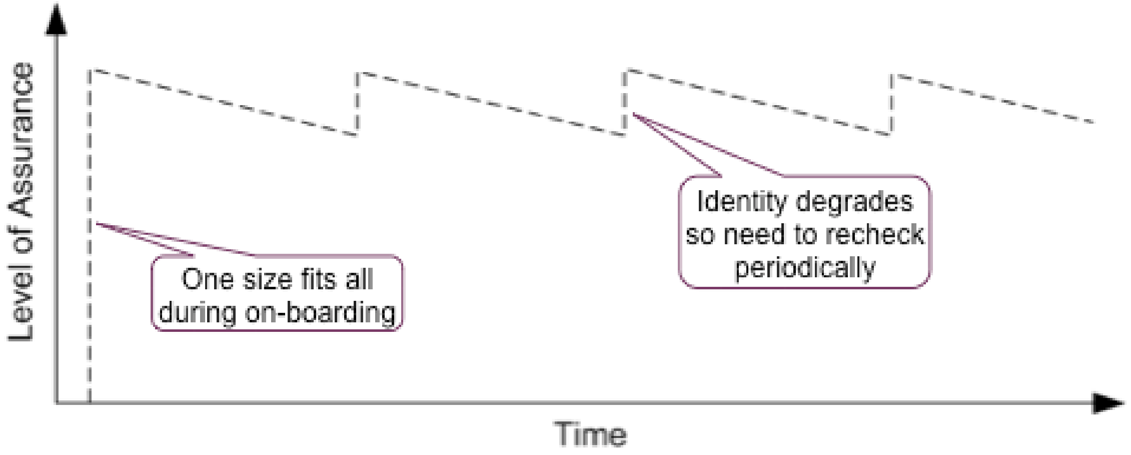

Figure 3 – Confidence in static digital identities over time

The static nature of these identities leads to concerns around their long-term adequacy and quality. The consequence of this is that they need to be periodically re-verified if they are to be trusted, as is the case, for example, with the financial regulator's requirement for a periodic re-verification process in South Africa. The varying quality of static digital identities over time is illustrated in Figure 3.

Static digital identities are, of course, an important element in a national digital identity infrastructure, as a foundational identity forming an official document for access to government services, border control, etc. However, it is increasingly the case that more dynamic approaches need to be considered, easing the onboarding process and reflecting day to day usage, as outlined in the next section.

2.5.2 Online / dynamic

The second broad class of digital identities, online or dynamic identities, originate in the Internet corporations' need to build a profile of individuals, which can be extended by creating identities that can be linked to and used by other services. An obvious example of this is Facebook Connect – though this self-asserted, social identity must be regarded as having a LoA 1 associated with it.

In contrast to the hierarchical approach to establishing a conventional or static digital identity, illustrated in Figure 2, the creation and development of a dynamic digital identity is an iterative process, as illustrated in Figure 4.

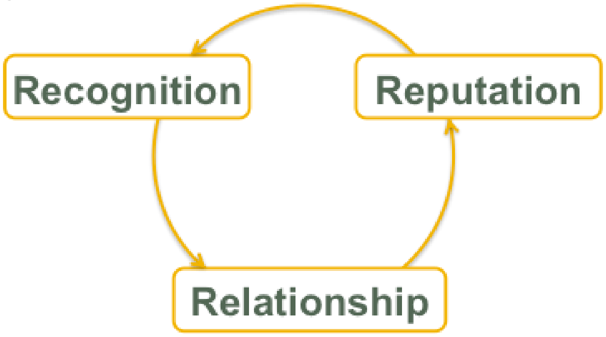

Figure 4 – Lifecycle of a dynamic digital identity

These identities are self-asserted, meaning that the individual states their identity, and therefore they offer – initially at least – a low level of assurance (LoA 1). However, over time, repeated usage, and the addition of further attributes (verified mobile phone numbers, passport numbers, perhaps validated and certified at the time they are added by a governmental or non-governmental authority), sponsorship by other citizens with stronger digital identities (similar to the social graph model), and frequency and longevity of use, confidence in that assertion grows, as illustrated in Figure 5. This might be supplemented by specific checks for services that require a level of assurance beyond that currently offered by the digital identity. An example might be strengthening the assurance associated with the digital identity through the use of 2FA using a mobile phone, which as well as mitigating the risk of account takeover, also strengthens the level of assurance by adding a verified data attribute – a mobile phone number. This dynamic approach has the advantage that the necessary checks, and the associated expense, need only be undertaken once it becomes necessary for service access – an approach commonly known as **stepping up**.

An important characteristic of this form of digital identity is the use of multiple sources (including, but not limited to, the individual's mobile phone, their social media activity (also known as their 'social graph'), pattern of usage, location, etc.) can all feed into the level of assurance, so continuous assessment and monitoring is essential. Such an approach has clear synergies with the risk-based approach used by financial service providers.

By diligent and continuous application of these techniques, issues such as fake social identities can be addressed, though it is as yet unclear what LoA might commonly be achieved using this approach.

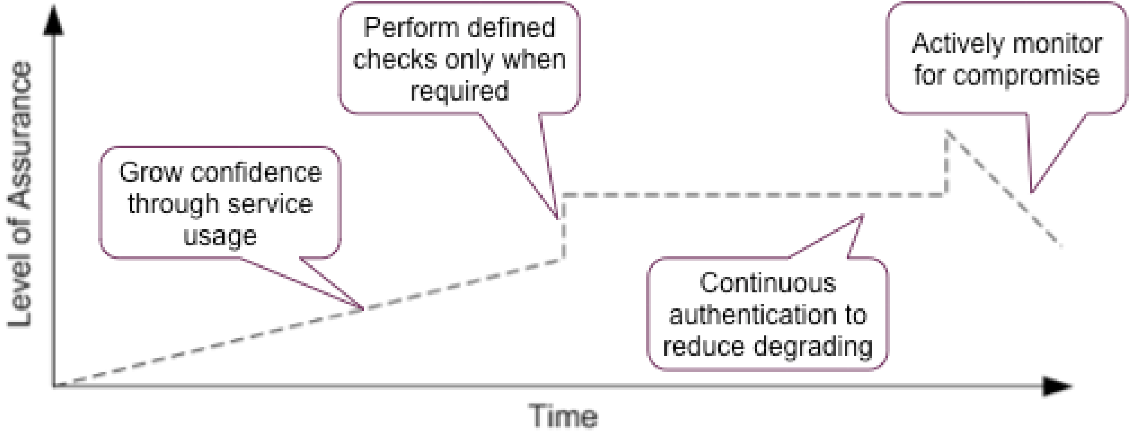
Level of Assurance
Time
Grow confidence through service usage
Perform defined checks only when required
Continuous authentication to reduce degrading
Actively monitor for compromise

Figure 5 – Changing LoA of a dynamic digital identity

The dynamic approach to digital identity building has a number of key advantages over the static approach:

- There is considerably reduced friction around onboarding, as an initially self-asserted identity has few barriers to entry.
- It presents new ways for a citizen to build reputation, and so grow confidence in the quality of the digital identity.
- It's better for financial inclusion, as it enables identification and the consequent level of assurance to grow over time, as needed to access new services, which in this market is preferable to the initial 'all or nothing' approach.
- It enables better fraud control by making good use of data through active monitoring – always assuming that data protection and privacy requirements can be met.

However, these advantages should be balanced with the reality that there are currently no clearly defined metrics for measuring the strength or assurance of dynamic identities. Without detailed analysis, it is not clear that this approach will be reliable enough to meet strict KYC and anti-money laundering (AML) requirements.

3 Technology supporting digital identity

Digital identity dictates the use of various solutions to satisfy the requirements of its generic architecture. Annex A identifies technologies that are used to support either identification, authentication, or authorisation activities. This section looks at key examples from this list and analyses their strengths, weaknesses, and applicability as relevant to DFS.

3.1 Identification technologies

Establishing an individual's identity during registration for DFS can be one of the most significant barriers to adoption when trying to drive inclusion. The process of registration can be slow and cumbersome, and is often impaired by low income and rural demographics being unable to meet qualification requirements. New and emerging technologies alongside the FATF RBA present an opportunity to overcome these issues.

3.1.1 Unstructured and structured data analytics engines

The practice of analysing aggregated data in order to draw insight from personal information is gaining momentum within the financial services industry. GO Finance in Tanzania leverages digital data to underwrite loans for small and medium-sized enterprises[9]. Konifo, from Mexico, is another example which uses credit algorithms based on alternative data sets to extend the same services[10].

Although much of the hype surrounding the use of this technology is centred on data from social media, low penetration among target demographics does not necessarily dictate a lack of usable information. Any existing services that facilitate the potential for individuals to produce a digital footprint can be leveraged for identity.

Typically, platforms capable of establishing data attributes from alternative sources can be measured according to a two factor criteria:

1. Their ability to **capture** and **structure** useful information from traceable interactions between individuals and software.
2. Their ability to **draw insight** from the aggregated data they collect: including the relationship between individual data attributes and links between the attributes of separate entities.

As connectivity improvements increase the scope of available data, the use of analytic engines within developing economies will become a progressively valuable prospect. However, the integrity of the calculations used in order to establish a level of assurance around a consumer's identity is critical. It is unlikely that parallel mechanisms for converting unstructured data into an identity will be the same. Therefore, regulators will be required to establish complex benchmarks in order to satisfy international and domestic obligations on AML monitoring and counter terrorism funding (CTF) prevention. Adequate protections around user privacy will also have to be established.

In order to meet the demands imposed on regulatory authorities by this type of technology, parallel investment in tools that allow regulatory compliance to be adequately monitored whilst also ensuring compliance with privacy obligations is crucial if the technology is to achieve widespread acceptance.

Examples	Hello Soda[11] Konifo[12]

[9] https://cfi-blog.org/2015/10/13/the-data-story-in-the-fi2020-progress-report-on-credit-reporting/#more-19663

[10] https://konfio.mx/

[11] http://hellosoda.com/

[12] https://konfio.mx/

3.1.2 Image processing software

Image processing tools can alleviate the need to manually verify the genuineness of paper identity documents. However, the extent to which providers of DFS could benefit from this type of system depends on the capability of the software and the level at which it is deployed. For example, during the customer and agent registration processes for mobile money, time and cost is wasted processing applications which do not satisfy registration requirements, and image processing software could improve efficiency, depending on how providers chose to enable access to it:

- **Image processing for administrators**: When used as part of an administrative management (back office) suite to verify that genuine documents have been submitted as part of customer or agent registration; the technology can save time by automating what would otherwise be a manual process, but will not necessarily stem the flow of ineligible documents being submitted.
- **Image processing for agents**: When deployed at the agent level, greater time and cost efficiencies may be achieved through a reduction in false or ineligible document submission, however submitted customer applications may still be rejected on the basis of validity (i.e. individual is blacklisted on authoritative database). Call outs to 3rd party databases in order to prevent this are possible, but (unlike straightforward rejection of false or ineligible documents, which can happen offline) would require Internet connectivity at the point of registration, and in any case, are unlikely to be an appropriate function for agents.

Examples	Aut10tix[13], Jumio[14], Mitek[15].

3.2 Authentication technologies

Authentication technologies provide a filter allowing only legitimate entities to assert the attributes established during identification. In addition, low literacy levels in emerging markets exacerbate usability requirements.

3.2.1 PINs

The PIN is the authentication technology that almost all payments in the industrialised world currently rely on (though there is a gradual evolution towards biometrics, in the form of Apple Pay, Android Pay, et al). Similarly, almost all mainstream DFS providers currently rely on PINs for customer authentication.

However, there is a commonly held view that many of those at the bottom of the pyramid (BoP) cannot use PINs reliably, due to illiteracy, innumeracy, lack of familiarity, etc. It is likely that in most cases the issue stems instead from low frequency of use, since many of these customers will access financial services infrequently – perhaps as little as once every three months, or even less. Since frequency of use is linked to memory, it should come as no surprise that PINs are forgotten. Further, the lack of use leads people to write their PINs down, often on the back of the card or even the mobile phone they're using. This naturally leads to PIN compromise.

Alongside this, it would appear that global and national fears around terrorism are beginning to have an effect on PIN use, as the regulatory authorities in a number of countries are deciding that a PIN is not enough, for at least some financial transactions. For example, in India – and soon in Pakistan – online biometric authentication for bank transactions, based on Aadhaar, is becoming the norm.

[13] http://www.au10tix.com/

[14] https://www.jumio.com/

[15] https://www.miteksystems.com/

Further, the 2015 terrorist attacks in Paris were reported to have been financed using prepaid debit cards, which reflects a broader issue with payment cards in that one person (who passes KYC checks) can acquire the card and top it up, whilst another person uses the funds, with the PIN being forwarded in some way alongside the card – perhaps by post. This is very difficult to track, and raises the possibility of the increased use of biometric verification of cardholders, to ensure that the person who registered and passed the KYC checks is the person who uses the card. This was further evidenced by the announcement[16] that the Payments Association of South Africa (PASA), in partnership with Visa and Mastercard, is seeking to introduce biometric authentication of payment cards in South Africa.

3.2.2 Smartcards

Smartcards are widely recognised as a robust solution for authentication, however widespread use within DFS is limited by the ubiquity and reliability of the acceptance network. In markets where card acceptance infrastructure is not well developed, the additional costs associated with issuing devices to agents and then training them how to use them can also create a barrier.

Examples	Nigeria eID card[17]

3.2.3 Biometrics

Biometrics is an umbrella term for a set of complex technologies that seek to identity individual people by their physical or behavioural characteristics for the purpose of identification or authentication/service access. The different biometric technologies have varying strengths and weaknesses, and an important aspect of their use is the selection of an appropriate biometric for the intended purpose.

A biometric measurement is expressed in a computer system as a biometric template, or profile, which is a statistical analysis of the measurement, resulting in a specific reduced data set that can be used to represent the physical characteristics or features of an individual. It is important to emphasise that, for example, a fingerprint template is not the same as a fingerprint.

In all cases, biometric technologies are easy to use badly (often giving a sense of security that isn't really there), and difficult to use well.

3.2.3.1 Why biometrics?

Biometrics is a subject of particular relevance to financial inclusion in general, and DFS in particular. It has the potential to fulfil the basic need for customer authentication when accessing services, and overcomes two of the main shortcomings of the more conventional PIN, as described above.

For these reasons, and in view of the increasing sophistication and reliability of biometrics as the technologies advance, it is likely that biometric technologies will form an increasingly significant part of financial services offerings not just in the emerging economies, but in the industrialised world as well. This is despite the complexities and potential misgivings highlighted in this document.

3.2.3.2 Complexities

Biometric technologies are often regarded as a magic bullet. Unfortunately, this is not the case – they are a set of highly complex technologies, which need careful management if they are to be effective. The principle issues are:

[16] http://www.fin24.com/Tech/Companies/fingerprint-authentication-coming-to-sa-bank-cards-20160726?isapp=true

[17] http://www.nimc.gov.ng/

- **Registration**: It can be difficult to successfully register people, if the equipment is less than perfect, the environmental conditions are less than ideal, or if the selected biometric is inappropriate for the people being registered. The result can be poor quality registrations, which cannot be used to reliably, or robustly, authenticate the registered person at a later date. Unfortunately, it is likely to be the case that the poor quality of registrations is not apparent to the relying parties, and are used in live service.
- **Purpose**: Different biometrics might be used for different purposes. For example, a facial biometric might be used for de-duplication at the time of registration, whilst a fingerprint might be used for subsequent authentication.
- **Biometric selection**: It is important to choose an appropriate biometric. For example:
  - Fingerprints are used very successfully with young office workers, but will not work reliably with older manual workers, or those living in an arid environment.
  - Finger vein appears to be reliable and easy to use with all sectors of the population, but the equipment is expensive, and some versions of the equipment require the customer to place their finger into a small tube – which many people are reluctant to do.
  - Palm vein has gained traction in some markets for use at ATMs, and appears to achieve customer acceptance. However, the equipment is expensive and relatively bulky, so integration into an ATM may be the only practical use case.
  - Face and iris biometrics can be reliable with a camera of sufficient quality, but environmental conditions – poor lighting, lack of contrast, inappropriate backgrounds – can make their use less reliable. However, the increasing quality of smart phone cameras make these biometrics increasingly attractive.
- **Liveness checks**: These are essential – for example, checking for a heartbeat, or body temperature, or a blink.
- **Risk**: There is an obvious and substantial risk that, if an individual's biometrics are compromised, they can be used by an attacker to impersonate that individual. Because of the nature of the biometric, there is no prospect of revocation of that biometric credential.
- **Centralised or distributed**: Related to the **risk** issue is the decision on where to store the biometric data, a decision which is based on the particular use case and the associated risk and privacy rules.

  When stored centrally, biometric data can present privacy and security implications. Whereas alternative forms of authentication, such as password credentials, can be changed in the event that data has been compromised, biometric profiles are consistent, at the very least, within the domain that they were initially captured. Once an individual's biometric information is compromised, its usefulness within future services may be limited.

  When stored locally on personal devices, the consequences of breach are less severe and transactions can be processed locally. However, use cases for the information may be restricted to authentication only.
- **Disease**: There are concerns that the contact nature of many readers (fingerprints, finger/palm vein in particular) can cause disease transmission – for example in the recent Ebola epidemic there was understandable resistance to the use of fingerprint readers for cash transfer (DFS) services. Of course, the same applies in principle to PIN entry systems, but in that case gloves can be worn.
- **Security**: It is important that the registered biometric is stored in a secure manner, since compromise renders it useless due to the potential to replay it for service access. One solution is to store it on a suitably-secured device in the possession of the registrant, such as a smart

(digital identity) card or a secure enclave on a mobile phone (for example, the subscriber identity module (SIM)). Alternatively, it can be stored centrally in a highly secure server facility for later online authentication. However, since there is of course no such thing as perfect security, the latter approach raises the possibility of a population-wide compromise of biometrics, rather than the compromise of a single individual's biometrics if the distributed approach is used.

3.2.3.3 Accuracy

A biometric system needs to have an acceptable level of accuracy that can be defined in an unambiguous manner. As highlighted above, a biometric template is only a statistical representation of a physical feature, not the feature itself; so a fingerprint template is not a fingerprint. By its nature, a statistical system is not 100% accurate and deviations from the ideal occur.

The accuracy of the biometric solution is measured by three metrics: (1) failure to enrol (FTE) rate; (2) false rejection rate (FRR); and (3) false acceptance rate (FAR). These are described below. Although the accuracy issues described may represent a small proportion, when scaled to a population, accuracy issues can affect a great many people.

FTE

The FTE rate is the percentage of people who fail to be enrolled successfully into a biometric system.

A notable FTE problem is associated with fingerprint biometrics, because a percentage of the population have unusable fingerprints for measurement due to imperfections, wear, or being an amputee. This is particularly an issue with a population in a dry, dusty environment, manual labourers (including farmers), smokers, and older members of society.

FRR

The FRR is defined as the percentage of verifications in which an incorrect verification or false rejection occurs – that is, people whose attempt to verify themselves fails even though they are in fact the registered person. For example, if the FRR is 0.1 per cent, it means that on average, out of every 1000 persons attempting to access the system, one will not be recognised by that system.

It is important to note that the occurrence of an instance of false rejection may result in denial of service to a valid user.

FAR

The FAR is defined as the percentage of verifications in which an incorrect or false acceptance occurs. For example, if the FAR is 0.01 per cent, it means that on the average, one out of every 10,000 impostors attempting to breach the system will be successful.

It is important to note that the occurrence of an instance of false acceptance may result in access to a service being granted to the wrong person, in impersonation of another person.

Service requirements for accuracy

For any biometric technique, there is a direct relationship between the failure rates for FRR and FAR – that is, decreasing one rate increases the other. This means that for a specific service a trade-off must be made between the settings for FRR and FAR. The trade-off made will depend on the application; for example, in financial services, it may be most important for rejections to be low, while in a government identity scheme, the opposite may be true.

This trade-off is a decision that the organisation deploying the service elements must take. If a service is relying on someone else's biometric readers (for example, fingerprint readers built into mobile phone handsets) then the service may not be able to decide on the balance between failure rates and may have to adjust their policies to accept the reader owner's selection.

3.2.3.4 Necessary developments

The benefits of the prevention of dual registrations, as well as convenience are driving the use of biometric technologies in public identity schemes such as Aadhaar, NIMC, and NADRA. However, ubiquitous adoption within both the private and public sector in the future is likely to be dependent on a number of key developments:

- **Quality of data captured**: The quality of the data captured by biometric technologies has to be appropriate to the intended use for that data. In the case of biometrics for identification activities for example, the data captured has to be sufficiently unique to distinguish it from all other profiles within a given ecosystem. However, for use in authentication, the data collected may only need to be sufficient enough to confirm a 1:1 match. Failure to meet an appropriate balance between quality and intended use has the potential to shape consumer opinion on the use of biometrics in the future and ultimately adoption of them.
- **Centralised or distributed**: The decision of where the biometric data is held (see section 1.3) is influenced by use cases and risk, and privacy rules. A decision is also dependent on ongoing developments – such as is the case with some services that carry out biometric authentication on a client personal device, and then generate and deliver a cryptographic token with a claim about the authentication result, rather than the biometric itself.
- **Usability and reliability**: One of key benefits of biometric technologies to the developing world is presented by a reduced dependency on alphanumeric inputs. This has the potential to promote inclusion among low literacy demographics, provided the accompanying mechanism is sufficiently usable.

  For example, the UIDAI's biometrics standards committee in India published a report in 2009 advising that the use of fingerprint recognition may present challenges for people engaged in manual labour[18]. This is particularly relevant in developing economies where a large proportion of the population resides in a rural environment. In Africa, rural communities constitute 46 per cent of the total population[19].

Examples	Safran[20], Crossmatch[21]

3.2.4 Mobile phone technologies

Mobile penetration has seen continued growth with more than 4.7 billion unique subscribers recorded in 2015 globally[22], up from 3.6 billion at the end of 2014[23]. As increases in data connection speeds converge with the proliferation of new capabilities on personal devices, the use of the mobile phone for authentication is becoming increasingly important. In particular, the use of the SIM is of specific interest within DFS due to its ubiquity within the target market and its capacity to securely store cryptographic keys. Assuming use of the SIM is readily accessible, the technology could enable a user's control over a digital identity without the need for an additional form factor.

[18] https://authportal.uidai.gov.in/static/role_of_biometric_technology_in_aadhaar_authentication.pdf

[19] http://www.geohive.com/earth/pop_urban.aspx

[20] http://www.morpho.com/

[21] http://www.crossmatch.com/

[22] http://gsmamobileeconomy.com/

[23] http://gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf

However, the secure hardware in the SIM is typically controlled by mobile network operators (MNOs), and as such, commercial relationships may need to be established before utilisation of its capabilities for digital identity. Furthermore, in models which involve the use of a 3rd party controlled secure element, access is ultimately subject to the conditions of the controlling party, which are often regulated by local data protection, and privacy rules. This can present both limitations and opportunities for the scope of any services offered.

Examples	Samsung[24], Apple[25]

3.3 Authorisation technologies

Advances in authorisation activities are focused on the standards surrounding the data exchanged during digital identity transactions. The use of more advanced technologies is enabling previously excluded individuals control over an increasingly complex range of attribute sharing capabilities. It is essential that industry standards evolve to protect users' rights to privacy and bridge the gap between consumer understanding and the commercial use of personal data.

Recent movements within the authorisation domain have ranged from the standardisation of basic logon mechanisms (such as those provided by OpenID, and Connect), towards the more nuanced requirements of managing what data is shared and when. In 2015 the Kantara Initiative published "User Managed Access" standards, representing an example of what future mechanisms might look like[26]. The initiative utilises an OAuth-based protocol designed to give an Internet user a unified point for authorising who and what can get access to their online personal data, content and services. However, it is too early to determine whether the adoption of such standards will be widespread.

Adoption of intricate authorisation mechanisms in the developing world has additional barriers to overcome, in the form of access to compatible personal devices and (as previously mentioned) lower literacy levels. As such, it is likely to be essential, for the foreseeable future, to adopt solutions that do not rely so heavily on user management.

Examples	Kantara initiative User Managed Access[27].

[24] http://www.samsung.com/uk/consumer/mobile-devices/smartphones/

[25] https://www.apple.com/uk/

[26] https://kantarainitiative.org/confluence/display/uma/Home

[27] https://kantarainitiative.org/confluence/display/uma/Home

4 Digital identities for DFS

4.1 Customer registration

It is the accepted norm that a customer cannot be registered for a financial service (including DFS) without providing some form of identity documentation; and the provision of a properly authenticated foundational digital identity is the gold standard for this. This is particularly valuable where, as is the case with Aadhaar and other similar services, additional attributes (name, address, etc.) are returned by the identity scheme to the bank/DFS operator, for comparison with documentation provided by the prospective customer.

4.2 Transaction authentication

Once an account has been opened, all use of the service by the customer, whether it is related to account maintenance or to transactions, must be authenticated.

How this is achieved is an important decision. In the case of India – and soon Pakistan – it is a requirement that all such touchpoints should be authenticated against the national identity service. Whilst this may meet various state objectives, it is arguable that it is not practical in the longer term. Even a simple projection of, for example, Aadhaar authentications against projected use in five years' time would suggest that the UIDAI servers are likely to be amongst the world's busiest, with commensurate availability requirements.

It is possible that a more practical approach might be to devolve the customer authentication requirement to the financial service providers (backed by suitable regulatory reporting and data access requirements, which are outside the scope of this document). This can be achieved by enhancing the customer registration process to include the creation of a transactional digital identity, derived from, and linked to, the state-issued foundational identity. This bank-issued digital identity would be backed by suitably robust customer authentication methods, such as biometrics.

The reliability and efficiency of this approach can be enhanced still further by ensuring that the customer authentication takes place at the edge of the network, and is sufficiently robust to support substantial confidence in the process. This would mean matching a strong biometric or other authentication mechanism locally in a suitably secure environment, such as a smartcard or a mobile phone. The result of the authentication would of course be available to the bank and (via reporting and other mechanisms) to the regulatory authorities.

4.3 Customers without identity documents

Although many potential DFS customers will have a suitable set of identity documents (for example, it was reported that Aadhaar registrars found that a remarkable 99.97 per cent of Indians had two identity ("breeder") documents, sufficient to register for Aadhaar), this is not always the case, and an approach to the financial inclusion of such customers' needs to be defined.

An approach that might be worthy of consideration is the creation of a dynamic digital identity for such customers; so they can be registered with self-asserted attributes (name, address, mobile phone number, etc.). Such a digital identity has a very low level of assurance[28], and would need to be developed before it can be considered sufficient for the delivery of financial services. Development of the dynamic identity can be achieved by:

[28] It is analogous to the digital identities created by UNHCR when registering refugees.

- Associating a strong form of authentication, such as biometrics (subject to the considerations set out in Section 3.2.3), with the identity at time of registration, so that the service provider can be assured that the same person is accessing the service on each occasion through an authentication challenge.
- Attaching an attribute noting sponsorship/endorsement from someone who does have the necessary documentation/state-issued digital identity[29].
- Verifying the 2FA opportunity based on the self-asserted mobile phone number. A higher level of assurance may be achieved where the SIM has been registered by the mobile operator to the customer using, for example, biometric authentication against a national identity scheme, followed by KYC processing. For example, his is the approach used by mobile operators in Pakistan, who use NADRA for SIM registration. However, in that case it is often the head of household who registers all SIMs for his family, and this aspect may be problematic.
- Adding additional attributes as further documentation becomes available – for example, if a passport is issued to the customer.
- Noting repeated/consistent usage of the digital identity over a period of months.

All of these steps, singly, and together, increase the level of assurance associated with the customer's dynamic digital identity.

The nature of the financial services that can be delivered to the customer can then be linked to this level of assurance, rather than the initial lack of documentation, in an approach that can contribute to the Financial Action Task Force's (FATF's) risk-based approach (RBA).

[29] This is the basis of the other 0.03 per cent of Aadhaar registrations.

5 Digital identity and DFS practical example

To add context to this report, this section sets out a practical example of how a provider of digital identity services and a mobile money (DFS) operator may collaborate in order to gain mutual benefit. Figure 6, below, illustrates a scenario where a consumer has pre-registered with a state issued eID scheme and leverages that identity during the application for a mobile money account. The process is as follows:

1. Consumer cryptographically signs an application for a mobile money account using their state-issued eID card via a compatible agent owned smartphone.
2. The mobile money operator requests the personal attributes of the consumer from the eID scheme using the signed application.
3. Once the relevant data has been received, the mobile money operator (in this instance also a MNO), uses the data to create and issue a functional identity for the consumer via the mobile connect service. From that point onwards, the consumer is able to authorise mobile money transactions via their mobile connect identity.

The benefits of the model described include reduced friction during customer registration with the mobile money provider, increased convenience for the customer when authorising transactions and access to other services within the mobile connect ecosystem. However whether such a scheme would turn into a success would be dependent on the specifics of the user experience, commercial structure, and functionality of the DFS product.

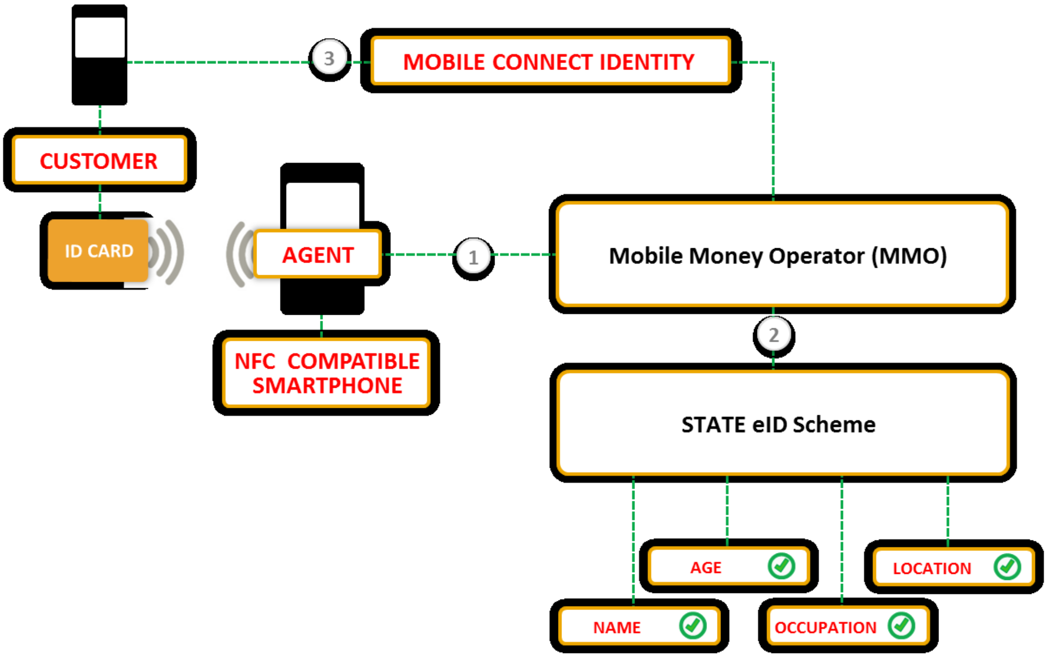

Figure 6 – Mobile Money, state-issued eID, and GSMA mobile connect

6 Digital identity in action

As a continuation of section 5, this section of the report details a sample of live scenarios where digital identity systems are used in DFS.

6.1 National ID number for SIM registration (Pakistan)

Expanding on the progress that has been made by NADRA and the computerized national identity card (CNIC) program, the Pakistan Telecoms Authority (PTA) and the Ministry of IT (MoIT) collaborated to introduce the biometric verification system (BVS) program. The program made it mandatory for all cell phone owners to register each new SIM and have their identity biometrically verified against the NADRA database. As part of this process, the PTA required the mobile industry to develop and operate a SIM registration information system, which links a customer's CNIC with a number of SIMs registered to that person. The biometric linking process is not done for corporate accounts, but as these comprise less than 1 per cent of the market (which is almost entirely pre-paid), and other checks are done to prevent fraud and other issues with corporate accounts, this is not felt to be significant.

The SIM registration database is operated by a joint venture[30] between all of the mobile operators reporting to the PTA. No SIM registration data is shared between mobile operators.

SIMs can only be activated after the purchaser's biometrics (thumb/finger impressions) have been verified against NADRA. In addition to the verification requirement, a limit was placed on each person obtaining SIMs, and a cap of five voice and data SIMs and two data-only SIMs per individual is enforced. Unlike the CNIC, the gender demographic of SIM registration to CNIC skews towards the male population, as the typical scenario includes a father as head of household registering all the SIMs used by a family, including his spouse and children.

There was an initial period of time when re-enrolment and verification was conducted to account for all SIMs obtained prior to the new rules being in place. During the initial re-enrolment, approximately 10-15 per cent of SIMs were not replaced and subsequently blocked from being used. In order to facilitate the completion of this verification, as many as 70,000 biometric terminals have been installed by mobile operators at sales locations throughout the country.[31]

6.2 Mobile transaction data for loan application (Pan-African)

Cape Town-based JUMO has partnered with MNOs to gain access to data relating to a consumer's mobile transactions. It analyses this data to allocate subscribers with a JUMO score dictating their creditworthiness. Using this score, consumers are able to apply for loans from conventional lenders using the service and have cash sent straight to their mobile money accounts[32].

6.3 Benefit disbursement via National ID number (India)

The Aadhaar payment bridge system in India enables government to distribute benefits and subsidies to individuals using their unique Aadhaar number. The system (provided by the National Payments Corporation of India) routes funds into Aadhaar Enabled Bank Accounts (AEBA) of the intended

[30] It is understood that the Board of the joint venture includes representatives from each of the mobile operators, in addition to the PTA.

[31] http://www.dawn.com/news/1157106

[32] https://www.jumo.world/

beneficiaries. This ensures funds are transferred in a timely manner, directly and eliminates the need for consumers to convey bank account details to government departments or agencies [33].

6.4 Social media data for access to banking services (Nigeria)

Sterling bank in Nigeria has partnered with lending platform Social Lender to enable consumers to apply for loans by providing access to their social media data. For example, individuals register on the Social Lender platform via Facebook Connect. Once access to their personal information is authorised, consumers are assigned a credit score based on a proprietary algorithm[34]. This score can be used to apply for loans from the bank.

[33] https://www.ucobank.com/pdf/faq-apb.pdf

[34] https://pageone.ng/2016/07/11/nigerias-social-lender-set-launch-south-africa/

7 Impact of digital identity on DFS and barriers to adoption

The impact of digital identity systems on DFS will depend entirely on the context within which a solution has been deployed. How appropriate an implementation is to any given environment will depend on the demands of local infrastructure, regulation, cultural, technical, social, and commercial requirements.

However, in analysing the potential effects of a proposed system, there are overriding impacts associated with the concept of digital identity that should be taken into consideration. A selection of key impacts within commercial, social, and regulatory domains are presented throughout this section.

7.1 Commercial impacts of digital identity on DFS

Large scale adoption is often necessary in order to support a viable commercial model for the provision of DFS. Integration to, or utilisation of, a parallel digital identity service has the potential to affect the business case through a variety of drivers.

7.1.1 Increasing the size of addressable markets

Mass adoption of digital identity services has the potential to expand the addressable market for DFS operators by providing registration credentials for previously excluded individuals. This enables providers of DFS to lower the adoption benchmark for critical mass within their target market. However, the balance between cost of integration against the perceived savings made when partnering with such a service is key in establishing whether the overall commercial impact is likely to be positive.

7.1.2 Cost of regulatory compliance

As fintech services expand, digital identity technologies and architectures are helping to bridge the gap with partner technology groups, specifically including aspects such as regulatory monitoring tools (regtech). From a commercial standpoint, the adoption of digital identity services, alongside monitoring tools for legislative bodies, has the potential to alleviate some of the costs incurred through regulatory compliance.

The costs associated with the KYC due diligence processes, for example, can be significant when dealing with paper-based documents which need to be scanned and maintained within a proprietary secure database. These costs can be reduced by multiple DFS providers leveraging a shared resource controlled by a digital IDP and monitored by a local supervisory/regulatory authority.

For DFS providers, the transactional fee charged by the identity service may be lower than what is otherwise incurred by individual DFS operators, due to economy of scale benefits derived from an all-around larger pool of transactions.

Regulators benefit from an increased understanding of the services they are supervising; greater confidence in the compliance of the service operators; and improved, and potentially cross-industry reporting.

7.1.3 Enabling additional revenue streams

As the scope of available data sets for consumers of DFS expands, the potential to leverage this information to enhance existing and future financial services is substantial. Subject to permission from regulatory authorities, new data-driven services could be used to impact future commercial growth.

7.2 Social and cultural impacts of digital identity on DFS

Naturally, the flow of personal information throughout private and public domains has the potential to fuel both positive, and negative social impacts. The analysis in sections 3 and 4 of this document reveals that identity schemes and technologies are often positioned in a trade-off between privacy and inclusion.

7.2.1 Increased risk to an individual's right to privacy

Privacy is an obvious concern in the delivery of digital identity systems, particularly when utilising those systems to enhance inclusion in developing markets. Although legal frameworks advocating privacy are relatively well developed in western geographies such as Europe (for example, GDPR[35]), the same protections are not as well developed in emerging markets. There are some noticeable contrasts; for example, in the United States, there are privacy controls in place against public sector usage of personal data, but few controls apply to the private sector – in India, by contrast, there are controls against private sector usage of personal data, but few controls on Governmental usage of citizen data.

Technological advances in systems supporting digital identity have the potential to expose the gap between referenceable data points and required access permissions. With potential IDPs positioned to be able to expose this vulnerability, the privacy of underserved individuals is clearly at risk.

7.2.2 Enhanced inclusion

Digital identity systems have the capability to establish a point of reference for individuals who would have otherwise been financially excluded. Although the benefits of inclusion are well documented, the most enabling services are typically the ones with the highest potential for detrimental effects on privacy. As such, it is likely that, in due time, regulation will be implemented preventing use of their full potential.

7.3 Regulatory impact of digital identity on DFS

Regulation plays an important role in managing the risks associated with digital identity services and is a key factor in influencing how they impact DFS.

7.3.1 Driving adoption of the risk-based approach among regulators

Developments within digital identity are enabling regulators to implement a risk-based approach to local legislation, with more confidence.

For example, the Central Bank of Nigeria's "regulatory framework for mobile payments services" defines a "name and number" requirement for "unbanked" registrations, as part of a three-tier structure[36]. Each tier has set transaction limits relative to the risks involved with the level of due diligence performed. As consumer data footprints become more accessible, regulators will be able to set greater limits for individuals who are only able to provide single points of reference. In addition, in response to delays in the roll out of the Government eID programme managed by NIMC, the CBN launched a programme to issue bank verification numbers (BVNs) to all holders of bank accounts – effectively a private sector-led digital identity. The BVN allows account holders to be identified across financial service providers, thus significantly simplifying the account opening

[35] http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

[36] Source: http://www.cbn.gov.ng/OUT/CIRCULARS/BOD/2009/REGULATORY%20FRAMEWORK%20%20FOR%20MOBILE%20PAYMENTS%20SERVICES%20IN%20NIGERIA.PDF

KYC process and regulatory compliance, to the benefit of both the banks and their customers. It is expected that the BVN programme will be extended to the DFS sector in the coming months.

There are moves to 'harmonise' BVNs and the national identity numbers (NINs) issued by NIMC, with the NIN being the primary identifier and the BVN being a secondary field. However, given the relative ubiquity of BVNs when compared to NINs (and NIMC cards), this process may take some time.

7.3.2 Liability

The gap between consumer awareness and industry use of personal data defines a requirement for consumer protection beyond the realms of consent.

Consent legislation is becoming increasingly undermined by unrealistic expectations placed on the consumer to understand what they are consenting to. As this trend develops, there is a need to establish regulation (where there are deficiencies) defining standards of conduct between consumers and the entities which use their data; to establish best practice guidelines; and to promote their adoption.

8 Recommendations

Recommendation 1 **At the time of registration, a DFS operator should create a digital identity for their customers, for use in both DFS transactions and (where relevant) in identity assertion with external service providers:**

- This transactional identity should be derived from a state-issued foundational identity to ensure reliability, flexibility, and control.
    - Clearly this is not possible if there is no state-issued foundational identity service that can support the validation of a foundational ID against the national identity service in quasi-real time. In this case, see **Recommendation 2**, below;
- Ensure that the transactional eID is authenticated locally, not remotely, to ensure maximum security;
- Ensure authentication (local) is separate from authorisation (centralised);
- Make provision for periodic re-verification of identity attributes.

Recommendation 2 **Where a customer is unable to provide a foundational document of digital identity, consider the issuance of a dynamic, self-asserted digital identity, which may be 'stepped up' over time and as required.**

- The LoA of this digital identity should be developed over time, as required to access new services, by measures such as:
    - Associating a strong form of authentication such as biometrics (see the limitations of biometrics described in Section 3.2.3) with the identity, so that the service provider can be assured that the same person is accessing the service on each occasion;
    - Attaching an attribute - noting sponsorship/endorsement from someone who *does* have the necessary documentation/state-issued digital identity;
    - Verifying the 2FA opportunity presented by a self-asserted mobile phone number, backed by SIM registration;
    - Adding additional attributes as further documentation, which may be subject to validation, becomes available;
    - Noting repeated/consistent usage of the digital identity over a period of months.
- The nature of the financial services that can be delivered to the customer can then be linked to this LoA, rather than the initial lack of documentation.

Recommendation 3 **Regulators should standardise digital identity registration, and ensure interoperability between DFS operators and service providers relying on the digital identity.**

- This would allow the delivery of a value-added financial service to a DFS operator's customers by a third-party service provider – for example, an insurance broker.
- Relying parties need confidence that a digital identity is standardised (in format, reliability, and confidence) across DFS operators.
- The nature of the financial services that can be delivered to the customer should be linked to the LoA associated with the digital identity.

Recommendation 4 **DFS operators should build in customer privacy measures, compliant with national legislation either current or anticipated.**

- Citizen data protection and privacy measures are becoming increasingly common – so DFS operators should build them in even if the legislation is not yet in place, and ensure that any parties they provide with identity and attribute data (relying parties) take the same approach.
- To this end, DFS operators should adopt and apply globally accepted "Privacy by Design" principles when dealing with and sharing personal data.

9 Glossary

Term	Range of meanings
Identity	• An individual, distinguishable from other individuals within a population. • The core attributes associated with an individual (name, address, date of birth).
Attribute	• A specific data item pertaining to an individual.
Credential	• An authentication token (e.g. smart card) used to assert identity. • A verifiable attribute, e.g. a digital certificate that demonstrates an entitlement or qualification.
Binding	• The process of linking an authentication credential to an identity in order that the authentication credential can be relied upon later as a means of asserting the identity.
LoA	• A measure of the quality of the identity derived from both the quality of the identification process, and the strength of the authentication credential used when asserting the identity.

Appendix A - Identity architectures

A.1 Monolithic IDP architecture

Monolithic identity models typically involve a large commercial entity acting as a digital IDP, offering identification and authentication services for third party organisations. Google and Facebook Connect provide market examples, collecting large amounts of consumer data as part of the identification process (often self-asserted) and leveraging username and password credentials in order to authenticate consumers to that data. Figure 7 illustrates the logical architecture of the monolithic IDP model.

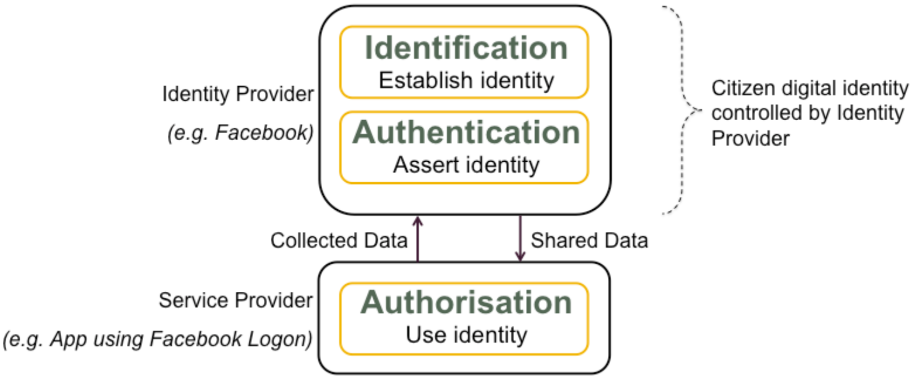

Figure 7 – Monolithic digital identity architecture

Applications within DFS

To date, implementation of this model in the developed world has surrounded two main use cases:

- **Providing access to third-party online services:** Consumers can register for or log onto third party online services by providing/consenting to access for that party to the personal information held by the IDP.
- **Targeted marketing services:** Providers use the large quantities of personal data attributes collected from consumers in order to offer targeted advertisement services to third party organisations. The success of Facebook's targeted marketing services is such that the platform auctions its advertising space to the highest bidder in order to manage demand[37].

In recent years, broader use cases, involving the use of monolithic architectures for credit risk and enhancing financial inclusion, have been explored. Germany-based Kreditech uses information from Facebook to supplement other data in order to determine an individual's credit risk[38]. A recent study by Consult Hyperion, Visa, and Hello Soda revealed the scope of application could stretch further still[39]; utilising an individual's social media footprint to increase convenience in consumer payments and establishing more personalised relationships between financial institutions and their consumers.

However, applications within the developing world are encumbered by relatively low penetration rates among data aggregating Internet giants, particularly among the target market for DFS.

[37] https://en-gb.facebook.com/business/help/197976123664242/

[38] http://money.cnn.com/2013/08/26/technology/social/facebook-credit-score/index.html

[39] https://www.visaeurope.com/media/pdf/the%20use%20of%20social%20data%20in%20financial%20services.pdf

According to data from We Are Social, Africa contributes less than six per cent of active social media profiles globally[40] despite making up roughly 15 per cent[41] of the world's population[42].

Still, this is not to suggest that there are not suitable organisations already established within DFS target markets with the ability to act within the monolithic identity model. Table 1 provides a comparison between Facebook and China Mobile, illustrating the MNO's capacity to operate in a similar role. Rather than highlighting synergies between the business models of the two organisations, Table 1 demonstrates the MNO's capacity to collect information from social interactions (over GSM networks). This alludes to a scenario where China Mobile could establish a social data profile for low income groups with no Internet access.

An added benefit of a mobile network provider operating within the monolithic role is that consumer privacy rights may be better protected. Whereas Facebook open APIs provide third parties with a relatively sophisticated means of interrogating consumer data, the proprietary systems of an MNO are likely to be less accessible.

In addition, there are market examples to support the use of GSM transactional data in the support of DFS. JUMO, the microfinance unit of Cape Town-based AFB Pty. Ltd., analyse an individual's calling records, airtime purchase, and other mobile data to determine credit scoring for loans[43].

However, perhaps the most valuable application to DFS can be found in a monolithic IDP's capacity to alleviate some of the friction involved in customer registration procedures: It is expected that an entity operating within the monolithic role will have acquired a substantial user base supported by substantial amounts of information that could be leveraged for identity services. The difference is in contrast to other models where identity assertion may present a barrier to adoption, users of social media platforms, and GSM networks proactively, and iteratively repeat the process of establishing identification attributes allowing the platform to develop an increasingly valuable cache of personal information.

Still there is an argument to suggest that though the analysis of an individual's social graph can enable a strong means of verification, the LoA provided by models which rely on self-assertion (of identity during the initial registration) is questionable.

[40] http://wearesocial.com/uk/special-reports/digital-in-2016

[41] http://www.bing.com/search?q=population+of+Africa&form=IE11TR&src=IE11TR&pc=TEJB;

[42] http://www.worldometers.info/world-population/

[43] http://www.bloomberg.com/news/articles/2015-09-23/phone-stats-unlock-a-million-loans-each-month-for-african-lender

	Facebook (United States)	China Mobile (China)
Market penetration	156 million[44] (48 per cent[45]).	1.28 billion[46] (92 per cent[47]).
Identification mechanism	Rich data sets of self-asserted information collected through regular consumer interaction.	Transactional data sets collected through regular consumer interaction
Authentication mechanism	Username and password.	SIM.
Authorisation opportunities within DFS	Access for credit scoring, targeted marketing, and powering personal finance management services.	Access for credit scoring, targeted marketing, and powering personal finance management services.
Assurance mechanism for self-asserted data	Analysis of social graph information to determine level of assurance.	Analysis of social graph information to determine level of assurance.

Table 1 - MNO's capacity to collect information

Monolithic IDP summary

Monolithic IDP model	
Description	Large commercial entity acting as a digital IDP, offering identification and authentication services for third party organisations.
Strengths	• Collect rich data sets from regular interactions with consumers; • Inclusion enabling; • Leverage existing scale to alleviate barriers to adoption.
Weaknesses	• Typically dependent on self-asserted data; • Poor penetration among target demographic for DFS; • Do not promote consumer choice; • Create concerns around consumer privacy and data breach vulnerability.
Examples	Facebook Connect, Google.

A.2 Federated Internet IDP architecture

Federated identity systems offer many of the benefits of the monolithic IDP model. Key differences are the number of concurrent service offerings and often, the specification of protocols for interoperability e.g.: OpenID Connect. Whereas in the monolithic model, a dominant market player offers identity services, federated architectures involve consumers choosing from multiple offerings from separate providers. Figure 8 illustrates the federated identity architecture model.

[44] http://www.statista.com/statistics/398136/us-facebook-user-age-groups/

[45] https://www.census.gov/popclock/

[46] http://www.statista.com/statistics/278204/china-mobile-users-by-month/

[47] http://www.worldometers.info/world-population/china-population/

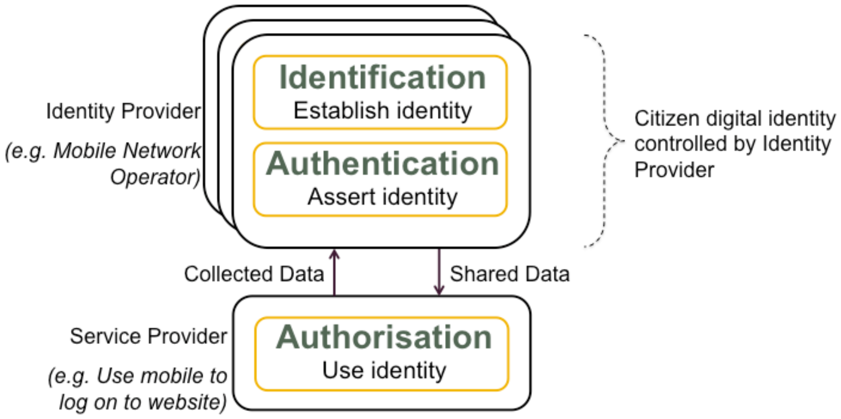

Figure 8 – Federated internet identity architecture

A.2.1 Applications within DFS

One of the most prominent examples of federated identity architecture within the developing world is found in the GSMA Mobile Connect programme[48]. This service enables multiple and separate mobile network operators to provide digital identity services to third parties via the same standards.

To date, Mobile Connect has mainly been applied to online login services, leveraging the due diligence performed during registration with the MNO to establish an identity and utilising the SIM card as an authenticator. However, recent expansion of the service to potentially 800 million subscribers across India[49] provides opportunity for enhanced application within the field of DFS.

Due to the similarities of the federated identity model to monolithic architectures, many of these applications remain comparable. However, specific benefits can be drawn from the nature of having multiple service offerings in the marketplace. For example, the liability risk that would normally be associated with a single provider is spread across multiple service offerings. This offers the advantage of damage limitation in the event of a data breach as only a limited percentage of the accumulated data pool will be compromised.

Furthermore, federated architectures enable the opportunity for greater co-operation and sharing of resources among both public, and private ventures. This becomes particularly interesting when considering the scope of useful attributes not currently achieving widespread utilisation within the field of DFS.

For example, a 2013 report from the Consultative Group to Assist the Poor (CGAP)[50] revealed a correlation between the attributes surrounding a subscriber's SMS, phone call, and data transactions, and a higher or lower propensity to adopt mobile money services. With such a strong relationship between mobile data and DFS, the federated model could be used to bridge the gap between MNOs and financial institutions in markets where legislation has excluded non-bank entities from offering mobile money services.

A study from the GSMA in 2014[51] revealed "non-enabling regulation" (regulation forbidding MNOs from leading mobile money offerings) was a key contributor to services not reaching their potential in certain markets. By positioning the MNOs in these markets as digital IDPs, the incumbent mobile money operators could benefit from crucial mobile data and the MNOs could benefit from commercial participation within DFS.

[48] https://mobileconnect.io/

[49] http://www.gsma.com/newsroom/press-release/gsma-announces-launch-mobile-connect-across-india/

[50] http://www.cgap.org/publications/power-social-networks-drive-mobile-money-adoption

[51] http://www.gsma.com/mobilefordevelopment/programme/mobile-money/is-regulation-holding-back-financial-inclusion-a-look-at-the-evidence#!

However, in order for these applications to be successfully implemented, competition between IDPs needs to be carefully regulated. Too many providers operating in any single market can confuse consumers and lower the prospect of investment from 3rd party funders.

A.2.2 Federated IDP summary

Federated internet IDP model	
Description	Multiple digital IDPs offering federated ID services via interoperable standards for communication protocols.
Strengths	• Enables interoperable standards for IDPs; • Promotes competition and consumer choice; • Privacy liability is spread across a number of providers.
Weaknesses	• Competition needs to be carefully regulated; • Adoption of interoperable standards needs to reach sufficient scale in order to be effective.
Examples	GSMA Mobile Connect, OpenID Connect

A.3 State-issued eID provider architecture

State-issued ID cards typically involve the control and access of personal data through a consumer issued authentication token (usually on a smartcard or mobile device) and a service provider-accessible middleware (e.g.: card reader infrastructure). Citizen data for the identification process is collected during government interactions such as birth registration. When a service provider wishes to gain access to this data the middleware is able to authenticate the card, for example, via cryptographic exchanges for, and provide access to the relevant data attributes. Usually both identification and authentication are performed as part of the scheme and hence the state can be viewed as an "IDP".

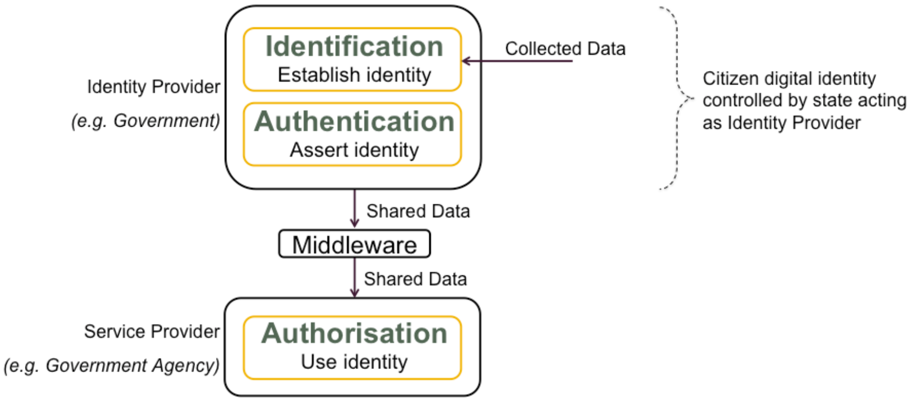

Figure 9 – State-issued eID Cards

A.3.1 Applications within DFS

The usage of state-issued eID cards ranges from limited government applications to broader support for commercial services. Applications within DFS are limited by how many citizens are registered and the accessibility of the middleware.

For example, where a national eID card scheme may potentially ease the registration process for a mobile money provider, the necessity to purchase an additional card reader, for every agent, in order to gain that benefit could significantly impact an already tightly-margined business model.

In order to present a viable proposition, the number of individuals registered with the eID scheme needs to be sufficient, such that the benefit of integration (for DFS providers) is significant to offset what would otherwise be expenses incurred in the registration and storage of KYC documentation.

However, the presence of scale alone does not define a capability for widespread application. The security surrounding the storage and communication of personal data by third party IDPs is a major concern for DFS operators. Any breach within a digital identity service which is integrated into DFS could ultimately undermine the security of the DFS provider service and run the risk of funding criminal and terrorist objectives.

National schemes with market dominance are also subject to certain competition concerns. One of the principle drivers behind DFS is inclusion. In Pakistan, it was necessary to register for the NADRA scheme in order to access utilities such as gas and electricity[52]. Although the scheme employed mobile vans to travel to rural areas in order to register people, the lack of choice for citizens puts a huge amount of leverage in the hands of the enumerators responsible for registration.

A.3.2 Summary of state-issued eID systems

State-issued eID architecture	
Description	Typically involves the control and access of personal data through a consumer-issued authentication token (usually on a smartcard or mobile device) and a service provider accessible middleware.
Strengths	• Enables foundational ID that can be used for DFS registration; • Uses high quality data during identification activities.
Weaknesses	• Requires middleware access for service providers; • Can create a barrier to adoption of DFS for low income demographics; • Application within DFS is dependent on scale of the service.
Examples	NADRA (Pakistan), Aadhaar (India), NIMC (Nigeria)

A.4 Brokered IDP architecture

The brokered IDP model involves a number of IDPs undertaking identification and authentication services and sharing data with service providers via a central hub. Once an identity is asserted, the data to be shared is standardised and routed to the appropriate service provider via the hub. Figure 10 illustrates the brokered IDP model architecture.

[52] http://www.cgdev.org/publication/ft/technology-service-development-nadra-story

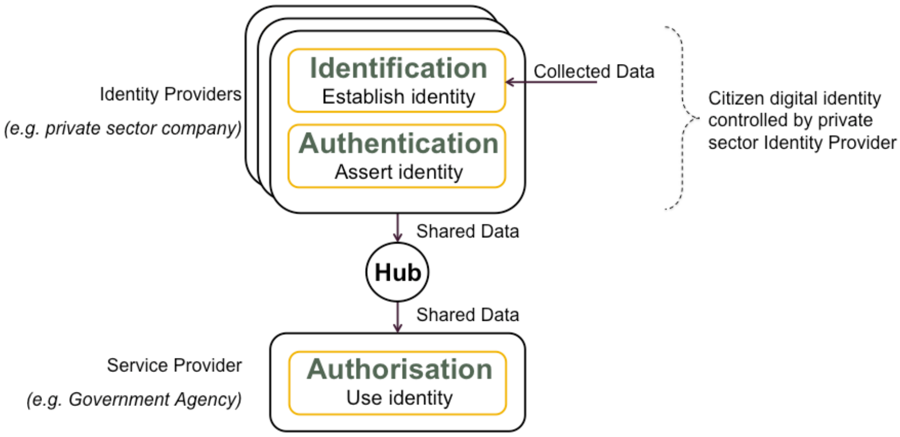

Figure 10 – Brokered identity provider architecture

A.4.1 Applications within DFS

Although similar to the federated IDP model, the intermediary hub in the brokered IDP architecture creates a number of key differences.

The hub provides a layer of anonymity between the IDPs and the service providers they are sending data to. Service providers are unable to identify which provider made the assertion and IDPs are unable to see which service providers their assertion is being delivered to. In instances where a consumer transactional identity is held with a mobile money provider, a layer of anonymity may not be appropriate, however this model does provide opportunity to restructure the delivery of DFS services in a manner which leverages the use of shared distribution networks.

Although certain regulations explicitly forbid exclusivity arrangements between mobile money providers and agents, commission structures and loyalty incentives are often imposed to a degree where this is *de facto* not the case. As a result, situations can occur where multiple mobile money providers compete for agents rather than customers to the detriment of consumer choice. Through leveraging the brokered identity model alongside a separation of consumer and agent management liabilities, it is possible to increase the quality of competition at the consumer level. Figure 11 illustrates a scenario where the presence of a local mobile money agent would facilitate access to multiple service offerings rather than just the market leader.

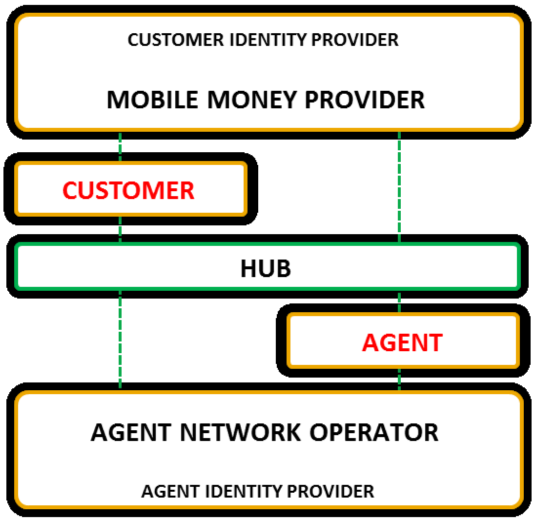

Figure 11 – Anonymity between agents and mobile money providers

The hub would facilitate anonymity between the mobile money operators and agent network services whilst providing assurances that each party was genuine during transactions. Reconciliation of funds and electronic float would be managed by the hub between master accounts and subdivided by either the mobile money operator or agent network manager as appropriate. Liability for each party would lie with the identities they manage.

However, concerns relating to this model include the potential for the conventionally government-operated hub to track usage between parties. Depending on the data recorded the integrity of the service could be undermined by a lack of privacy for both agents and consumers.

A.4.2 Brokered identity model summary

Brokered IDP model	
Description	Involves a number of IDPs undertaking identification and authentication services and sharing data with service providers via a central hub.
Strengths	• Enables cost savings through the use of shared resources; • Facilitates competition and consumer choice; • Privacy enhancing.
Weaknesses	• Privacy benefits are dependent on the storage of transaction data by the central hub; • Competition among IDPs has to be carefully regulated.
Examples	UK Verify, US Connect.gov

A.5 Brokered credential service providers (CSPs) architecture

In the brokered credential service provider model identification and authorisation activities are left to the service provider. The CSP focuses specifically on establishing reliable credentials that can be used transactionally to assert an already-established identity.

Typically, the same consumer will establish a separate credential for every service provider they wish to interact with. The mechanism for authenticating the consumer in order to forward this credential however may be consistent regardless of where it is being sent. Consequently, each service provider may undertake parallel identification activities for the same consumer. Transactions in this model are intermediated via a central hub.

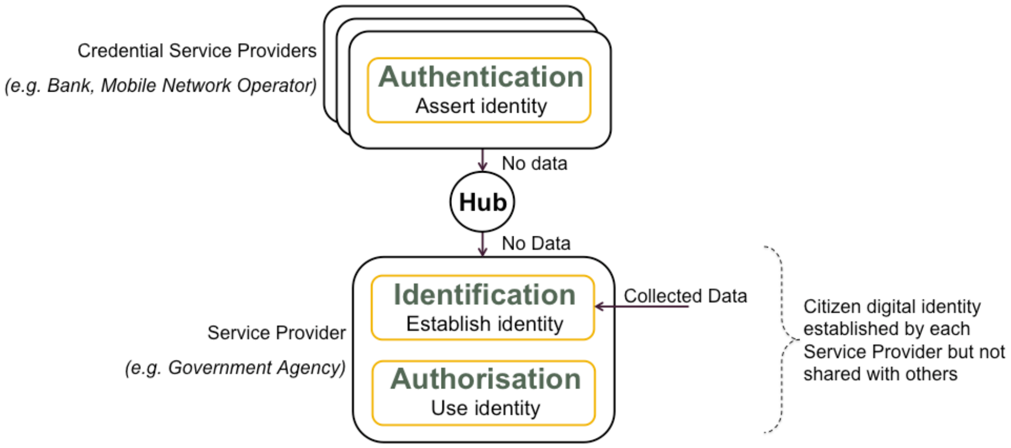

Figure 12 – Brokered credential service model

A.5.1 Applications within DFS

Although this model is currently believed to be unique to the Canadian Central Broker Service, other *similar* schemes such as those implemented through the FIDO alliance may have beneficial applications within a DFS environment.

Bangladesh has one of the lowest rates of mobile money usage among women globally (women make up less than 18 per cent of total digital finance users in the country[53]). Among other contributing factors, a recent study by CGAP[54] identified low literacy rates as one of the key reasons for this. Schemes such as FIDO have the flexibility to support different user authentication mechanisms via a single point of integration; thus facilitating an environment where market-appropriate solutions such as biometrics can be universally deployed through compliance to a single standard, the results of which could enable a reduced dependency on knowledge of a particular dialect. This could prove particularly useful in countries such as Burundi where (according to the CIA World Factbook) only 29.7 per cent of the population speak the official language[55]. Users could also benefit from enhanced privacy as credential brokerage services have a higher propensity for personal identifiers between service providers to be unlinkable.

Although the brokered CSP model can enable certain usability and privacy benefits, it does not provide a holistic approach to digital identity and in many cases, reduces customer convenience by requiring identification activities from each individual service provider.

A.5.2 Brokered credential service provider model summary

Brokered credential service provider	
Description	Identification and authorisation activities are left to the service provider. The CSP focuses specifically on establishing reliable credentials that can be used transactionally to assert an already established identity.

[53] http://www.cgap.org/blog/digital-finance-bangladesh-where-are-all-women
[54] http://www.cgap.org/blog/digital-finance-bangladesh-where-are-all-women
[55] https://www.cia.gov/library/publications/the-world-factbook/geos/by.html

Brokered credential service provider	
Strengths	• Transactions between service providers are less easily linked; • No attribute data is exchanged during identity transactions; • Simplifies access to service providers.
Weaknesses	• Does not enhance inclusion; • Specifically focused on authentication; • Potential for central hub to link transactions depending on how system is implemented.
Examples	Canadian credential broker service

A.5.3 Personal identity provider architecture

In the personal IDP model, a personal data store controls the ways in which previously collected identity attributes are shared. It achieves this by encrypting data using keys under the control of the individual. Attributes held within the store are signed by a trusted third party such as a bank or a mobile network operator in order to verify their accuracy. Figure 13 illustrates the personal IDP model architecture.

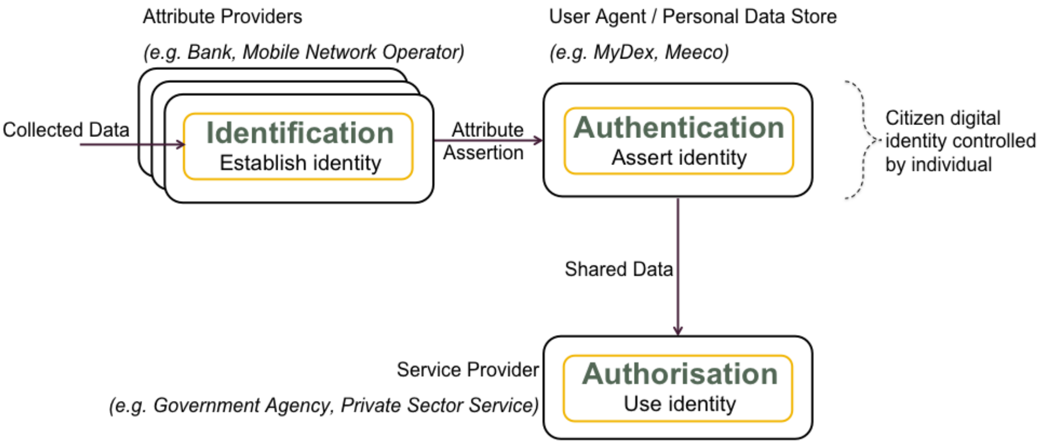

Figure 13 – Personal identity provider architecture

A.5.4 Applications within DFS

The benefits of the personal IDP model are situated mainly around user privacy and control. However, in the absence of trusted automation the model imposes a significant requirement on the citizen to administer access consistent with their understanding of privacy implications. In low literacy economies, such as Burkina Faso[56], the integrity of this type of system is likely to be undermined in the wake of convenience. Furthermore, the necessity for consumers to have access to a means of administration for the data store adds further argument to suggest the solution is more appropriate for developed markets.

[56] https://www.cia.gov/library/publications/the-world-factbook/fields/2103.html#wa

A.5.5 Personal IDP model summary

Personal IDP model	
Description	Involves the use of personal data stores to control the ways in which previously collected identity attributes are shared.
Strengths	• Less susceptible to large scale data breaches; • Greater control passed on to the individual; • Privacy enhancing.
Weaknesses	• Potential for unrealistic expectation on individual to manage complex range of data attributes; • Security of personal data is subject to personal storage device, or cloud encryption mechanism; • Business model for this architecture remains yet to be proven.
Examples	MyDex, Meeco, Microsoft U-Prove

A.6 No IDP

The no IDP model replaces intermediary IDPs with technologies that facilitate decentralised management. Blockchain/shared distribution ledger technologies provide an example of the "No IDP" model enabling support for highly decentralised and anonymous forms of digital ID. Figure 10 illustrates the no IDP model architecture.

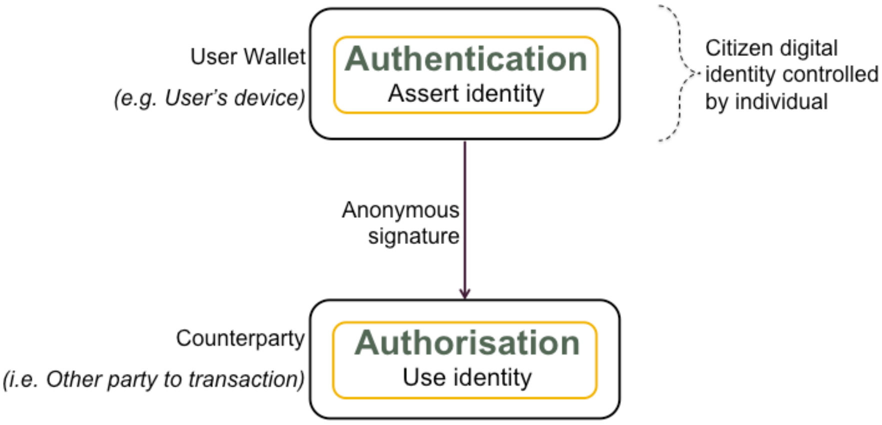

Figure 14 – No IDP model

A.6.1 Applications within DFS

Implementations built upon the no IDP model are at the forefront of current research and, as such, no clear model for identity has been established.

Typically, application of shared ledger technologies such as Bitcoin[57] involves users self-asserting an identity via the creation of cryptographic keys. These keys establish ownership of the currency and no other personal attribute data is shared with the blockchain. Although models such as this enable a high level of privacy, concerns with the underlying technology and access requirements create barriers to adoption and are particularly unsuitable for targeting unbanked demographics.

The requirement for Internet-enabled smartphones or computers in order to access the service presents a limitation for use in countries such as Benin where internet penetration is low as 9.3 per

[57] https://www.bitcoin.com/

cent (2014)[58]. Furthermore, in the absence of central governance, upgrades in security or architecture will be difficult to co-ordinate and execute.

A.6.2 No IDP model summary

No IDP	
Description	Intermediary IDPs are replaced by technologies that facilitate decentralised management e.g.: Blockchain / shared distribution ledgers.
Strengths	• Potentially privacy enhancing; • Difficult to fraud due to requirement for consensus across network for ledger updates.
Weaknesses	• No clear model for identity has been established to date; • No clear governance on the upgrade of public blockchains; • Places potentially unrealistic expectation on consumer to manage their own identity.
Examples	Bitcoin

[58] http://data.worldbank.org/indicator/IT.NET.USER.P2

Appendix B: Identity technologies

Technology	Type	Application within DFS
Europay, Mastercard, Visa (EMV)[59]	Authentication	EMV uses strong cryptographic security. This can be provided via a smart card, a secure element within a mobile phone or potentially via a "hardened" app in a mobile phone.[60]
Subscriber Identity Module (SIM)[61]	Authentication	A GSM-compliant mobile phone's SIM is a specialised smart card (qv), and offers a tamper-resistant cryptographic environment. It can host apps created in the SIM Toolkit (STK) environment, which can use encryption for transactions and general communication. It can support communication over any of the mobile phone's network connections, including mobile data, SMS, and USSD.
Smart card[62]	Authentication	Tamper resistance cryptographic hardware. Established and recognised secure technology.
Physiological biometric[63]	Identification or authentication	For identification needs, multiple biometrics are necessary to establish uniqueness. By contrast, for authentication, a single biometric can provide effective means of authentication of asserted identity.
Behavioural biometric[64]	Authentication	The technology is less mature than physiological biometrics (qv), and more aligned to risk management than absolute or explicit authentication.
Mobile app	Authentication	Can be high security, depending on protection built into the app.

[59] Europay, Mastercard, Visa (EMV) is the set of standards for worldwide interoperability and acceptance of secure payment transactions.

[60] Host Card Emulation (HCE) has caused the payments industry to consider software approaches to EMV leveraging techniques such as white box cryptography. In these solutions, authentication credentials are usually tokenised to reduce the risk associated with the compromise of a credentials. Typically, the numerous measures including software hardening, and server side risk monitoring are employed to ensure the overall residual risk is acceptable.

[61] Subscriber Identity Module

[62]A smart card is a device that includes an embedded integrated circuit that can be either a secure microcontroller with internal memory or a memory chip alone. The card connects to a reader with either direct physical contact, or with a remote contactless radio frequency interface.

[63] Physiological biometrics is the field of study related to the measurement of innate human characteristics such as fingerprints or iris patterns.

[64] Behavioral biometrics is the field of study related to the measure of uniquely identifying, and measurable patterns in human activities, rather than innate human characteristics.

Technology	Type	Application within DFS
Risk-based authentication (RBA)[65]	Authentication	Like behavioural biometrics, RBA provides corroborating evidence for authentication rather than explicit authentication. No standard way to measure performance.
SMS	Authentication	SMS used straight relies on mobile network encryption, which is known to be weak. It needs to be augmented with application security, implemented, for example in a mobile app or in a SIM Toolkit app (see SIM), both of which can use SMS as the bearer technology.
Transactional access numbers (TAN List)[66]	Authentication	Access to physical list required but can be easily copied once access is obtained.
OAuth	Authorisation	A protocol for providing access tokens (which may be temporary) to allow third party applications to access resources (data) on behalf of the resource (data) owner.
User Managed Access (U M A)	Authorisation	A recently established standard that defines how a resource owner (e.g. an individual) can control access to their resources (e.g. personal data) by third parties. The standard was developed by the Kantara Initiative[67].It builds on and extends OAuth (qv).
Scanning documents	Identification	Digital validation of documents using image processing; a relatively new technology but thought to be robust. AU10TIX is a leading vendor in this space[68].
Credit reference agency data	Identification	In developed markets this is a de facto method of establishing identity. Can appear invasive, where knowledge-based questions are generated from credit data.
Government registries	Identification	Usually viewed as authoritative. Anecdotally can often contain significant numbers of fraudulent identities. Privacy will depend on amount of data held and control of access to it.
Social identity verification	Identification	The use of social media data including self-asserted data and social graph to establish

[65] Risk-based authentication is a dynamic authentication system which takes into account the profile of the agent requesting access to the system or service in order to determine the risk profile associated with that transaction. The risk profile is then used to determine the complexity of the challenge required.

[66] TAN list – a printed list of codes from which the user is asked to select one, as a means of authentication. Used in the Danish eID system NemID (https://www.nemid.nu/dk-da/om_nemid/sikkerhed/teknikken_bag_nemid/).

[67] http://kantarainitiative.org/

[68] http://www.au10tix.com/index.php/products/front-end-solutions/

Technology	Type	Application within DFS
		identity. The strength of such an approach is unproven. It relies on sufficient data being readable.