The LSE Identity Project

Alternative blueprint for a national identification system

Draft version for public consultation

This section of the LSE's report has been published in advance of the release of the final report to enable us to consider responses to our alternative blueprint for a national identification scheme. We welcome feedback, which should be emailed to i.r.hosein@lse.ac.uk

The study has established a number of potential shortcomings of the government's identification proposals. These include cost, complexity and probable failure to attract consumer trust. In reaching those conclusions we recognise the importance of constructing an alternative model. In this section of the report we set out our vision for a more cost effective, secure, reliable and trusted identity structure that meets key objectives of the current Bill.

In doing so we have adopted the following assumptions:

- No national identification system is totally secure, nor can any system ever be immune to the risk of accepting false or multiple identities. Any such claim would not only be demonstrably false, but it would lead to substantial and sustained attacks. Biometrics can be spoofed, registration data falsified, corruption exploited and social networks manipulated. At both a human and a technological level, a fixation on achieving perfect identification across the entire population is misguided and counter-productive. Such emphasis is disproportionate and will lead to substantial problems relating to cost, security and trust.

- The choice of any national identification system should involve careful and sensitive consideration of key aspects of cost, security, dependability and functionality. This exercise is not necessarily a Zero Sum equation where the value of one element is traded off against the value of other elements. The aim of a genuine evolution of thinking is to achieve high scores on all key elements of the scheme. Only a spirit of openness makes it possible for this outcome to be achieved.

- Public trust is the key to a successful national identification scheme. Public trust can only be secured if issues of cost effectiveness, dependability, security, legal rights and utility are addressed, and are seen to be addressed. We believe it is

possible to achieve these goals while also ensuring a system that offers reliable means of achieving the government's stated objectives.

- A genuinely cooperative approach to finding a national identity solution must involve consultation based on principles as well as objectives. We believe the government's model has failed because it has evolved exclusively through the pursuit of objectives. While this may create an identity system that suits key stakeholders involved in specific goals, the approach imperils other essential aspects such as public trust.

We have identified a set of principles that should guide the design and execution of a national identity scheme.

An identity system must be proportionate. Aspects such as complexity, cost, legal compulsion, functionality, information storage and access to personal data must be genuinely proportionate to the stated goals of the identification system.

An identity system should be inspired by clear and specific goals. Successful identity systems embrace clear objectives that facilitate responsive, relevant and reliable development of the technology, and which limit the risk of exclusion and abuse.

Identification systems must be transparent. Public trust is maximised when details of the development and operation of an identification system are available to the users. Other than the identifier and card number, no information should be hidden.

Identity disclosure should be required only when necessary. An obligation to disclose identity should not be imposed unless the disclosure is essential to a particular transaction, duty or relationship. Over-use of an ID system will lead to the increased threat of misuse and will erode public trust.

An identity system should serve the individual. Public trust will not be achieved if an identity system is seen as a tool exclusively for the benefit of authority. A system should be designed to create substantial economic, lifestyle and security benefits for all individuals in their day-to-day life.

A national identity system should be more than just a card. Identity systems must exploit secure and private methods of taking advantage of electronic delivery of benefits and services.

Personal information should be controlled by the individual. Any biometrics and personal data associated with an identification system should remain to the greatest possible extent under the control of the individual to whom it relates. This principle establishes trust, maximises the integrity and accuracy of data and improves personal security.

Empathetic and responsive registration is essential for trust. Where government is

required to assess and decide eligibility for an ID credential, the registration process should, to the greatest possible extent, be localised and cooperative.

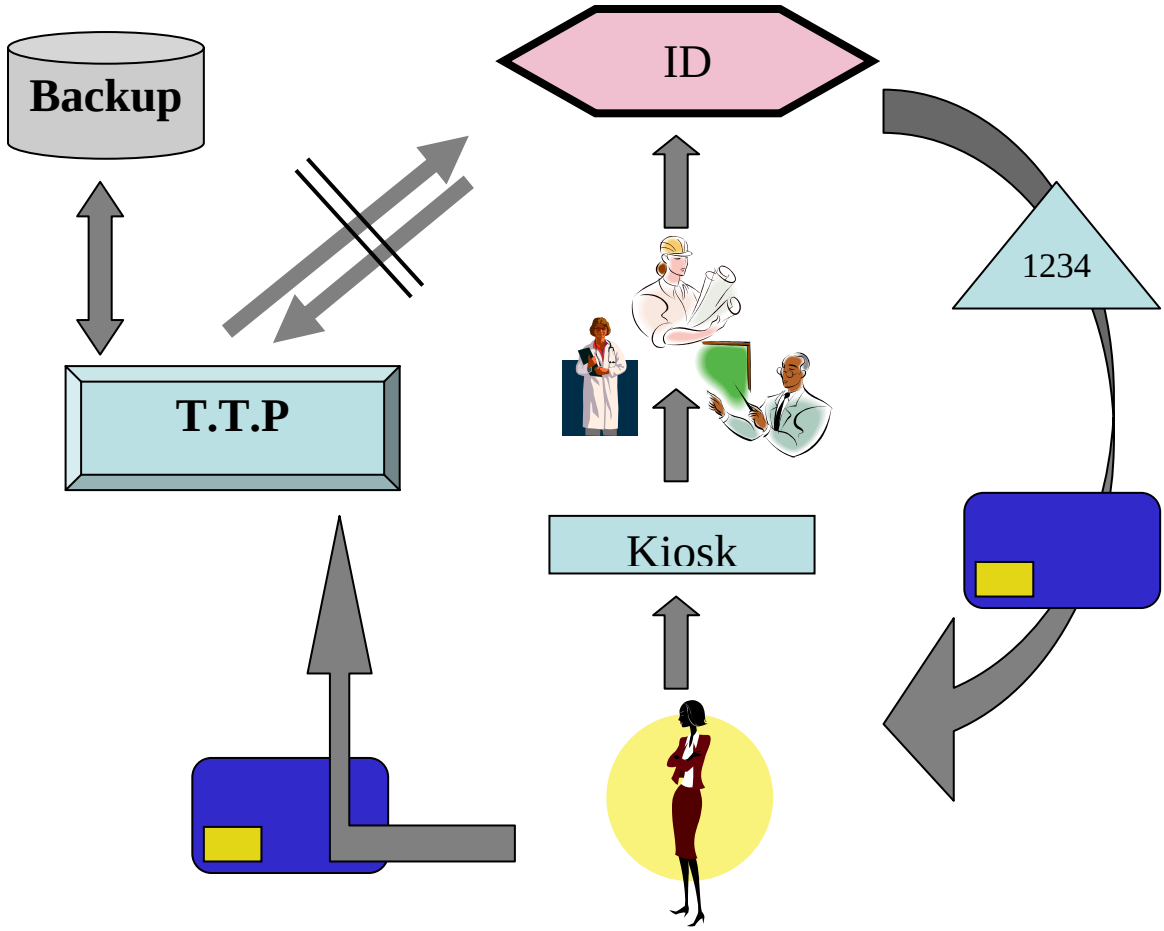
Revocation is crucial to the control of identity theft and to the personal security of individuals. Technology should be employed to ensure that a biometric or an identity credential that has been stolen or compromised can be revoked.

Identity numbers should be invisible and restricted. Any unique code or number assigned to an individual must be cryptographically protected and invisibly embedded within the identity system. This feature will protect against the risk of identity theft and will limit "function creep" through extended use of the number.

Capability for multiple authenticated electronic identities. An identity system should allow individuals to create secure electronic identity credentials that do not disclose personally identifiable information for use within particular social or economic domains. The use of these different credentials ensures that a "master" identifier does not become universally employed. Each sectoral credential is authenticated by the master identifier assigned to each individual. The use of these identifiers and their control by individuals is the basis for safe and secure use of federated identity systems.

Minimal reliance on a central registry of associated data. Wherever possible, in the interests of security and trust, large centralised registries of personal data should be avoided.

Permit secure and private backup of associated data. An identity system should incorporate a means of allowing individuals to securely and routinely back up data stored on their card. This facility will maximise use of the identity credentials.



The LSE's ID model embraces a number of key features:

The database controlled by central government contains the minimum amount of information necessary to authenticate cards and to store unique ID codes. This reduces the security and privacy threats to a reasonable level. The potential for hostile attacks and mass identity theft is substantially reduced.

Personal information remains under the control of the individual. This facilitates he use of the card and the related master identifier for a variety of e-government and e-commerce functions.

In the LSE model, the government establishes a network of Trusted Third Parties (banks, police stations, court houses, solicitors) which are authorised to maintain secure backups of the information contained on the card.

Summary of stages

1. To obtain the card, applicants visit a job centre, post office or other authorised facility. There they enter an electronic kiosk that takes a digital photograph, accepts basic identifying data, and embeds these into the coded application form that is dispensed at the point of contact. A temporary electronic file is created containing this data.

2. The applicant secures the endorsement of two or three people in a position of trust. Once endorsed by the referees, the form is handed in at a post office or other facility.

3. The form is sent for processing. Processing of the form is largely automated. Random checks on some references will in time be conducted online or via email.

4. When the card is ready, the holder takes it to a "trusted third party" - a bank or post office for example – which is local to the applicant. The card is then connected to the Government's temporary file. If the codes match, the card is validated and all data is deleted from the government file apart from the name, code and card number. A copy of the data on the card is stored securely at the TTP.

5. The mater identifier can be used as a means of establishing a number of assured sectoral (or “spin-off”) identities that can be used in numerous domains. This “private credential” facility allows the development of such innovations as federated identity management.

The scheme in detail

Identity vetting and registration.

All identity registration depends on one or more of three common processes (a) personal interview, (b) production of primary documents, (c) endorsement of applicant by referees.

In the government model, vetting (authentication) would require all three elements. Additionally, it is proposed to register an applicant’s biometrics and to undertake “biographical footprint checking” to inquire more thoroughly into life history and activities.

We believe this proposal should be replaced with a less costly and less intrusive approach. The current passport application procedure, while vulnerable to some current risks, establishes the basis of an alternative model.

We propose abandoning mandatory personal interviews and replacing these with a more informal and flexible process. Personal interviews can still be conducted on request but we believe most people would prefer a more localised procedure. A substantial part of the procedure is automated, with scope for manual checking and auditing.

The application procedure – Stage One.

The applicant first visits a post office or government facility such as a Job Centre or local government office, where electronic kiosks have been installed. One of the functions of these kiosks is to dispense tamper resistant application forms. The kiosks are designed to permit a second person to be present to assist the applicant when needed.

When activated by the applicant, the kiosk displays a short video explaining the application procedure. This video can be repeated at any time during the process. Visual and audio prompts support the procedure throughout, and the applicants are asked at each stage whether they are happy to proceed.

Through a keyboard, applicants then supply the kiosk with their name and National Insurance (NI) number. The NI number is checked online to verify the applicant's name, though at this stage the success of the application does not depend on a match. The applicant is notified if a match to the NI number is not found, but no other action is taken.

***Note**. We do not see the number as a reliable identifier by itself. Its use in this situation does however have the dual benefit of allowing a triangulation for security, with the added benefit of providing a means of eventually cleaning the NI number database.*

The applicant can submit the paper form without the NI number, but must supply additional data so the number can be manually found. This circumstance will be dealt with on a case-by-case basis at the processing stage. If a match still cannot be made, or if the applicant has no NI number, a personal interview may be necessary.

The kiosk then takes a digital photo of the applicant and embeds this onto a coded paper form. The final printed form will thus contain the photograph, name and unique reference number for the application.

Finally, applicants are asked to provide a simple biometric of choice, such as a single fingerprint, for local verification against the card that is to be issued (not for the current purpose of mass matching one-to-many against the entire population). A PIN can also be requested for additional security. Total time for the procedure in the kiosk will vary from 5 to 15 minutes.

The form is immediately printed and dispensed to the applicant, and the data is simultaneously uploaded as a secure temporary file. This temporary file is inactive, and at this stage is not scrutinised either electronically or by a human. Another form can be obtained by again visiting the kiosk and by repeating the procedure.

The form will have a number of pages, each of which contains the basic data.

***Note**. Consideration was given to making the application an online process. The option was viewed as unworkable because referees are often contacted in an informal setting.*

The application procedure – Stage Two.

Once in possession of the form, the applicant secures endorsement on it from a "trusted personal network" of either two or three referees of good standing. The current passport application guidelines suggest an extremely wide spectrum of people who would be considered suitable as referees. These include accountants, bank/building society officials, chemists, chiropodists, local or county councillors, civil servants (permanent), dentists, engineers (with professional qualifications), fire service officials, funeral directors, insurance agents (full time) of a recognised company, journalists, justices of the peace, local government officers, minister of a recognised religion, nurse (SRN and SEN), opticians, paramedics (state registered), police officers, post office officials, social workers, solicitors, surveyors, teachers, lecturers, trade union officer and qualified travel agents.

Each page of the form has a section for a single referee. This ensures that a referee cannot see who else has vouched for the applicant unless the applicant wishes to disclose this information.

The current passport requirement is a single referee who has known the applicant for two years. It is proposed to set the new standard at two years for one referee, and one year for the other referee(s).

***Note**. It should be kept in mind that if any applicant is unable to secure these referees, or has difficulty dealing with the process, the option of a personal interview would be available. However it is expected that many people in this situation will have a person who will help them through the process without the need to be interviewed.*

As an additional security measure, the applicant's writes the NI number on the form. The applicant then delivers the completed form to a kiosk centre, where it is forwarded through internal mail for processing.

The application procedure – Stage Three.

From the perspective of government, the approval stage of this model is the most labour intensive element of the application procedure, though much less labour intense in most cases than the current proposals.

The paper form is manually checked. Its number is matched with the temporary file number, and the digital photo on each is then compared. This is to ensure that the document was not spoofed or the photo altered during the endorsement phase. The NI number recorded on the temporary file is also compared with the NI number on the form.

***Note**. It is possible to automate this process, though this may be difficult if the form has been damaged. Automation is perhaps more achievable if the forms are scanned electronically at point of receipt. Key details on the temporary file should exactly match the completed form.*

Assuming that all data matches correctly, the referees must be verified. This would be done randomly and the process could again be automated. We believe that in time this element of the checking can also be largely automated using a secure online facility that can be used by referees.

Setting up the registration.

Once registration has been completed (following approval at stage 1), a unique identifier code (master identifier) would be generated. This code, equivalent in some basic respects to a unique national identification number, is both invisible and cryptographically protected.

This code is then placed onto a card. The government keeps a temporary record of the application information together with any supporting information, and then places this data, encrypted, onto the card. At this stage the identifier is dormant and so cannot be used until a final stage has been completed.

Distributed backup.

Once in receipt of the card, the newly validated citizen at leisure then attends an authorised Trusted Third Party (TTP) of choice (such as a bank, solicitor, local government office, court or police station). Each TTP is equipped with card reading machinery, secure data storage and a secure means of communicating with the centrally held data. The newly issued card is locally verified by a PIN and the biometric to authenticate the user. The TTP then communicates securely with the government's records for confirmation that the card is still valid.

The TTP downloads all remaining data relating to the applicant and places these on the card.

Once downloaded, all but the essential data held by government is removed. Essential data is possibly no more than the unique code, card number (which is invisible) and possibly the name of the cardholder. At this point the identifier becomes "active". The TTP keeps a secure backup of the data on the card, along with any certificates and biometrics.

***Note**. This process can be conducted privately through a privacy platform without the need for a TTP. The crucial element in this stage is that the data is securely backed up so the registration process does not have to be repeated if the card is lost.*

The individual now possesses a card, a unique identifier and a secure backup that can be updated at will.

Exploiting the system's potential

The envisioned national ID system would replace today's local non-electronic identifiers by *universal* identifiers that are processed fully electronically. This migration would *remove* the natural segmentation of traditional activities. In the case of a pub, if additional information was disclosed, say through presentation of a national ID card, malicious staff could steal this information, or this information can be abused in other ways. As a consequence, the damage that identity thieves can cause would no longer be confined to narrow domains, nor would identity thieves be impaired any longer by the inherent slowdowns of today's non-electronic identification infrastructure. Furthermore, service providers and other parties would be able to electronically *profile* individuals *across multiple activities* on the basis of the universal electronic identifiers that would inescapably be disclosed when individuals interact with service providers.

Ironically, the currently envisioned ID card architecture therefore has severe implications for the security and autonomy of service providers. When the same universal electronic identifiers are relied on by a number of autonomous service providers in different domains, the security and privacy threats for the service providers no longer come only from eavesdroppers and other traditional outsiders. A rogue system administrator, a hacker, a virus, or an identity thief with insider status would be able to cause massive damage to service providers, could electronically monitor the identities and visiting times of all clients of service providers, and could impersonate and falsely deny access to the clients of service providers.

Over the course of the past two decades, the cryptographic research community has developed an array of entirely practical privacy-preserving technologies that can readily be used to design a better national ID card. The system would not need to be centralised, could build on existing societal relationships to better ensure security and privacy.

Technologies such as digital credentials, privacy-friendly blacklist screening, minimal disclosure proofs, zero-knowledge proofs, secret sharing, and private information retrieval can be used as building blocks to design a national ID card that would simultaneously address the security needs of government and the legitimate privacy and security needs of individuals and service providers. The resulting ID card would minimise the scope for identity theft and insider attacks. A Federated solution would also create a more useful model and better suit existing relationships, whilst ensuring proportionate data practices.

These solutions are well known to the private sector, but are rarely exploited when Government endeavours to develop national identification systems. The reasons for Government reluctance to consider these technologies are many. One reason includes the poor design principles behind national ID cards, always perceived as large projects that enable only the full flow of information, rather than the proportionate flow of information. Another significant reason may be because these alternative authentication systems empower individuals to control the amount of information that is disclosed.

If the Government wishes to improve identification in general throughout British society it needs to consider all the relationships involving the citizen.

Notably, proper use of privacy-preserving techniques would allow individuals to be represented in their interactions with service providers by local electronic identifiers that service providers can electronically link up to any legacy identity-related information they hold on individuals. These local electronic identifiers within themselves are untraceable and unlinkable, and so today's segmentation of activity domains would be fully preserved. At the same time, certification authorities could securely embed into all of an individual's local identifiers a unique "master identifier." This embedded master identifier would remain unconditionally hidden when individual authenticate themselves in different activity domains, but its presence can be leveraged by service providers for security and data sharing purposes – without causing any privacy problems.

Designing such systems is possible, but the government's proposed scheme aims only to increase the links to and from, and enable the full flow of information across, sectors and other boundaries.

In Federated Identity systems, there are pluralities of Credential Providers (public and private sector) who issue cryptographic security tokens for representing identity in some limited domain or linked sets of domains. The credentials can be designed to permit records of transactions to be either linkable or unlinkable, or some spectrum of properties between with two. For example, it is possible for identifiers to:

- be bi-directional or unidirectional, so that multiple identities can be traced from one domain to another, but not in the reverse direction;
- for facts ("attribute values") to be asserted and trusted without disclosing a specific identity;
- for separate identities to be selectively united, either under the control of the individual or another party;
- for infringement of rules to be penalised by disclosure of identity if and only if infringement occurs.

Also, embedded master identifiers could be blacklisted across multiple segmented activity domains to ensure that fraudsters in one domain can be denied access to services in other domains, while preserving the privacy of other individuals. Similarly, service providers would be able to securely share identity assertions across unlinkable activity domains by directing these assertions in digitally protected form through the ID cards of their customers in a privacy-friendly manner.

There is thus ample scope for designing identity systems for e-government with rules that can be specifically tailored to intentionally isolated domains of health entitlement and patient records, taxation and benefit claims, border-control and travel, and inter-operation with private sector systems. The rules of each system would constitute the procedure for Data Protection compliance, and could allow good governance of data sharing for

legitimate public policy reasons, whilst limiting infringements of privacy to the minimum necessarily required by ECHR Article 8.

Such flexibility does not of itself answer difficult questions about how much data-sharing and non-consented identification is justifiable in a democratic society. However, adopting such a fine-grained system allows the processes of democratic legislation and oversight many more options than a monolithic identity system predicated on a unique and ubiquitously traceable identity for each individual. Monolithic systems, in comparison to Federated ID, have much poorer resilience and scaling, and offer nugatory privacy, security, and reliability protection.

The practice of illicitly loaning Federated ID credentials to other people is discouraged by the fact that those to whom a credential is loaned can damage the owner's reputation, incur liabilities in that domain and learn personal information.

In a limited way, biometrics can prove a useful tool. Simplifying the cryptographic details, the card could present a biometric template encrypted with a different key specific to the NHS, Asylum/Immigration etc. This can be designed in such a way that duplicate (encrypted) biometric identities could be detected and traced within a limited domain (e.g. an international border-control system), but ad-hoc data-matching across domains could not occur unless designed and authorised.

Therefore, the frequently made observation that the jurisprudence of ECHR plainly allows national identity cards must be reconsidered when contemplating a system based on a general purpose central biometric database and a monolithic unique identity that facilitates arbitrary infringement of Article 8.

Is there a "pressing social need" for a general purpose central biometric database if the interests of national security, the prevention or detection of crime, the enforcement of immigration controls, prohibitions on unauthorised working or employment, and efficient and effective provision of public services can all be accomplished with Federated Identity systems and biometrics compartmentalised to specific domains, physically stored only in tamper-resistant devices, and matched with offline biometric readers?

In summary, the national ID system as currently envisioned by government poses threats to the privacy of UK citizens as well as to the autonomy and security of service providers. While the card may well be acceptable for the internal needs of businesses that engage in employee-related identity management within their own branches, the privacy and security risks of adopting the card as a national ID card for citizens would be high.

Cost

The government's proposals will involve approximately 100 million person hours (7,000 person years) for personal interviews, document handling, checking procedures and management for registration of the entire population.

Using automated techniques and streamlined administration, the alternative system would involve perhaps one eighth of this workload. The kiosks and TTP backups will partially erode these savings, but these facilities will allow a citizen driven interface with the system, thus reducing the requirement for ongoing administrative, data input and support staff.

The absence of personal data held by the government will eliminate the need for a legal requirement on individuals to constantly update their file held in a central register. As we outline in the costs section of this report, this will produce a saving of between £1 billion and £3 billion over the rollout period.