A new way forward for an effective identity policy in the UK

By Dr. Edgar Whitley, Reader in Information Systems in the Department of Management and Research Co-ordinator of the LSE Identity Project, London School of Economics

Dr. Edgar Whitley is a reader in information systems in the Department of Management at the London School of Economics and Political Science and the Research Co-ordinator for the LSE Identity Project. Here Edgar provides Security-news.tv with his vision for an effective identity policy in the UK.

☐ The fate of the UK National Identity Service is increasingly uncertain, facing the dual threats of 'wise spending reviews' from the Labour government and immediate cancellation from the two main opposition parties. However, the need to identify, and more importantly authenticate individuals will increase rather than disappear as more and more activities take place online. Politicians and businesses will still be faced with the need for an identity policy that addresses the needs of individuals and organizations. The key question is, what principles such a new policy should adhere to?

Starting from the perspective of business (which can include the 'service' side of government as well), one body (the 'relying party') needs to know that the other is who they say they are (or have the attributes that they claim to possess) and they need to know the basis of this assertion (i.e. who is the 'identity service provider'?). Before deciding to interact with the individual, to provide services for them or to allow them access to some of their resources, the relying party takes a commercial decision based on the identity assertion being made. This commercial (risk) decision may include consideration of what is known about the identity service provider, an evaluation of any mediation activities and consideration of liability / repair issues if problems arise.

Identification and authentication

Identity policies seek to address the trust-related issues that arise from identification and authentication interactions. Thus, individuals may need to identify themselves or may wish to confirm that they are over 18 to access particular 'age-restricted' resources or services, or may need to confirm that they are entitled to particular government services or benefits. Identification is taken as a process whereby someone's identity is revealed ('This is Jo Bloggs'), whilst authentication is a process that results in a person being accepted as authorized to engage in, or perform some activity ('I am allowed to withdraw money from this bank account', 'I am Edgar Whitley' or 'I am old enough to buy alcohol'). Identification and authentication are therefore distinct activities with authentication typically undertaken far more frequently than identification.

The individual perspective on identity management is increasingly driven by privacy concerns and consumer choice. Just as it is no longer accepted that the government is necessarily the best (sole) provider of telephone services or water supplies, so it is not necessarily the case that identity services should be driven by the government. This is particularly the case when much of the data used to enroll in an identity scheme will be found in commercial databases held by credit reference agencies and others.

For commercial organizations, particularly those in high assurance environments, there is a particular emphasis on the initial enrolment, which might typically (but not necessarily) be tied to government-issued credentials. In such cases, the enrolment process might be described as 'identity proofing' and may also incorporate vetting processes. For other organizations however, this link to nationally-issued credentials is less important. Thus, in the case of age-restricted purchases, the relying party needs to trust that the identity document does confirm that the person satisfies the age requirement but

For commercial organizations, particularly those in high assurance environments, there is a particular emphasis on the initial enrolment.

this does not necessarily have to be a government-issued document as many other services providers (banks / schools / mobile phone providers, etc.) might be prepared to stand behind the age-related assertion. For example, a mobile phone company may already restrict access to 'adult' sites via its phone internet services based on existing age checking and can use the same processes to allow third parties, such as bars, to confirm that the phone user is over 18.

In other cases, the assertions might be provided by a low-integrity source that is appropriate for that context, so in an online game environment, the attribute that another player has particular powers might be provided by no more reliable authority than the game provider.

Despite these sophisticated requirements the resulting identity policy does not need to follow the same assumptions as the current UK Scheme and there are alternative design choices made in identity policies around the world. Thus, key assumptions underlying the UK Scheme – the collection, storage and use of irrevocable biometrics, the storage of vast quantities of personal data on centralized government databases and a complex legal regime that imposes a series of new duties on individuals to notify the government of changes in their personal circumstances – need to be reconsidered.

Perhaps the most important assumption to question however, is the strong link made between identity cards and passports. This link has existed since the earliest discussion of entitlement cards and has resulted in a single body, the Identity and Passport Service, being responsible for issuing both passports and identity cards.

The most important limitation of the link between identity cards and passports relates to the principle purpose of a passport, namely to facilitate cross-border travel.

The initial plan for the roll-out of identity cards was to be closely linked to the issuing / renewal of passports and the link continues with the unsupported assertion that the government was under an international obligation to update its passports and passport-issuing processes to include fingerprint biometric information.

Perhaps the most important limitation of the link between identity cards and passports relates to the principle purpose of a passport, namely to facilitate cross-border travel. The passport never was intended as the basis of identity assurance. Moreover, there are a number of situations in which the state might revoke the right of travel of individual citizens whilst not intending to revoke their right to use an identity card to assert their identity securely.

In the UK, passports can be withdrawn from those with a banning order issued in relation to the Football Spectators Act and the Football Disorder Act and there is also discussion that absent parents who fall behind in child maintenance payments should follow suit. These people however, cannot be denied the benefits of an identity card, but will instead be issued with an identification card that is very clearly marked to indicate that it cannot be used to travel within Europe.

Someone issued with such an 'identification card' that is not valid for travel in Europe will be able to use it to assert their identity when, for example, registering with a GP, collecting a parcel or opening a bank account.

However, the distinction between identity cards valid for travel in Europe and identification cards that are not valid for travel will also, of course, be observable by individuals not associated with travel, such as the GP's receptionist, the Post Office employee or the bank official. Further complications are likely to arise with the increasing requirements to provide personal and travel details up to 72 hours before departure and where online check-in is permitted. In these cases, the online registration and check-in systems of all participating airlines will presumably have to include a real-time 'valid for travel' checking function for UK identity documents.

Perhaps a more significant privacy problem from the link between identity cards and passports arises because the identity card has to satisfy the International Civil Aviation Organization (ICAO) requirements for Machine Readable Travel Documents (MRTDs). These requirements

MRTDs also print the holder's date of birth on the face of the card.

ensure that the documents are usable in a variety of situations from high-tech modern airports to border crossings where online connectivity is limited or non-existent.

This means that the main data about the holder of the card is found in human-readable form on the face of the card. Thus, passport pages typically include details of the holder's name, place and country of birth, expiry date of the document and details of the issuing authority. Crucially, MRTDs also print the holder's date of birth on the face of the card. This means that if the identity card is to be used as a basis for determining whether an individual is of the appropriate age to enter or use certain age-restricted products and services, the MRTD requirement automatically discloses their date of birth, which is more detail than is required to achieve this particular function.

There is no shortage of advice and exemplars that address many of the articulated goals of an effective identity policy:

Sir James Crosby (2008) Challenges and opportunities in identity assurance Archived at http://www.hm-treasury.gov.uk/d/identity_assurance060308.pdf

Information Assurance Advisory Council (2009) Identity assurance concluding report Archived at http://www.iaac.org.uk/Default.aspx?tabid=105

Edgar A. Whitley and Hosein Gus (2010) Global challenges for identity policies. Palgrave Macmillan, Basingstoke.

An identity policy that breaks the link with the passport however, opens up the opportunity for a much more privacy-friendly alternative that adheres to the principle of data minimization

This principle states that organizations 'should collect only what is essential', to be stored only for as long as is necessary.

recommended by the Home Affairs Committee amongst others. This principle states that organizations 'should collect only what is essential', to be stored only for as long as is necessary.

A corollary of this is that even if more extensive data has been collected, the principle of data minimization should also apply to the data that is disclosed and shared.

To illustrate this point, consider again the example of access to age-restricted services, such as entering a bar. Here the relying party (the bar manager) needs to know that the person buying the drinks is of legal drinking age and that the person claiming this attribute is the person presenting the identity credential.

The formal requirement in this situation, of course, is simply authenticating that a particular individual is able to access particular age-related services. The person's identity is not required. The age satisfying requirement is clearly a function of the relationship between today's date and the person's date of birth. It does not, however, require the disclosure of the data of birth (that is, whilst a person's date of birth falls within the set of data that would be collected even when following the principle of data minimization, it does not fall within the minimal set of data that needs to be disclosed).

It should also be possible to ensure that control over what information is disclosed remains with the individual.

It should also be possible to ensure that control over what information is disclosed remains with the individual. Thus, the individual could control whether or not to disclose that they are over 18 by requiring the bar manager to first authenticate that he / she is authorized to ask for proof-of-age authentication from bar guests.

This 'allowed-to-confirm-age' check can be undertaken in exactly the same way as the proof-of-age check is undertaken. The individual can also control that only confirmation of age data are transferred. This issue of symmetrical checking can be particularly significant for vulnerable groups, such as the elderly greeting someone claiming to be from their electricity company. That person's identity credentials can be checked in the same way and the householder can decide whether to let them into their property based on whether that person's identity credential has been issued by their electricity company. The processes underlying such a minimal disclosure process are infinitely scalable and allow for a market of authentication providers to exist, offering differing levels of authentication assurance. For example, those individuals who simply require the ability to confirm that they are able to access age-restricted services do not necessarily need this functionality to be provided by a government-based identification scheme. Instead the age-verification used by the device can be based on, for example, details held by their mobile phone company, bank or even education provider (school, university). This pushes the responsibility for confirming the date of birth of the individual, for example, onto these other organizations but given the relatively low level of risk associated with age-verification services, this is a manageable risk that these companies might be prepared to take.

This issue of symmetrical checking can be particularly significant for vulnerable groups, such as the elderly greeting someone claiming to be from their electricity company.

Despite the challenges an effective identity policy for the UK may face, it should be one based around the needs of citizens and organizations rather than just government. Information and communications technology will play a key role in implementing the policy and the UK is uniquely placed to utilize the best available technology to achieve this goal. ☒