eID: Identity Management in an Online World

Jerry Fishenden, London, England

Abstract: Reliable electronic identity (eID) lies at the core of delivering successful, trustworthy online government services. Yet in the move away from paper- and documentary-based forms of face-to-face identity management complex questions arise, such as "How can any user's true identity be proven?" This paper discusses proposed 'laws' for identity. It outlines a need for eID models that recognise the need for both integration and federation. And it looks at various national eID programmes, examining in particular the Belgian eID card and the proposed UK National Identity Card, summarising the extent to which these developments appear to conform to the proposed laws of identity. In a European context, federated trust approaches for user identity management are emerging as a compelling model – one that matches local, regional, national and international aspirations with the need for cross-issuer trust and recognition. An outline model of a federated user identity management framework is discussed that aims to tackle some of the most common issues facing online government services (both internal and cross-boundary). The paper concludes by outlining options for the evolution of improved eID frameworks.

Keywords: eID, Identity Management, privacy, digital identity, single sign-on

1. Identity and Electronic Identity

Electronic Identity (eID) has become a key issue, both for online commerce – where many citizens first experience the need for some kind of online identity – and for public sector organisations. In reality, many online "identities" are intended more as a convenience to both supplier and consumer than as a serious attempt to tackle the complex issue of identity. So how should we address the issue of verifying the identity of an individual in an online environment? And how could that identity be used for single sign-on to services provided by a variety of underlying government organisations?

Existing online identity verification models (such as those of the credit reference agencies, who use knowledge of individual-specific financial information to check online identity) apply within a restricted identity relationship: that which exists between the authenticating organisation and the individual. They cannot make any claims about other identity relationships which that individual may have (or claim to have). In the public sector, verifying identity online requires proof of identity relationships with government entities, not third parties.

This paper considers some of the initiatives attempting to tackle this problem domain.

1.1 The Problem of Identity Relationships

Identity spans many different contexts and purposes: for example, we have multiple individual identity relationships (one with our employer, one with our bank, possibly several with the many different parts of government). There are also role-based identities – a by-product of our current employment, or position. Equally, there are group identities ranging from families through to companies. And so too there are objects or resources, such as publications (using ISSNs) and books (ISBNs). Identity is a context-sensitive and multi-dimensional concept. Yet many identity solutions seem to assume a simple, monolithic model architected on the assumption of a universal identity that can be used for all interactions. To be successful, identity management solutions need to recognise that identity arises from contextual relationships between parties. Whilst it may be desirable to cluster or *integrate* some of these (for example, our dealings with some groupings of government agencies), others we may deliberately want to keep separate (such as identities used for online banking and access to our medical records) and *federate* instead. Both integration and federation are valid and complementary aspects of successful identity management.

The following Figure illustrates just some of the many identity relationships an individual citizen is likely to have with the State.

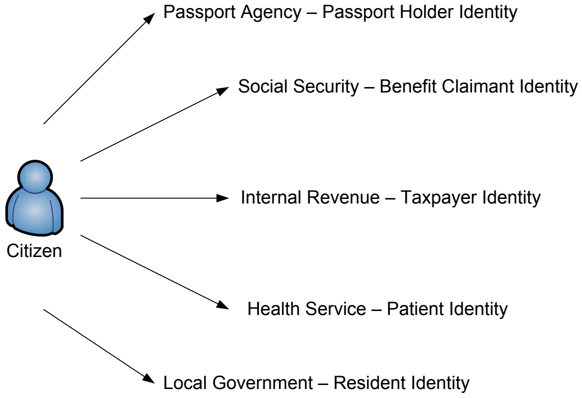

Passport Agency – Passport Holder Identity
Social Security – Benefit Claimant Identity
Internal Revenue – Taxpayer Identity
Citizen
Health Service – Patient Identity
Local Government – Resident Identity

Figure 1: a citizen typically has many identity relationships with government entities

The extent to which these many different identity relationships with government are kept separate is dependent upon political and cultural traditions. Some countries, such as the USA with its Social Security number, may index off a common identity relationship. Others, such as the UK, have a much more complex set of identity relationships in which the individual often maintains a separate identity relationship with each part of government.

E-government programmes typically assume the need for a citizen to use a consistent single online electronic identity – since a key objective is to provide a more ‘joined-up’ and integrated interaction with government services. Potential solutions to this issue involve either government moving towards a single identity relationship to replace the multiplicity of existing identities (a non-trivial task, since there may well be no single trusted identity relationship on which this can be rooted), or providing the citizen with the ability to maintain their different identity relationships whilst associating them with a single on-line credential. (A citizen might equally choose to continue to maintain their separate identity relationships, despite the complexity this could involve, for reasons of privacy.)

As well as multiple identity relationships with the State, we also maintain other identity relationships. These can be informal, such as those of family and friends, through to banks, employers, utility companies, airlines and online commerce outlets. Whether we wish to let any one of these many entities have visibility (or ownership) of our other identity relationships should remain a matter of personal preference. An eID card infrastructure will need to be clear about the degree to which that card allows the citizen to maintain their separate identity relationships without inappropriate bridging between parties: there should be clarity and transparency about who has control over the extent to which an eID provides access to the identity relationships which it manages.

1.2 The Problem of Identity Verification

Before we can benefit from the use of an eID, we need to verify that we are the individual who owns the identity relationships to be associated with that eID. In the paper world, proof of identity is typically paper-oriented: a birth certificate, copies of utility bills and so on. But such paper documentation in fact proves very little. The most commonly required piece of paper – a birth certificate – is merely a documentary record of an event in time: namely the birth of a child. It indicates nothing about whether the recorded event has anything in common with the person possessing the piece of paper. Given this, it is little surprise that identity theft is so prevalent: in the USA alone, approximately 7 million people became victims of identity theft in 2002/2003 (ITRC, 2005).

In reality, absolute proof of identity is almost impossible to establish: what we rely upon is a set of mutually-reinforcing, convergent identity relationships. So, for example, the fact that your doctor has known you for many years, your bank, local authority and so on is collectively assumed to demonstrate you have consistently claimed a particular name and identity with a variety of people and organisations over a sustained period. In some countries and cultures the problem may be less complex where existing paper-based national identity cards are already in use. But much will depend upon their issuance processes and the degree of identity verification originally conducted.

John Sergeant, the former BBC political journalist, quotes an example that shows how absurd our attitudes to identity can be:

> *I was on my way to talk to Tony Blair about Margaret Thatcher. The policeman on the gate greeted me in his customary way. "Hello, Mr Sergeant. Can I check your identity?" I was never sure if he realised he was being funny, but it always cheered me up. .. I found it oddly relaxing to have a policeman who knew me well look at my Westminster pass to see if my face matched the photo.* (Sergeant, 2005)

2. Towards an eID Framework

There continues to be debate about whether identity laws or identity principles are needed to develop a digital identity model. Thomas Barnett (Barnett, 2005) developed the concept of "Rule Sets" as applied to globalisation – with a proposition that conflicts and breakdowns occur when activity races ahead of the "Rule Sets" that govern that activity. Chris Ceppi (Ceppi, 2005) believes that Barnett's ideas have relevance to the complex issue of digital identity – which needs an Identity Rule Set. Kim Cameron's (Cameron, 2004) "Laws of Identity" however are not so much a matter of the "philosophy of identity", but the definition of a set of "objective" dynamics that constrain the definition of an identity system capable of being widely enough accepted that it can enable distributed computing on a universal scale (Cameron, 2004[2]). These laws are worth narrating here since they identify an emergent framework for effective identity management in an online world.

2.1 Cameron's "Laws of Identity"

1. The law of control
2. The law of minimal disclosure
3. The law of fewest parties
4. The law of directed identity
5. The law of pluralism
6. The law of human integration
7. The law of contexts

Figure 2: a summary of Cameron's 'Laws' of identity

Kim Cameron has set out seven 'laws' which cover the following:

- **1 – the Law of Control.** *Technical identity systems MUST only reveal information identifying a user with the user's consent*

  The principle of informed user consent is a widely recognised basis for general acceptance of – and trust in – an identity system.

- **2 – the Law of Minimal Disclosure.** *The solution which discloses the least identifying information is the most stable, long-term solution*

This too is a fairly well-established principle (included in the likes of Data Protection legislation) that any information held – and disclosed – should be the absolute minimum required to fulfil its purpose.

- **3 – the Law of Fewest Parties.** *Technical identity systems MUST be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship*

  This law ensures that no-one other than those who absolutely need access to identifying data are granted access. This is likewise in accordance with the basic laws of many countries.

- **4 – the Law of Directed Identity.** *A universal identity MUST support both "omnidirectional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles*

  Both parties in an interaction clearly need to identify each other – and whilst public entities need to prove their identity to many ("omnidirectional"), private entities (citizens) may wish to preserve and control their separate identities ("unidirectional").

- **5 – the Law of Pluralism.** *A universal identity system MUST channel and enable the interworking of multiple identity technologies run by multiple identity providers*

  This is a principle of identity interoperability – and assumes an architecture that mirrors the reality that identity itself is widely distributed.

- **6 – the Law of Human Integration.** *The universal identity system MUST define the human user to be a component of the distributed system, integrated through unambiguous human-machine mechanisms offering protection against identity attacks*

  Involvement of the human aspect, rather than a purely mechanistic approach, will only hold capable of preventing identity attacks and identity fraud/theft if the initial identity verification and issuance process is sound – and that the overall identity system is not vulnerable to social engineering or other forms of manipulation. For example, if someone else was able to claim *your* identity and have *their* biometrics associated with it – how would you ever prove that you were the person whom the identity system showed as being somebody else? In this context, biometrics are a useful additional authentication factor: not a panacea to the problem of identity management. The human integration aspects of eIDs present some of the most challenging aspects of this problem domain.

- **7 – The Law of Contexts.** *The unifying identity metasystem MUST facilitate negotiation between a relying party and user of a specific identity – presenting a harmonious human and technical interface while permitting the autonomy of identity in different contexts.*

  Being able to interact in an identity relationship and decide which elements of identity are required is an interesting consideration: for example, if a Web site needed proof that the holder of an identity was over age 21, that should not require disclosure of any aspect of that user's identity other than their verified age. It is important that such negotiations of appropriate information can be incorporated into the design of the interaction between users and relying parties.

Collectively these laws provide useful foundation principles for identity management against which eID programmes can be validated.

3. Online Identity Verification and Management

3.1 Verification Models

One method for online user identity verification is achieved by challenging users with a variety of questions and matching the answers provided against data already held against that particular claimed identity. This is how credit reference agencies such as Experian and Equifax work: provided the user responds appropriately, the credit reference agency will establish, to a calculated degree of validity, the identity of the person online. This is often referred to as knowledge-based authentication (KBA). At the USA's National Institute of Standards and Technology (NIST, 2004) symposium in 2004, Rudell (Rudell, 2004) characterised KBA as:

- the claimant does not need a previously established relationship with the relying party
- verification of an identity is based on information associated with and provided by the identity claimant
- the result depends on an acceptable level of consistency with information held by the authentication verifier

KBA 'proof of identity' is in fact proof of only one identity: the one we have with the authentication verifier. For a child who has never had any contact with a financial institution of any kind, or an adult who has chosen perhaps to remain in a cash-based society, such 'identity' checks with a credit reference agency would yield no results. And even when matches are made for an individual and the credit reference agency vouches for them, what does this mean? Such identity is limited to the context in which it was established. The fact that an Experian or an Equifax has proved someone is indeed John Smith is little use to a government department that has many occurrences of that identity and is indexed on the basis of another set of identifiers about which the credit reference agencies know nothing (such as a social security number, pension number or any one of the multitude of different identifiers by which the many parts of government choose to know us).

KBA can also be used for additional purposes such as setting up a reusable authenticator, or reclaiming a lost authenticator. Given that many interactions with government can be infrequent (such as an annual tax return), it is not uncommon for citizens to forget their eID if its only purpose is for use with government services: being able to reclaim a lost or forgotten eID can therefore be an important element of a well-designed system. The basis of e-government systems are likely to rely upon KBA – using information that is known only between an individual asserting an identity and the owning organisation (or an organisation trusted by the relying party). Such models for example are used by the UK Government Gateway, which challenges users with a set of 'known facts'. Verifying the identity of a citizen when setting up their access to an online system can include not only knowledge of specific identity relationship identifiers (such as unique departmental reference numbers), but also be backed up by reference to recent relationship information (such as the amount of a recent payment or bill).

The extent to which identity verification is required will depend upon the sensitivity of the service being accessed. Requests for a government benefits claim form to be sent to a citizen are not likely to require high levels of verification – whereas a request for an actual benefits payment is likely to require both verification of the individual and their asserted circumstances given the evident risk to the State of fraud or misuse. The various levels of online services provided by a government are consequentially categorised dependent upon their required levels of identity verification and authentication based upon perceived and actual risk metrics.

3.2 Government eID Projects

There are a wide range of ambitious identity management initiatives around the globe. Angola for example (Angola, 2005) is leading the first national eID project on the African continent. In Europe, Belgium (Belgium, 2005) has already started its own eID roll-out. The UK, the USA and many others are actively developing the legal framework for their own programmes. These projects range in scope and scale, from more traditional PKI style projects using smartcards with embedded chips, through to those that will also include biometrics. We will consider two countries – Belgium and the UK – and various aspects of their approaches to eID management on a national scale. In Europe, Directive 1999/93/EC of the European Union (EU, 1999) on electronic signature use provides the baseline for many European eID initiatives.

The Belgium eID card programme is already well advanced. This is largely a traditional PKI style deployment, replacing an existing paper-based identity card system with a smartcard based system that incorporates digital certificates.

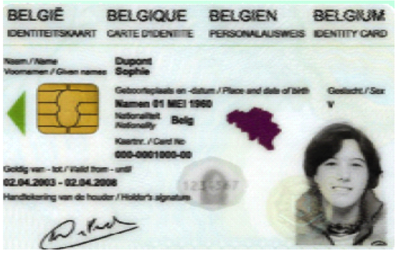


Figure 3: Illustration of the Belgian eID Card

The Belgian eID card is the digital equivalent of the previous paper based identity card. As illustrated in the preceding Figure, it is a credit card sized plastic card with the citizen's photo, full name, gender, handwritten signature, nationality, place and date of birth, and card and National Number. The chip included on the eID card contains the citizen's identity information and address together with identity and signing certificates. This enables the chip to be used for authenticating information and generating digital signatures that are regarded as equivalent to handwritten signatures. The card is valid for 5 years with processes in place to handle lost, stolen and damaged cards.

As Belgium already has a national identity card, albeit paper-based, the issuing procedure for the eID relies to a large degree upon this existing card for proof of identity. The citizen first attends a government office to request the eID card, using their existing paper-based card to prove their identity. Their picture is captured. A few weeks later, the citizen will receive a letter with a PIN and a card activation code in the post. The citizen returns to the government office to collect the card, taking that letter with them. The information in the letter is used to activate the eID card, which will be exchanged for their current paper-based card. The citizen will generate two test digital signatures: one identity and one qualified signature to prove the proper functioning of the eID card. This activation process is estimated to take around 15 minutes per card. The cost to the citizen is 15 Euros.

During the pilot phase, some 4,500 eIDs were issued each month. Once up to full national production, some 1,500 eID cards will be provided and activated each working day. More than 97% of the 589 Belgian municipalities are already issuing eIDs and it will be used for a wide range of purposes, spanning e-government (uses such as official document requests, online voting, tax returns, online access to services) through to digital rights management, e-banking, authenticated email and other optional uses. Third party companies have announced support for the Belgian eID card for online authentication to Internet services. From a privacy perspective, citizens can also choose to de-activate the authentication and signature functions.

Law	Description	Assessment
1	The Law of Control	*The system holds minimal information and only discloses it with the user's active consent*
2	The Law of Minimal Disclosure	*The system holds only a subset of personal information, deemed the minimum necessary for its stated purpose*
3	The Law of Fewest Parties	*Only appropriate organisations are granted access to personal information*
4	The Law of Directed Identity	*It is not apparent that the Belgian eID card will support anything other than common correlation handles*
5	The Law of Pluralism	*Whilst PKI-based, the eID system proposed appears based on a non-pluralistic model rather than the interworking of multiple identity technologies from multiple identity providers*
6	The Law of Human Integration	*The card provides only two factor authentication (possession of the card and knowledge of the PIN to be used with its digital certificates)*
7	The Law of Contexts	*The proposed approach does not appear to facilitate negotiation between a relying party and user of a specific identity, denying the autonomy of identity in different contexts. If the card was limited purely to a subset of government-related interactions this might matter less – but the card has clear aspirations to be more than this and engaged in more complex identity relationships. It is not clear that the current model will be able to provide suitable support across other identity contexts*

Table 1: Summary "Cameron's Laws" assessment of the Belgian eID Card

By contrast to the Belgian eID card, the proposed UK National Identity card is aiming by 2010 to create a large central database and a system of eID cards which will include chips that carry both personal information and biometric identifiers. As with the Belgian eID, this information will include each citizen's name and address but in addition it is proposed to include biometric information such as fingerprints, facial scans and iris scans. This data will also be replicated in a central database to be known as the National Identification Register.

Ahead of these formal eID cards, UK passports and driving licenses are likely to incorporate aspects of the new system, with biometric facial identifiers included on all newly issued British passports by the end of 2005. Feedback from this deployment will also be fed into the eID card programme. However, reservations have been expressed by a range of parties, including the major credit card companies, that biometrics are not mature enough to be used in this way and on this scale (Rohde, 2005).

Law	Description	Assessment
1	The Law of Control	*The proposed UK system has the potential to enable access to personal data without the consent or knowledge of the user concerned*
2	The Law of Minimal Disclosure	*The proposed system would hold information about an individual and potentially make this available to variety of authorised parties: this is part of the function of the centrally maintained register*
3	The Law of Fewest Parties	*A wide range of organisations potentially have access to the personal information held in the central register since it is intended to help with data-sharing between government organisations*
4	The Law of Directed Identity	*The proposed system appears to assume a monolithic correlation handle and a notional single government identity*
5	The Law of Pluralism	*It is not currently clear whether the proposed system would be based on a single supplier model rather than an interoperable model from multiple sources*
6	The Law of Human Integration	*Three factor authentication is envisaged: possession of the card, a PIN and combinatorial biometrics*
7	The Law of Contexts	*There appears to be no provision for the autonomy of identity in different contexts. Current proposals indicate that the scheme will attempt to bridge multiple separate identity relationships*

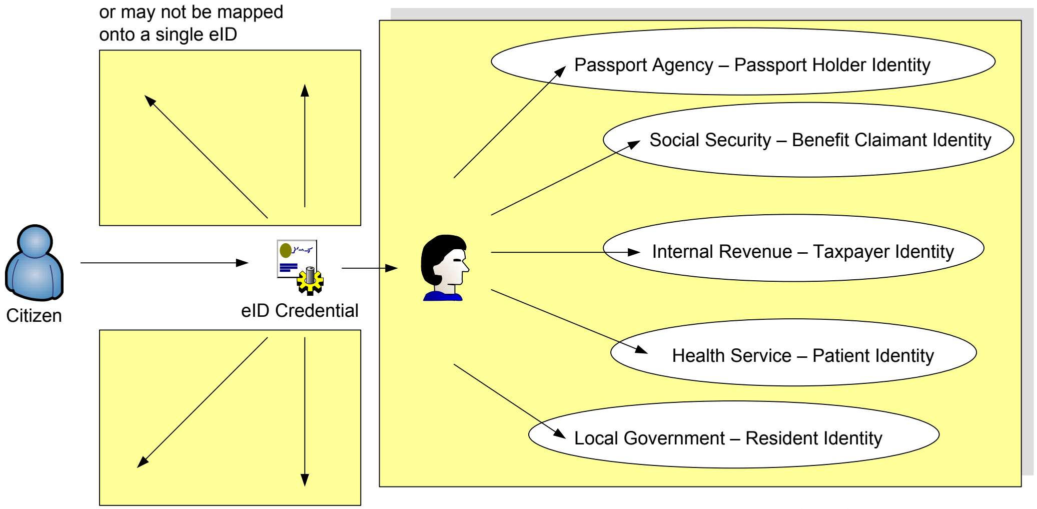
Table 2: Summary "Cameron's Laws" assessment of the proposed UK National ID Card

The UK does not currently have a national identity card, so the problem of identity verification and authentication of individuals is an additional factor to be resolved. Some clues for how this could be addressed may be provided by an existing online identity management solution already available in the UK: the UK government's 'Government Gateway'. Since early 2001 this system has formed the backbone of the UK's e-government programme for delivery of government services online. In excess of five million registered users are now making use of this system.

The Government Gateway's identity management services provide the ability for UK citizens to associate an eID with a variety of government identity relationships. The credential used can range from userID and password through to the most sophisticated smartcards and biometrics – but in practice, userID/passwords have proved the credential with the highest take-up, with some third party PKI-based digital certificates also used, mainly by businesses. Users are able to assert a particular identity relationship, undertake some verification of that claimed identity (using KBA) and then associate it with their chosen online credential. Over time a user can associate against their credential the many different identity relationships that they have with government organisations.

The end result is that the citizen can choose to end up with a single eID that they can use with all online government services, regardless of the fact that those services continue to maintain their many separate identity relationships with the citizen. This is illustrated in the following Figure.

non-government identity relationships – which may or may not be mapped onto a single eID


Passport Agency – Passport Holder Identity
Social Security – Benefit Claimant Identity
Internal Revenue – Taxpayer Identity
Health Service – Patient Identity
Local Government – Resident Identity
Citizen
eID Credential

non-government identity relationships – which may or may not be mapped onto a single eID

eID mapped to a common cross government identifier – for use across multiple government identity relationships, each of whose identifiers are mapped back to the one common root. Although controlled by the same eID, each identity relationship is kept separate from each of the others, preventing inappropriate breaches of personal privacy.

Figure 4: Government Gateway mapping of government identity relationships

Even where third party digital certificates are issued – which involves a degree of identity verification set out in UK government guidance (HMG, 2003) and realised in practice by an industry group known as t-scheme (t-scheme, 2005) – the Government Gateway effectively treats the credential initially as anonymous: since it has no context concerning government relationships and identities. The only identity relationship established at the time the digital certificate is issued is the one between that individual and the issuing organisation. It is only as a user asserts and then proves (or fails to prove) their ownership of a particular government identity relationship that their credential can be legitimately linked to that relationship. Each identity relationship mapped to their credential remains separate and under the user's control: each government entity continues to see only the unique relationship identifier relevant to their services, not the user's wider identity relationships.

Law	Description	Assessment
1	The Law of Control	*The Government Gateway holds only a lightweight index between different identity correlators mapped back to a single eID/credential*
2	The Law of Minimal Disclosure	*The Gateway holds and provides minimal information and discloses only information relevant to the interrogating party*
3	The Law of Fewest Parties	*The Gateway maintains each identity relationship separately so that, for example, one government entity never gets to see information about another identity relationship*
4	The Law of Directed Identity	*The Gateway maintains a separate correlation identifier for each relationship. However, it does also hold a universal correlation identifier*
5	The Law of Pluralism	*The Gateway uses a range of trusted third party identities and credentials (including third party digital certificates) as well as its own self-issued credentials*
6	The Law of Human Integration	*The Gateway offers only userID/password directly. It does offer two-factor authentication with the use of third party digital certificates and smart cards, but no unambiguous human integration*
7	The Law of Contexts	*As it maintains details of each identity relationship separately from each other, the Gateway provides reasonable conformance*

Table 3: Summary "Cameron's Laws" assessment of the UK Government Gateway

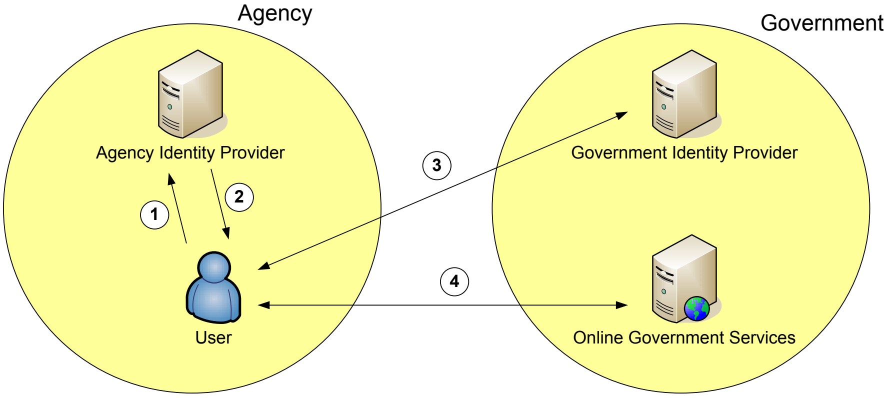
Based on these outline assessments of the various schemes, it is noted that the proposed UK National Identity Card appears to offer a less functional and conformant identity management solution than the UK government already has developed with its Government Gateway.

4. Federated Identity and Federated Trust

For an eID to work across many different services, trust is an important consideration. Current models are largely predicated on narrow trust – where entities only trust the eID they themselves have issued. For example, VISA will only trust a VISA issued chip and PIN card. There are clear commercial and branding reasons for this model on the supplier side and there may well also be privacy considerations on the consumer/citizen side (for example, deliberately keeping certain types of transaction on a particular bank card).

Federated trust is an increasing area of activity, ranging from the WS-I's WS-Federation specification model (WS-I, 2003), through the Shibboleth (Shibboleth, 2005) project in education and academia, the use of SAML (the Security Assertion Markup Language) tokens (SAML, 2004), all the way to other less mainstream approaches such as LID (Lightweight Digital Identity) (LID, 2005). These all attempt to address aspects of all or some of the same problem domain – defining mechanisms that can be used to enable identity, account, attribute, authentication, and authorisation across different trust realms.

An example of how such trust models work, using WS-Federation as a model, is illustrated in the following Figure.



1. User authenticates to internal agency Identity Provider
2. User obtains federation token from internal Identity Provider – claims to business level agreement between Agency and Government Identity Provider
3. User obtains security token from Government Identity Provider – claims specific to cross-government services
4. User accesses online Government services with Government token

Figure 5: federated trust relationship between two organisations

Cross-realm trust is relatively commonplace in enterprise environments: national populations present a massively scaled-up instance of the same problem space, with the additional challenge of operating outside a controlled perimeter. The aspiration is to achieve a model that places identity in the hands of its owner and ensures there is a clear understanding of where risk lies between relying party and authenticating party. A successful model also needs to be able to accommodate a financing system that ensures the relying party (who take the benefit of authenticated identity for their services) pays any fee required to the authenticating party (who take the risk). Such financing models already exist, for example, for credit reference agencies that provide identity verification services to banks and other organisations.

The use of a trust architecture provides the potential for multiple token issuers to provide tokens that can be trusted by a relying party. Such tokens become analogous to the type of distributed trust only previously possible with a PKI based on digital certificates. In the model illustrated in the preceding Figure, multiple trust relationships can exist. The mechanism of security token acquisition and exchange is at the machine-to-machine level, not one that involves user intervention. And federated trust is becoming closely integrated with existing directory authentication systems: the user experience will be that they sign onto their PC and are then able to access all appropriate services without needing to re-authenticate or to use different logon IDs for each of the many different systems involved. This is equivalent to the single sign-on experience that currently exists only inside an organisation, but extended to external services where trust relationships exist.

5. Privacy

Many users remain distrustful of online systems and the potential abuses of personal data that could take place. Such concerns are not unique to online identity management (many are echoed by privacy and citizen campaigners around paper-based identity cards). It must be possible to demonstrate that identity providers or maintainers cannot violate privacy.

Existing digital identity models have not been overly problematic in this regard, since each identity is narrowly defined and used often within only one relationship (e.g. a bank card from one bank is only used with that bank, amazon.com is separate from borders.com, an employee ID is only used within and for the purposes of that employment). The drawback is that this model produces a great deal of inconvenience in an online environment and a complex of online identities and credentials. But equally, with proposals for more integrated online identities, the opposite issue – of misuse – becomes more problematic.

Taken from this perspective, a model is required that establishes the nature of information to be exchanged by participants of online services. The PRIME project (PRIME 2004) for example is exploring a framework that would ensure for each transaction a precise specification of what pieces of certified data should be revealed to each participant. As per Cameron's Seventh Law (of Contexts), such a framework must be able to facilitate an appropriate negotiation between a relying party and the user of a specific identity.

In reviewing the proposed UK eID initiative, the Houses of Parliament Joint Committee on Human Rights has raised some far-reaching questions about the nature of any central register associated with eIDs and its impact on human rights (JCHR 2005). The European Court of Human Rights has held that "information relating to private life" is to be construed broadly (Niemitz v Germany, 1993 *et al*) to include any information relating to an identified or identifiable individual (Amann v Switzerland, 2000 *et al*). In many areas the proposed UK central register was found by the Joint Committee to be in breach or potential breach of Article 8.

It is not clear that the development of a central electronic register is either necessary for the purposes of user identity verification, or that it provides the best technical solution. Alternative models exist – which include the potential for an identity verification system that can operate both online and offline: and require no central data or information on an individual to be held at all. Such approaches range from self-contained identity cards which can be retained under the control of the individual at all times, to the type of online distributed architecture enabled by a federated model.

6. Summary

This short paper cannot do justice to a rich and complex topic such as eID, but it has highlighted some of the main current issues and developments in the use and adoption of eIDs. To quote Cameron:

> *… current identity systems are too hard to deploy. They are too hard to understand. And too hard to use. The different systems exist in silos, making everything harder still … Many people feel the only way to get anything done quickly is turn protection off - maybe with the intent of turning it on later... But if you forget, there is no way to know what you've left undone or who can access what.*
>
> *All of this needs to be fixed. At the center of everything is the construction of a unifying and easily used identity system.* (Cameron, 2005)

We should take advantage of the learnings from early eID deployments such as the Belgian eID and the UK's Government Gateway project and combine these with the approaches set out in "Cameron's laws". This emergent framework of laws for effective identity management should be recognised in the evolution of effective national eID programmes. It offers the prospect of improved reliability and security, as well as better protecting the privacy of the individuals concerned: a framework where identities can be exchanged safely between the mix of identity providers, providing a good fit legally and to the nature of identity itself. Such characteristics for an eID solution recommend themselves for serious consideration to countries keen to ensure successful eID programmes that also respect an appropriate balance between the individual and the State.

7. Acknowledgements

The author thanks those many colleagues working in the field of identity management who have provided input to the development of the thinking outlined in this paper. Worthy of special mention are Phil Stradling, Kim Cameron, Caspar Bowden and the EURIM PI Subgroup.

References

Amann v Switzerland. (2000). *30 EHRR 843 para. 65; Rotaru v Romania (2000) 8 BHRC 43*

Angola. (2005). *Agreement on Information Technologies Promulgated, Angola Press Agency* (http://fr.allafrica.com/stories/200502140447.html)

Barnett. (2005). http://www.thomasbarnett.com/weblog

Belgium. (2005). *The Belgium National eID Card Programme,* http://www.esat.kuleuven.ac.be/~decockd/site/EidCards/belpic/mySlides/belgian.eid.card.technical.overview.pdf

Cameron. (2004). http://www.identityblog.com

Cameron. (2004[2]). http://www.identityblog.com/stories/2004/12/09/thelaws.html

Cameron. (2005). Feb 17 2005 entry, *Why Identity is Part of the Picture: What Stands in Our Way?*, http://www.identityblog.com

Ceppi. (2005). http://ceppi.blogs.com/2005/01/identity_rule_se.html

EU. (1999). *A Community Framework for Electronic Signatures*, http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

HMG. (2003). *HMG's Minimum Requirements for the Verification of the Identity of Individuals.* Online on http://www.govtalk.gov.uk

ITRC. (2005). *The Identity Theft Resource Centre*. http://www.idtheftcenter.org/facts.shtml

JCHR. (2005). *The Joint Committee on Human Rights, Fifth Report. Houses of Parliament, UK.* (see www.publications.parliament.uk/pa/jt200405/jtselect/jtrights/35/3506.htm)

LID. (2005). *The Lightweight Digital Identity*. http://lid.netmesh.org/

Niemitz v Germany. (1993). *16 EHHR 97 para. 29; Halford v UK (1997) 24 EHRR 52*

NIST. (2004). *Knowledge Based Authentication (KBA) Symposium*, http://csrc.nist.gov/kba/agenda.html.

PRIME. (2004). *Privacy and Identity Management for Europe* (see http://www.prime-project.eu.org)

Rohde. (2005). *UK Parliament passes biometric ID card plan*, Laura Rohde. http://www.thestandard.com/internetnews/000956.php

Rudell. (2004). *KBA Applicability to e-Government*. Mindy Rudell, Dick Stewart, Robin Medlock, Angel Rivera. See http://csrc.nist.gov/kba/Presentations/Day%202/Rudell%20-%20KBA%20Applicability%20to%20e-Gov.pdf

SAML. (2004). http://www.oasis-open.org/specs/index.php#samlv1.1

Sergeant. (2005). *Maggie – Her Fatal Legacy*. p 12, para. 1. Macmillan.

Shibboleth. (2005). http://shibboleth.internet2.edu/about-shibboleth.html

t-scheme. (2005). See http://www.tscheme.org/

WS-I. (2003). WS-Federation. http://www-106.ibm.com/developerworks/webservices/library/ws-fed/