Designing National Identity:

An Organisational Perspective on Requirements for National Identity Management Systems

Adrian Rahaman, Martina Angela Sasse
Computer Science Department
University College London
London, United Kingdom
a.sallehabrahaman@cs.ucl.ac.uk, a.sasse@cs.ucl.ac.uk

***Abstract* - Many National Identity Management Systems today are designed and implemented with little debate of the technologies and information required to fulfil their goals. This paper presents a theoretical framework detailing the organisational requirements that governments should consider to implement effective identity systems. Analysis is based on publicly available documentation on the implementation of National Identity Systems in the countries of Brunei, India, and the United Kingdom. The findings and the framework highlight the importance of clearly defining the purpose of the system, which has implications on the authenticity, uniqueness, and uses of identity; failure to consider these components is likely to lead to ineffective identity systems and policies.**

Keywords – identity; identity mangaement system; organisation; government; policy

I. INTRODUCTION

Identity is a valuable resource that shapes and defines social interactions [1] by reducing uncertainty and building trust between parties. Governments have traditionally provided identities for their citizens, and used them to manage the provision of services. In an age of growing travel and migration, and facing threats such as illegal immigration, crime and terrorism, *"many governments today are now trying to reassess their identity policies in light of technological changes"* [2].

Governments have tended to view National Identity Management Systems (N-IDMSs) technology as a silver bullet – or at least cornerstone – to tackling these problems, but fail to consider the complexity of delivering such systems [3]. In the UK, attempts to short-cut debate and deliver a system quickly led to adoption of a system that has now been scrapped [4]. Without proper consideration of purpose and operational requirements of the N-IDMS, it is unlikely they will deliver their stated goals.

Convinced that requirements for a strong proof of identity means an increase in security, governments have not examined the use of identity beyond it. But personalised and customer/citizen-centric services mean that identity is no longer just a mechanism for individuals to access resources - it has itself become a valuable resource being accessed by organisations to inform their decisions [5-7].

Still, most research on this topic focuses on identity as a security mechanism. For example, a very comprehensive model for governments' transition to digital N-IDMSs [8] mainly describes its use for online authentication purposes; [9] developed an IDMS architecture that places identity as a layer below information resources.

The research presented in this paper moves beyond the security perspective, viewing identity as a strategic resource. The aim of the study was to uncover organisational identity requirements, and their effects on the design and implementation of IDMSs (The term organisation as used within this document refers to the organisation that is implementing the IDMS).

Section II below explains the methodology followed in this study. In Section III, we present our findings, and explore the processes **of identity construction** and **identity use**. Section IV highlights the importance of **purpose**, which then ties all the findings into a single framework. In Section V, we discuss the implications for future N-IDMSs: to meet their defined purpose, the key factors of **authenticity, uniqueness,** and the objectives of the **relying parties**have to be clearly defined.

II. METHODOLOGY

Our research used a case study approach - a systematic analysis of the identity phenomenon in 3 different cases [10] of N-IDMS implementations in Brunei, India, and the United Kingdom.

The data analysed on the UK and India N-IDMSs was publicly available system documentation published by the respective lead agencies (IPS and UIDIAI respectively); for the Brunei case study, interview sessions with key government officials were recorded and transcribed; interviews were conducted with:

- 3 employees from the lead agency (BruNIR) that deal with strategy and implementation of the system.
- 2 employees from a security organisation that works with the lead agency on the N-IDMS.
- 3 employees from a Relying Party that makes use of the N-IDMS as an authenticator
- 1 employee from a Relying Party that was seen as a prime candidate during the initial phases but is now considering launching its own IDMS system.

The data was analysed using Grounded Theory, a method to develop theory that is grounded in data [11]; i.e., it does not start with a preconceived theory, but seeks to generate new theory through a systematic collection and analysis of data [12].

 ISBN: 978-1-61208-176-2

III. RESULTS

Our analysis revealed that organisational identity requirements, and its eventual impacts on the final design of the system, can be divided into two main areas; **identity creation** and **identity application.**

A. Identity creation

When an identity system is first implemented, a new and unique context is created, within which identities need to be instantiated. It is within this newly created context that an organisation needs to ensure the *correctness* of identities being enrolled. This process is important because it affects the integrity of the identity, and has an impact on the type and amount of personal information being collected and stored.

The challenge of the enrolment process it is that it involves the verification of unknown individuals. Organizations typically fall back on two main criteria when enrolling new identities: **authenticity** and **uniqueness.**

1) Authenticity

Authenticity describes the truthfulness of an identity created within the IDMS. It seeks to answer the question, *is the individual who he says he is?* Organisations typically ensure authenticity of an individual's identity by verifying his/her biographical information against different sources. Organisations can vary the source of information by choosing between two different schemes:

- **Introducer-based schemes** build on the concept of personal referrals - having an already enroled individual vouch for the authenticity of the individual who is attempting to enrol in the system.
- **Document-based schemes** are designed around the use of available identification documents provided by other organisations (bank statements, utility bills, etc). Such schemes rely on third-party organisations confirming the authenticity of enrolling individuals.

While an organisation can choose between the two sources of information, it is limited by the context of its implementation; the main contextual factors that influence the applicability of these schemes are **universality** and **intimacy**.

a) *Universality*

This concept captures how many members of the target population already possess widely accepted forms of identity documents. These are identities that individuals have established with third-party organisations with whom they have a trust relationship; examples of such organisations include banks, utilities, and municipalities that an individual has interacted with for a period of time.

The degree of universality in the target population will affect an organisation's ability to rely on a document-based scheme for authenticity. Specifically, having little to no universality would remove this option, because many individuals would not be able to provide the required documents.

The case study of the Indian NIDMS provides an example of the problem arising from low universality. A large section of the population has been locked out of both public and private services; the weak identity infrastructure has resulted in a fragmented approach to the enrolment in current systems, placing large burdens on most of the poor population to prove themselves, and being denied access to basic services as a result.

"...every time an individual tries to access a benefit or service, they must undergo a full cycle of identity verification. Different service providers also often have different requirements in the documents they demand, the forms that require filling out, and the information they collect on the individual. Such duplication of effort and identity silos increases overall costs of identification, and cause extreme inconvenience to the individual. This approach is especially unfair to India's poor and underprivileged residents, who usually lack identity documentation, and find it difficult to meet the costs of multiple verification processes." [13]

Given the aim is to provide access to its poorer citizens, India cannot create an N-IDMS that relies on a document-based scheme. Therefore, the UIDAI has chosen an introducer-based scheme, *"where introducers authorized by the Registrar authenticate the identity and address of the resident*" [14].

In contrast, the abandoned UK N-IDMS was strongly motivated by prevention of criminal activities and illegal immigration. While the system documentation does state that the UK N-IDMS will make it easier to prove identity [15], UK citizens were not being denied services because of a lack of identity - most of the population had recognised forms of identity provided by third-party organisations.

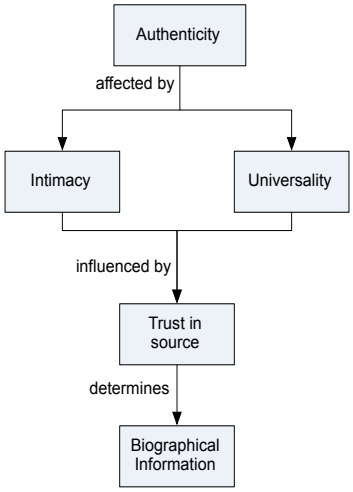

Figure 1. Organisatons Identity Creation process - Authenticity

The UK system took a document-based approach, requiring individuals who enrol for an identity to provide several different documents as proof for the authenticity of the claimed identity [16]. The government required that individuals provide documents that have some form of unique identifier such as passport numbers, driving license numbers, national insurance numbers and *"any number of any designated document, which is held by him"* [17]. This

 ISBN: 978-1-61208-176-2

creates an *information net* around the claimed identity, which the government can then use to ensure authenticity by verifying the individual's personal information with the relevant third party organisations.

b) *Intimacy*

The concept of intimacy captures how much of the targeted population is already known to the organisation. High levels of intimacy imply that the organisation can have more confidence in an introducer-based scheme, because it can support a transitive trust arrangement that extends from known individuals to unknown ones.

The effects of intimacy can be seen in the Bruneian context and its combined approach to ensuring authenticity, incorporating elements of both a document-based and introducer-based scheme. Running an identity system since 1949 [18], the government has been enrolling identities of all individuals born and staying within the country, and thus have established a great deal of intimacy with its population. While individuals are required to provide their birth certificates as proof during enrolment, the government also records the identity numbers of the individual's parents. This in effect creates a hybrid document-introducer-based scheme where the authenticity of the individual is being proven with a minimal amount of documentary evidence, which is further supported by linkages to introducers that are already enrolled within the system.

While India has an introducer-based scheme, the government's choice in the matter is forced by unsatisfactory levels of universality. However, India now faces the problem that there is not enough intimacy to support introducers, as used in the Brunei case. Having never registered identities of past populations, the UIDAI in India cannot currently rely on parents as introducers to the system. Therefore, the government has devised a scheme to artificially boost intimacy through a set of defined trusted recognised introducers.

Introducer and document-based schemes are not orthogonal. Both make use of transitive trust to ensure the authenticity of the claimed identity. The document-based scheme is basically an institutionalised version of the introducer-based scheme. At the centre of the document-based scheme is the reliance on identity documents that have been produced by third-party institutions, which fulfil the role of introducer. In the end, the authenticity of the claimed identity is verified by a trusted third party.

2) Uniqueness

Apart from authenticity, organisations also need to consider uniqueness - that is to ensure that identity cannot be enrolled more than once into the identity database. Organisations' desire for uniqueness is driven by concerns of identity fraud, where individuals might attempt to enrol multiple times, potentially using multiple personas, to gain extra benefits. Organisations typically attempt to tackle this issue of *de-duplication* through the use of biometric data [19].

Today, organisations can choose between various different biometric solutions; facial, fingerprint, and iris recognition being current solutions of choice. Organisation's choice of biometric are influenced by 3 main criteria; **obligations, performance, and population**.

a) *Obligations*

The first hurdle an organisation faces when choosing a biometric technology are the obligations that it must conform to, such as **international standards and current practices.**

International standards influence the choice of biometrics, especially if individuals' identity is meant to be portable across different countries, organisations, or contexts. If, the organisation aims to achieve interoperability, this determines not only the type of biometric used, but also the format in which the data is stored. For example, the UK government defended its choice of fingerprints with the need to comply with standards published by International Civil Aviation Organisation (ICAO) [20]; however, the ICAO standards only proscribe *how* fingerprints should be implemented *if* they are used on such documents – but do not proscribe the use of fingerprints itself [21].

Similarly, although the UIDAI did not focus on ensuring compatibility with other countries, adhering to an accepted standard remained an issue, to help create a consistent and portable identity within India's large borders. The report from the Indian Biometric Committee recommended the implementation of biometrics based on international standards (ISO 19794), stating that the *"standards are widely accepted, and best embody previous experiences of the US and Europe with biometrics"* [19].

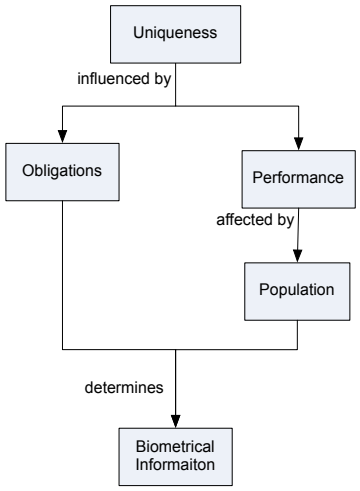

Figure 2. Organisatons Identity Creation process - Uniqueness

Organisations also face obligations around current practices that it, or other organisations that it might work with, have already implemented. The existence of current practices around the use of certain biometrics implies the availability of experience, expertise, and infrastructure around that particular biometric. Having such familiarity with a particular biometric can help to ease the

 ISBN: 978-1-61208-176-2

implementation of a new identity system that makes use of the same biometric.

In the UK context, this can be seen in the relationship between the Identity and Passport Service (IPS) and the Immigration and National Directorate (IND) [20]. Prior to the plans for an N-IDMS, the IND had already been processing, recording, and storing facial and fingerprint biometrics of foreigners for the purpose of UK visa applications. Thus, when the IPS finalised its plans for the N-IDMS it chose to build on IND's systems, directly storing fingerprints and facial biometrics on IND databases. In the Bruneian context, the biometrics deployed in the previous N-IDMS was carried forward into the new, making use of fingerprints and facial photographs that they were already familiar with.

b) *Performance*

Aside from its obligations, organisations are also influenced by the performance of the various biometrics; these can be expressed in terms of **accuracy** and **human interpretation**.

Accuracy captures the ability of the biometric technology to correctly match biometrics presented for verification against biometric templates that have been previously recorded. During enrolment, organisations typically want to prevent individuals from enrolling more than once. This is achieved by choosing biometrics that provides the required levels of accuracy. Failure to match comes in form of False Acceptance - an impostor being wrongly accepted against an enroled identity - and False Rejection, an enroled individual being rejected by the system [22] (Further discussion of these measures is outside this scope of this work). Organisations should also consider the ease of which the biometric can be circumvented. For example, Facial Biometrics is *"considered a poor biometric for use in de-duplication"*, as an individual can easily avoid identification through *"the use of a disguise, which will cause False Negatives in a screening"* [19].

While the use of biometrics to ensure uniqueness is typically an automated process, a manual form of checking identity is required when a false rejection is encountered. Since the system is unable to accurately distinguish between two or more biometrics, some form of backup authentication is required to confirm or deny the false rejection. Therefore, having a biometric that enables quick manual checking becomes a necessity. Most biometric do not lend themselves easily to manual inspection. As a result, facial biometrics becomes attractive to organisations simply because it provides a backup option through **human interpretation** [19].

"We use AFIS, Automated Fingerprint Identification System. All the fingerprints captured will be processed with the fingerprint matching, and this is very useful when the citizen does registration of the card. This is to ensure that one citizen holds one card and number only. Those who register will go through the AFIS matching, and if it is OK, then we will do the registration. Otherwise there will be human intervention; a matching process, the system will list the possible candidates that match, but normally we go for a 100% match. There is a possibility of 70, 80, 90 and 100% match by fingerprints. The system also makes use of facial image, from the entries identified by AFIS. So it's easy for us to do the matching, we can even assign the matching tasks to the clerk, by looking at the facial image and the percentage. It is very straight forward and user friendly." [23]

c) *Population*

An organisation's performance considerations are in turn mediated by the population characteristics in 3 ways: **size, compatibility, and geographic diversity**.

First of all, organisations need to consider the **size** of the target population. Large population sizes can negatively affect the accuracy of the biometric. The choice of the 10-finger biometrics proposed in the UK and Indian scheme was made on those grounds. The Indian Biometric committee [19] established that *"False Acceptance Rate is linearly proportional to gallery size"*; using a 2 fingerprint scheme with a population size of 1.2 billion, the FAR was estimated to be 14%, which is well above the 1% mark that they required. Therefore, it was recommended to proceed with a 10-fingerprint scheme, which was estimated to provide a 0% FAR, maintaining the uniqueness of individuals in the database.

The second population characteristic is **compatibility**, which captures the suitability of the biometric for use on the targeted population. Compatability is commonly captured by tests demonstrating that accuracy is not affected by characteristics of the target population (e.g. skin tone); the lack of such studies was highlighted by the Indian Biometric committee [19].

However, organisations must also consider other real world cultural compatability factors that are not captured by these tests. For example, the Indian Biometric Committee highlighted the use of Lawsonia Interims (Henna) by women, stating that it can prevent the accurate collection of fingerprints as *"sensors may not properly capture fingerprint features."* Another example is the large percentage of population in India who are *"employed in manual labour"*, and thus provide *"poor biometric samples"*, as their fingerprints have been worn away by the nature of their work. Because of these issues, iris is now seen to provide a better match for this population [19]. In Brunei, the BruNIR has encountered problems with the compatibility of fingerprints:

"…only one, the taking of the fingerprint. Because they can get worn out, and those are very difficult to capture. We identified that since the beginning of the project, and we came up with a solution to make use of moisturizer. It helps, but that is the major problem" [23].

Geographic diversity deals with the dispersion of the targeted population across the nation. This can affect the accuracy of the biometric because of varying conditions under which the biometric data is collected and used, and because procedures may be used differently. When a population is spread across a large geographic area, the organisation is unlikely to be able to collect all the information on its own; it will likely adopt an accredited enrolment strategy, where authorised third parties collect

 ISBN: 978-1-61208-176-2

information on their behalf. UK and India are prime examples of third-party enrolment, using private organisations to enrol and capture individual biometrics. This can result in *"several non-technical factors that can impact accuracy more significantly than technical accuracy improvement efforts, such as the lack of adherence to operational quality"* [19].

B. Identity Application

In addition to identity construction, the organisation is also concerned about the mechanism with which enrolled identities are accessed and used. There are four main dependent constructs that affect organisations identity access policies; **relying parties, objectives, conditions,** and **accessibility.**

a) *Relying parties*

At the most basic level, the organisation needs to specify the relying parties that require access to individuals' identity. There are two main types of relying parties: **organisational** and **individual.**

First of all, there are **intra- or inter-organisational** entities that require access to the identity. Intra-organisational access is typically a requirement since the organisation needs to create and manage identities in the first place. But access to identities within the organisation can support other functions that the organisation needs to carry out. For example, the BruNIR is not only responsible for the distribution of the identity cards in the country, but also for the monitoring of identities across borders. Recent developments have meant that the Brunei identity card can now be used as a passport at land borders with Malaysia. Therefore, the BruNIR requires other forms of internal access to support these activities.

This is not so in the Indian context, where the UIDAI was setup solely to handle the registration of identities. The main focus here lies on the inter-organisational access of identity. In its plans to introduce the identity system the UIDAI clearly established and discussed plans with several different third party organisations that include PDS, NREGS, as well as the general education and health provision systems.

In the UK, the IPS has defined both intra-organisational use of its systems (identity cards as passports), as well as its inter-organisational aims by identifying various agencies, such as law enforcement agencies and the Department of Work and Pensions. The Bruneian context, on the other hand, has comparatively ill-defined inter-organisational obligations, only stating its intent of creating a multi-purpose smart card, which can be used by any third-party organization.

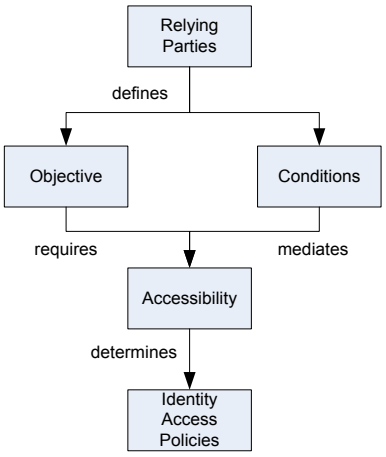

Figure 3. Organisations Identity Application requirements

In addition to organisational reliance on identity, the organisation also needs to recognise the **individual** as a relying party who may be able access his own identity and personal information. This is especially the case in the UK scenario, where IPS has specified that individuals should be able to access all their information on the system, which is envisioned to eventually be an online service [15], [20], [24]; India and Brunei have not specified any mechanisms by which individuals can directly access or view their identity records.

b) *Objectives*

Each relying party that the organisation identifies will have its own separate set of objectives. These can be expressed in terms of **enablement** and **proof**.

The use of identity to mediate the provision of services will always create a division between those who have access, and those who do not; identity systems are either primarily used to enable, or deny access. Whether the intention is to use identity to either enable or disable individuals is captured by the **enablement** construct. In India, the main intention of the relying parties is the enablement of poor citizens to access services that they have a right to, but currently do not find accessible. Additionally, Indian banks are focused on introducing new forms of mobile banking, thus enabling individuals to access new services that are to be developed.

The primary objectives in the UK context are to preventing undesirable activity (benefit fraud, crime, illegal immigration, and terrorism). The Bruneian context has described a largely enabling use of identity, with its intention to support the introduction of new on-line services introduced by third parties.

Proof describes the objective of the relying party in using individuals' identity as a single proof of identity, or as a key that enables the tracking of an individual across multiple interactions or contexts. The Indian case provides an illustration of a high-linkage scenario, where all relying parties are advised to use individuals' identity numbers as a foreign key to their own systems. It even suggests that relying parties make use of individuals' identity internally, so as to keep track of employees. The Bruneian case makes

 ISBN: 978-1-61208-176-2

no such recommendations, nor enforces any rules to such linkages, resulting in a mixed approach between parties where certain relying parties make use of the identifier as an index to their records, while others merely use the identity as a proof.

c) *Conditions*

The organisation will need to identify the conditions under which the access to the identity will take place, and may thus affect access requirements; this can be expressed as **risk level** and **timeliness.**

Risk level is a measure of the security sensitive nature of the information access. Information access that is done under high-risk conditions, such as that involving terrorism, would have greater access privileges, when compared to a low risk situation that has little implication for the country, organisation, or relying party.

The importance of risk level in the development of the identity system and the information access policies is most evident in the UK scenario. While most access by third parties would be recorded, any access for the purpose of counter-terrorism would take place without consent, and would not be recorded [15], [20], [24].

The BruNIR has created an official channel, through which law enforcement can send a written request, with supporting reasons, to obtain information. The UIDAI has not specified any direct access to the information by third parties, but, its N-IDMS plans state that one unique identifier per individual would be useful for third parties to keep track of employees that might pose a risk of corruption - for example, to track inspection officials who come into contact with food that is given out to the poor [25], or the presence of doctors and teachers ensuring they are where they need to be [14].

In addition to risk level, the **timeliness** of information access is another factor to consider. Since one of the many cited benefits of an identity system is improving efficiency, it is not surprising that the need to access information quickly is an important factor.

An example is the planned use of the UK N-IDMS for the purposes of Criminal Background Checks (CRB), which are required for persons applying for employment work in a range of sectors. Existing CRB procedures take a long time to verify individuals' identity to check their CRB status, leading to a backlog of applications. It would be beneficial if the agency carrying out these background checks could verify applicants' identity more quickly, and thus it was seen as a prime candidate for gaining some form of access to the identity system; *"the time for issuing Criminal Records Bureau disclosures could be reduced from 4 weeks to 3 days"* (ID Card Benefits Overview).

The UIDAI has also highlighted the time-sensitive nature of third parties, stressing the importance of addressing the application of current ration cards due to *"prolonged delays in processing the application"*, and the advantages in using the unique ID number in the distribution of rice grain [25]. The Brunei N-IDMS has no specific examples regarding the timeliness of information, but improved efficiency was a main factor in the introduction of the smart card system, as it would allow the transfer of information in digital format reducing the overhead for filling in forms [23].

d) *Accessibility*

Once the organisation has identified the relying parties their respective objectives, and the conditions under which they are operating, it can then go on to define the accessibility of the system to these parties. The access to the system can be described in terms of **information set, localised,** and **direction**.

Information set describes the type and amount of identity information that the relying party will have access to. For the UK system, with its emphasis on national security, certain authorities would be able to gain access to all the personal information without individuals' consent. The scenario in India is such that no relying party will have access to the personal information - the system will only confirm or deny the accuracy of personal information. . The BruNIR has stated that third-party organizations will not have any access to the database, and can only access the information that is visible on the card and stored on the smart chip.

Localised refers to the spatial mode of access to the identity system: at one end of the spectrum, a check of identity can be limited to a local point, at which an individual physically presents the identity, and at the other end is the remote access of identity through a networked database from any number of parties. The Bruneian N-IDMS does not provide third parties with any remote access to their database; all the information and authentication functions that the relying party can access, is stored on the card itself. The *raison d'etre* of the Indian N-IDMS is remote authentication, so third parties have access across a network. The UK N-IDMS specified a range of access options including local options (such as visual authentication and local chip authentication), but also fingerprint authentication across a network.

Meanwhile, the **direction** of information access describes the *push* or *pull* nature of identity access; this in turn defines the *read* (including authentication) and *write* capabilities of the relying party. The Indian N-IDMS does not provide relying parties with any ability write information to the database. The transactions are a pull of information, where the third party requests confirmation of identity. The UK N-IDMS is able to record information about the third party access when performing authentication procedures. A new entry is created on the database recording the time and location of the authentication; this represents a combined push-pull operation, where information is read from and written to the identity database.

The Bruneian N-IDMS does not provide any remote access, but law enforcement can send in a written request, which is a remote pull of information. However, third parties can store information onto the chip when required. This represents a local push of information onto the card, and therefore affects the overall information access policies that need to be set in place.

 ISBN: 978-1-61208-176-2

IV. FIT FOR PURPOSE

The previous sections have catalogued organisations' options in the construction and use of identity – and the choice of options has to match the purposes for which the system is deployed. *Who are the relying parties that require access, and what identity information does the system need to hold?* To ensure that that the system being implemented will be fit for purpose, an organisation needs to tailor the identity construction to support the requirements of those purposes.

The Indian system, with is stated purpose of enabling access to services for the poor, was quick to identify welfare agencies as relying parties, and to ensure that individuals are able to enrol (by devising the appropriate authenticity requirements for a target population that suffers from both low universality and intimacy).

In the UK, with the main purpose being the reduction of crime and terrorism, the organisation identified law enforcement agencies as a core relying party, as well as defining strict authenticity and uniqueness requirements that would support its security goals.

In Brunei, the main aims of the system were firstly to modernise their current identity infrastructure, and secondly to create a multi-function digital identity infrastructure that could be used by various third parties (especially in the provision of e-government services). As of now, there has been relatively low uptake of the system by third parties. This investigation reveals that this due to the lack of specifying relevant third parties, and thus catering for their needs and requirements. However, recent efforts to engage with a relevant stake holders in neighbouring country of Malaysia has resulted in the use of the identity cards as digital passports [26]

V. CONCLUSION AND FUTURE WORK

Using a case study approach, three different implementations of N-IDMS were examined and compared, has and this uncovered a set of choices that organisations can over **identity construction and identity use** processes. These choices must be made in line with the **purpose** of the IDMS

The organisation's requirements for identity construction will determine the amount and type of information that is collected and stored. The choice of biographical information is influenced by organisations' **authenticity** requirements, which is further mediated by the **universality** of current identity documents, and the levels of **intimacy** of the organisation to the target population. The organisation's **uniqueness** requirements influence the choice of biometric information; it is affected by the organisation's **obligations** to which it must adhere, as well as the **performance** of the biometric, which must be considered within the real-world **population** parameters.

The requirements for the use of identity will affect the identity access policies implemented. Beginning with the **relying parties** that need to access the system, the organisation must consider the various **objectives** of each party, as well as the **conditions** in which they operate. Only then will the organisation be able to specify **accessibility** of the system, and hence the identity access policies.

It should also be noted that the purpose also has an influence over the authenticity/uniqueness requirements, and vice versa. Certain purposes might require different sets of information, and the type of information within the system will place limitations on the purpose of the system; for example, a system that provides proof of age only needs to collect individuals' date of birth, whereas one designed to counter terrorism may require address information, and possibly audit trails of use.

The findings of this study further the current understanding of factors that should be considered in the design and operation of NIDMS; the codification of the identity requirements into a framework can be used to aid discussions and critiques of IDMSs. For example, [27] state that attention should be paid to issues of purpose, population scope, data scope, and users of the data. In our framework, those elements are refined into more detailed concepts and the relationships between the various concepts are elaborated. Similarly, [3] describes a short-circuiting of identity debates through the use of international obligations, language ambiguity, technological focus, and expertise. Our framework addresses these concerns by explicitly listing the considerations, thus reducing ambiguity and short-circuiting, while also introducing non-technological decisions such as relying parties, and their unique purposes.

The organisation's uniqueness consideration provides another area of comparisons to current work in the field. Drawing from [28] recommendations when implementing biometric systems, organisations should not only pay attention to the False Acceptance and False Rejection rates of biometric technology, but also consider how well they match and population characteristics, and how easy they will be to present; these are all present in the framework as sub-dimensions of the performance and environment constructs.

Therefore, the framework here serves as a guide for organisations and system designers to build effective N-IDMSs. It encourages focused debate, consideration, and definition of various critical components, ensuring that the identity information collected and the technology chosen are both fit for purpose, thus assisting in the implementation of successful identity systems.

A limitation of our current research is its emphasis on biometric identifiers; all the systems in all 3 case studies depend on them. Not all IDMS use biometrics systems, which limits the generalisability of the uniqueness framework. Future research will need to address these concerns, and further develop the framework to be applicable to non-biometric implementations.

Work will also need to be done to develop guidelines to effectively express requirements for uniqueness, authenticity and purpose; doing so will further help to increase communication in the field and encourage proper debate, while keeping the scope of the system concise and to the point.

 ISBN: 978-1-61208-176-2

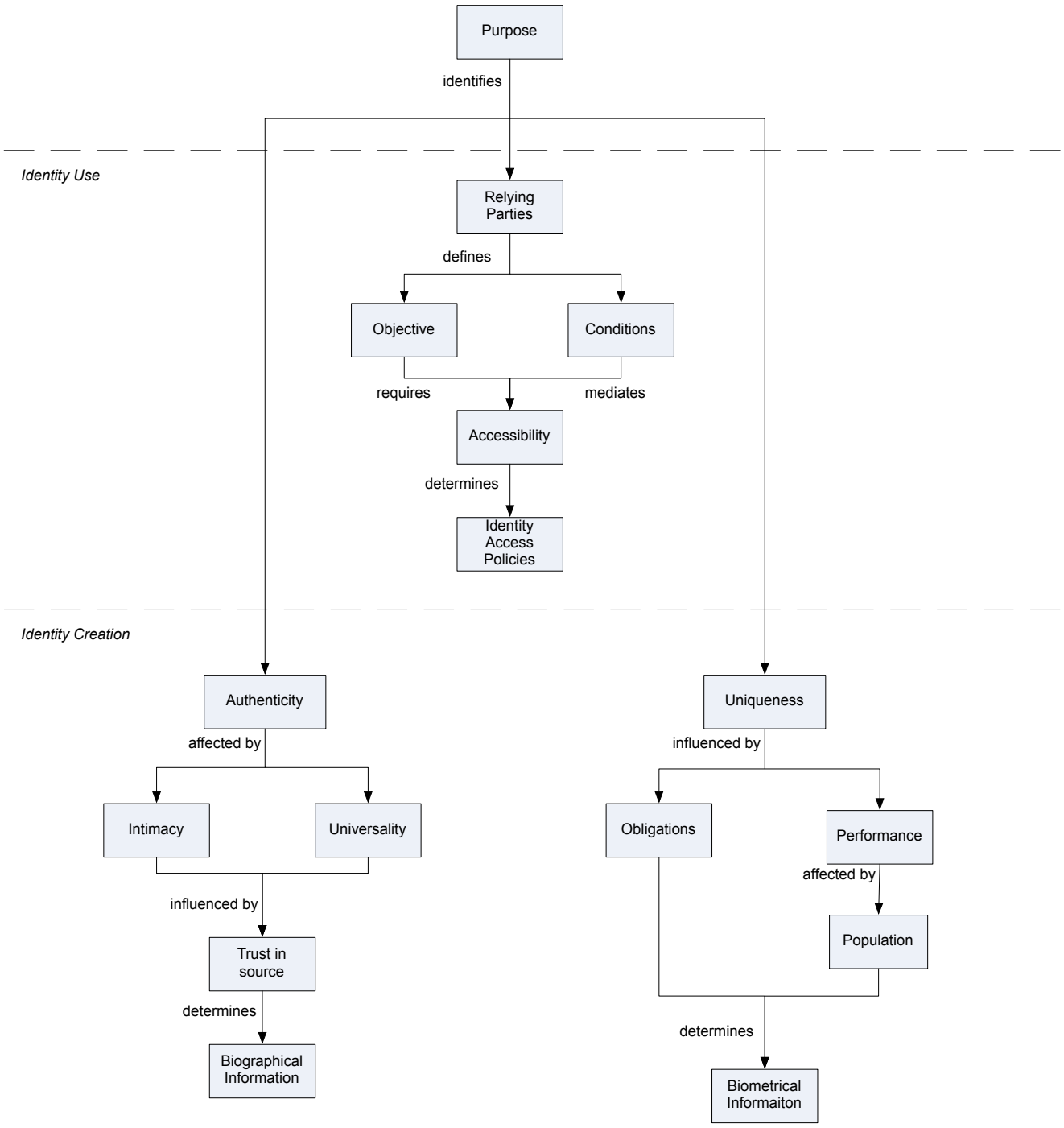

Figure 4. Complete framework displaying organisational identity requirements

 ISBN: 978-1-61208-176-2

REFERENCES

[1] A. Rahaman and M. A. Sasse, “A framework for the lived experience of identity,” Identity in the Information Society, vol. 3, no. 3, pp. 605-638, 2011.

[2] E. A. Whitley and G. Hosein, “Global identity policies and technology: do we understand the question?,” Global Policy, vol. 1, no. 2, pp. 209-215, May. 2010.

[3] E. A. Whitley and G. Hosein, Global challenges for identity policies. New York, USA: Palgrave Macmillan, 2010.

[4] BBC, “Identity cards scheme will be axed ‘within 100 days’,” BBC News, no. 2002, 2010.

[5] M. Meints, and H. Zwingelberg, "Identity Management Systems – recent developments," Deliverable 7.2, Future of Identity in the Digial Society, 2009.

[6] J. Taylor, M. Lips, and J. Organ, “Information-intensive government and the layering and sorting of citizenship,” Public Money and Management, vol. 27, no. 2, pp. 161-164, Apr. 2007.

[7] J. Taylor, M. Lips, and J. Organ, "Citizen identification, surveillance and the quest for public service improvement: themes and issues," paper to the European Consortium of Political Research ‘Privacy and Information: Modes of Regulation' Joint Session Helsinki 7-12 May 2007.

[8] H. Kubicek, “Introduction: conceptual framework and research design for a comparative analysis of national eID Management Systems in selected European countries,” Identity in the Information Society, vol. 3, no. 1, pp. 5-26, Apr. 2010.

[9] P. White, “Identity Management Architecture: a new direction,” in 8th IEEE International Conference on Computer and Information Technology, 2008, pp. 408-413.

[10] B. L. Berg, "Qualitative research methods for the social sciences," Boston: Allyn and Bacon, 2001.

[11] K. Punch, Introduction to social research: quantitative and qualitative approaches. Thousand Oaks, California, Sage Publications, 1998.

[12] J. M. Corbin and A. Strauss, Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Thousand Oaks, California, Sage Publications, 1990.

[13] Unique Identification Authority of India, UIDAI strategy overview: creating a unique identity number for every resident in India. India: UIDAI, 2010.

[14] Unique Identification Authority of India, Aadhaar handbook for registrars. India: UIDAI, 2010.

[15] Identity and Passport Service, National Identity Service: delivery update 2009. London, England: Home Office, 2009.

[16] D. Blunkett, Identity Cards: the next steps. London, England: Home Office, 2003.

[17] Identity Cards Act London, England: House of Lords, 2006.

[18] R. Yunos, “Immigration services through the ages,” Brunei Times, 01-Feb-2009.

[19] Unique Identification Authority of India, Biometric design standards for UID applications. India: UIDAI, 2009.

[20] Identity and Passport Service, Strategic action plan for the National Identity Scheme. London, England: Home Office, 2006.

[21] London School of Economics, The Identity Project: an assessment of the UK Identity Cards Bill and its implications. London, England: LSE, 2005.

[22] J. Ashbourn, Practical biometrics: from aspiration to implementation. London, England: Springer, 2004.

[23] A. Rahaman and B.I.N.R. Department, “Interview - BruNIR.” 2010.

[24] Identity and Passport Service, National Identity Scheme Delivery Plan 2008: a response to consultation. London, England: Home Office, 2008.

[25] Unique Identification Authority of India, Envisioning a role for Aadhaar in the Public Distribution System. India: UIDAI, 2010.

[26] A. Razak, “Brunei, M’sia first in SEA to use IC as passport,” Brunei Times, 2007.

[27] S. Kent and L. Millett, IDs? Not that easy: questions about nationwide Identity Systems. Washington, United States: National Academies Press, 2002.

 ISBN: 978-1-61208-176-2

TABLE I. SYSTEMS ANALYSED AS PART OF THE STUDY

	Brunei	**India**	**UK**
Population Size	**407, 000**	**1, 170, 938, 000**	**62, 218, 761**
Date Implemented	2000 – today	2010 – today	2008 – 2010 (abolished)
Purpose	Multi-function smart card	Support poor in accessing services	Prevent terrorism, crime, benefit fraud, travel card
Mandatory	18 and above	All citizens	Voluntary (mandatory for high risk personnel; airport staff, etc.)
Unique ID Number	Yes	Yes	Yes
Identity Card	Yes	No	Yes
Smart Chip	Yes	No	Yes
Centralised Database	Yes	Yes	Yes
Authentication (Against Card)	Yes	No	Yes
Authentication (Against Database)	No	Yes	Yes
Record Authentications	No	No	Yes (stored on Database)
Information Read	Third Parties can access biographical information on card and chip.	Third parties can confirm information accuracy (yes/no response).	Third parties can access biographical information on card and chip. Information can be pushed from the database to third parties. Security organisations can get access to all information on the database (through information commissioner).
Information Write	Third parties can to write to the smart card	None	Information can be pushed from third parties to the database.

 ISBN: 978-1-61208-176-2