“Some thoughts on the underlying logic and process underpinning Electronic Identity (e-ID)”

Originally published in Information Security Technical Report Vol13 no2

Tony Collings OBE
The ECA Group
Struan House
Pangbourne Hill
Pangbourne
Berkshire
RG8 7AS

tonycollings@ecalimited.co.uk
www.ecalimited.co.uk

Would you build an aeroplane without understanding the fundamental principles of flight? You would hope not. Yet this question is not as irrelevant as it may seem. Over recent years there have been many examples of identity schemes being proposed and enthusiastically endorsed with only the sketchiest understanding of the principles of Identity Management. In this article I have outlined the fundamental issues that underpin any Identity or e-ID Scheme and any attempt to turn them into an automated e-ID delivery. It is a huge and complex subject, I have tried to keep it simple, to cover some of the major international issues and discuss some of the most significant identity management principles and make it interesting. I will not dwell on technology, but on the far more operationally sensitive / fragile aspects of people and process.

As citizens, we have become accustomed, and reliant, on electronic tokens or keys that we accept as giving us a certain level of utility and underlying 'trust'. We use these with commercial electronic transactions such as those with our banks and financial exchanges and to a more limited extent with local and central government. When it comes down to the protection of personal identities and information there is huge disparity in the levels of integrity, trust and assurance that the electronic token, purporting to represent you or I, is correct, irrefutable and secure.

Until recently very little regard was paid to the underlying processes that collect the information and data used to award these tokens, or to ask whether these processes and procedures are of sufficient rigour to be used to award and guarantee that we are who we say we are. Now the UK Identity and Passport Service for (IPS) for example as anew departure will check the information you give for a first time passport application against data held by public & private sector organisations to check your identity.

The underlying trust and Integrity of the process to award an identity is key. I will return to this point as we develop our discussion on the real attributes of identity, and why they matter, before they become electronic tokens for e-ID. What I have described in the following pages is a review of some of the major issues that need to be considered if we are to gain a better understanding of current Identity, Data Handling, and Assurance. It is vital to understand the fundamental credentials that make up an individual's identity - the origins of each, their levels of assurance, interactions, dependencies and inter-operations at both the people and process level before attempting to impose technical solutions that will inevitably fail without this knowledge and rigour of approach.

Why Identity Matters

Identity is the dynamic collection of all attributes related to a specific entity, normally a citizen but the concept can be extended to include an enterprise, or object. It is generally recognised that an identity is what allows entities to be distinguishable. This is what makes identity a key component in numerous economic, social and administrative transactions. The ability to link a set of information to its owner and the effective and secure handling of entity-specific data are essential to numerous different interactions. Consequently organisational and technical infrastructures – Identity Management Systems - have developed to define, designate, specify authorisation levels, assign roles to and administer the identity attributes related to specific groups of people, such as employees, customers, patients or simply citizens.

Identity matters very much and its significance has almost gone un-noticed as our highly complex and interdependent technological society has evolved. It is only with the debate surrounding ID card systems and the rise of internet and electronic fraud that there is any awakening and understanding of the real issues that underpin identity and its impact upon society.

The European Commission viewpoint

EU NATIONAL ID CARDS

Many individual EU member states have significant national Electronic Identity experience.

In Europe, individual EU states have already issued eIDs to more than 22.5m citizens, with testing in Spain, Portugal; Germany and France considering eID systems and UK in process of resurrection.

The EU recognises that achieving common security standards in issuing procedures is highly desirable and that application, enrolment and issue form a single process, all of which needs to be as secure as practicably possible. The procedure includes people, processes and technology and they are all important. However, proportionality is important in that the costs and resources involved must be balanced with the likely result.

Significantly in the EU Council Conclusions of December 2005, Member States recorded the following agreement: "…to work towards putting in place the following minimum standards relating to the security of issuing processes":

And that:

- Applicants should appear in person at least once during the issuing procedure for identity cards;
- Applications should be verified by authorised personnel against existing databases which should be regularly updated, for example, civil registers, passport and identity cards databases or driving licence registers;
- Monitoring of the issuing process is recommended, including where processes are carried out by sub-contractors, and this should include regular audits;
- In principle, no single member of staff should carry out every part of the issuing process for an individual; and
- Secure storage, transport and transmitting of data and components of documents should be ensured;
- Checks should be made against any available watchlists or list of known forged documents;
- There should be secure, resilient back-up facilities for data;
- Only authorised personnel should be able to enter the initial application data on the database;

Across the European Union the Pan European electronic-Identify Management Framework (e-IDMF) recognises that:

"For eGovernment and eBusiness to function to their full potential, people need a secure, convenient and effective way of identifying themselves – replacing signatures and stamps used on paper – when using electronic communication. To make this a reality, EU Member States are investing tens of billions of euros in interoperable Electronic Identity Management (eIDM). Electronic Identity Management is a cornerstone of the implementation of the full range of eGovernment services, for both citizens and businesses, across the Union. As more government, personal and commercial transactions are conducted electronically – especially where documents exist only in digital form – parties need to be sure of a person's or an organisation's identity".

The European Commission believes that inter system reliability will boost confidence in the acceptability and use of e-ID across the EU. Signposting their roadmap to e-ID Management they state that:

"A reliable system of eIDM means citizens, businesses and government departments (even in different Member States) can identify themselves and certify their transactions accurately, quickly and simply. Widespread confidence in eIDM will enable the day-to-day transactions between public agencies and people and businesses to move on-line. That move will lead to gains in efficiency in public services, and corresponding gains in time and money for citizens and businesses through simplifying their dealings with government agencies. Making sure that systems are interoperable is also a critical part of reliable eIDM. EU-supported ICT projects aim to help regions and Member States develop eGovernment services which, while meeting local needs, are capable of working with systems from other regions and countries in Europe – something that Member States working in isolation would struggle to achieve otherwise".

An EU sponsored case study recently (IDBaleares : **www.identitatdigital.net**) recognised that:

"Digital Identity" is an exhibition held at the Sa Nostra Cultural Centre (Palma) which presents the concepts and the basic tools for creating and managing a digital identity. Following the sentence from Anil Dash, "I am the primary and principal source of information on myself", "Digital Identity" is a representation of ourselves, "auto constructed" on the web when we create a web domain, publish texts, photos, video, geographical localisations or simply when we leave traces of ourselves on the Internet though interactions, communications or interventions which we carry out with other digital individuals. The project includes the use of web spaces by a mannequin[1] (authors comment) called Josomid, the host and reporter of the project. In all those virtual spaces, Josomid has been finding out about the construction of digital identity and has been reflecting on the topic. It has published photographs and videos on Fotologs and Youtube. In addition, to further promote social relationships over the Internet, it is working on its positioning in cyberspace through spaces for content and relations like Twitter and Orkut. It is also profiling its digital identity based on the music listened to via LastFM. "

I included this case study to illustrate how those born in past 25 years view the credentials and attributes of identity as an extension of their persona and as a statement of their whole personality and lifestyle. That is why so many citizens use social websites in such an unguarded and open manner.

The EU Identity Juggernaut around the corner

The EU e-ID Management project has a roadmap to achieve by 2010. It aims to deliver a Europe-wide e-ID infrastructure as part of e-business enablement across the Commission. This will create an EU wide federated e-ID system of national services, each of which will differ in scope, application, ambition, technology and other factors.

This initiative, if successful, will directly affect every citizen and may eventually replace many other familiar icons, such as passport or ID cards, driving licences, access cards and social security/benefits cards, which many associate with freedom of choice and independence. There are a number of social, legal and acceptability issues that I will not cover here. What is inescapable is the lack of clear guidelines for identity standards with existing national standards being used as appropriate. At present the Commission is attempting to meet its business objectives with a light touch but ultimately e-governance will be the greatest challenge with the subjects of privacy and data-sharing heading the list. A federated system is not perfect and will not give consistent results for border control or law enforcement but is an acceptable first step for many. It ducks many of the deeper questions on definitions and standards. Work is, however, going on in these areas.

At the most basic Pan-European level these definitions might be seen as follows:

- "Identification" is the process of using claimed or observed attributes of an entity to deduce who or what the entity is. Identification in general refers to a process of deduction based on a set of information allowing determination to whom a given person is (with varying degrees of reliability).
- "Authentication" is the corroboration of the claimed identity of an entity and a set of its observed attributes. Authentication implies that a decision is made based on the actual corroboration of information, implying a larger degree of dependability.

The EU eIDM i2010 is unprecedented in terms of ambition, scale, complexity and variety of goals for the vision. Ultimately it will apply to electronic identities no matter how differently conceived and operated within the EU.

The USA

Following the experience of 9/11, the US Government took the whole question of Assured Identity very seriously indeed. Initially directed at a mechanism to assure identity of those where it had a measure of direct control, Homeland Security Presidential Directive 12 (HSPD 12) was issued on August 27, 2004, entitled "Policy for a Common Identification Standard for Federal Employees and Contractors." This directive drove the promulgation of a Federal standard for secure and reliable forms of identification for all Federal employees and contractors working for the US government. It further specified secure and reliable identification that:

- Is issued based on sound criteria for verifying an individual employee's identity
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Is issued only by providers whose reliability has been established by an official accreditation process.

[1] It is not clear if he is a mannequin, a manikin or an avatar?

The directive stipulates that the standards include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application Executive departments and agencies were required by August 2004 to implement the standard for identification issued to Federal employees and contractors in gaining physical access to controlled facilities and logical access to controlled information systems. To speed things up the US government gave the US Department of Defense (DoD) the lead to base initial identity cards and Personal Identity Verification (PIV) assurance standards on their extant Common Access Card.

The US authorities point out that the security provided by the PIV system is dependent on many factors outside the scope of the HSPD 12 standard. Upon adopting this standard, organisations must be aware that the overall security of the personal identification system relies on:

- Assurance provided by the issuer of an identity credential that the individual in possession of the credential has been correctly identified.
- Protection provided to an identity credential stored within the PIV Card and transmitted between the card and the PIV issuance and usage infrastructure.
- Protection provided to the identity verification system infrastructure and components throughout the entire life cycle.

Finally the US authorities point out that:

“Although it is the intent of the standard to specify mechanisms and support systems that provide high assurance of personal identity verification, conformance to this standard does not assure that a particular implementation is secure. It is the implementer’s responsibility to ensure that components, interfaces, communications, storage media, managerial processes, and services used within the identity verification system are designed and built in a secure manner

It was the lead set by HSPD12 and the US National Institute of Standards and Technology (NIST) Standards FIPS 201, the personal Identity Verification Standard that led to the widespread issuance of government ID cards for Federal employees and contractors. The ‘First Responder’ ID card programme, was introduced to deter the ‘Walter Mitty’[2] impersonation of emergency response staff. Whether it be the border crossing card or the mandatory requirements for the US Visits programme, the US government are taking the whole question of identity, personal identity verification (biographical with biometrics) and its’ use electronically very seriously indeed.

International perspectives

I have included a small example of international attempts to grapple with the complexities of making identity management work, collaboratively and commercially, as an international Identity Proofing and Verification process and practice. It is only one example of many but illustrates the practical challenge well:

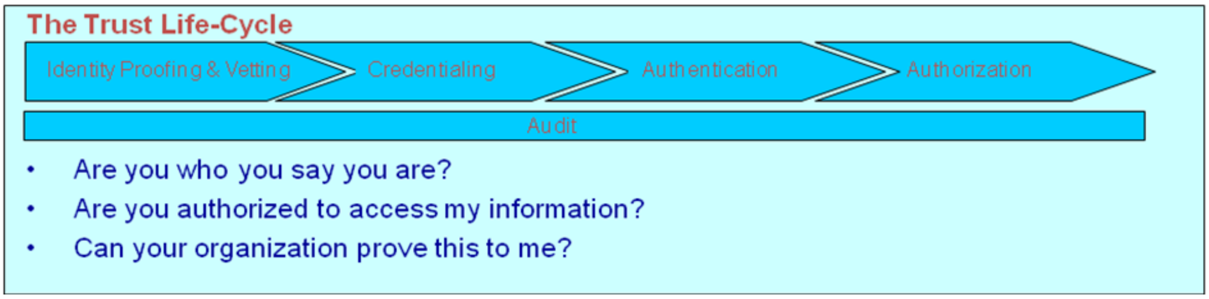
The Transatlantic (now Transglobal Secure Collaboration Programme (TSCP) describes itself as:
“The only government-industry partnership specifically focused on facilitating solutions to the most critical issues in Aerospace and Defence (A&D) today: mitigating the risks related to compliance, complexity, cost and IT that are inherent in large-scale, collaborative programs that span national jurisdictions. To do business in the world today, A&D companies must balance the need to protect intellectual property (IP) while demonstrating willingness and ability to meet contractual requirements from government customers for auditable, identity-based, secure flows of information. This duality requires that security be both within organisations and across extended supply chains and partners.”

The challenge TSCP faces is one of establishing a life cycle of trust in Identity. This is verified by our work with the International Proofing and Verification Working Group. The complication is that an employee of an aerospace or defence company is at one and the same time a citizen, an employee, a role holder with authorisations and permissions including national security clearances and a member of a collaborative consortium operating across national, EU, international and US Federal boundaries and borders. Add to this

[2] A fictional character with a vivid fantasy life

the complexities of national, NATO, US security regimes, export controls, IPR etc and the importance of identity credentialing, approval and assurance is pivotal.

The trust life cycle might look something like this:[3]



The Trust Life-Cycle

Identity Proofing & Vetting

Credentialing

Authentication

Authorization

Audit

- Are you who you say you are?
- Are you authorized to access my information?
- Can your organization prove this to me?

TSCP has 3 basic requirements for trust in identity within its community

1. Prove that you are who you claim to be.
2. Prove that you have permissions to be able to access specific information and/or carry out actions.
3. Provide 3rd party evidence that you are operating to common policy.

In the UK

Intellect, the UK security technology industry association, recognises the value of Identity and Identity management as:

"An enduring feature of modern society, delivering significant benefits to those who can authenticate themselves and entailing serious repercussions to those who cannot".

At present citizens rely on large commercial organisations and on government to safeguard personal information and keep it from being used for malicious purposes.

There are a number of initiatives regarding the identity debate in the UK

- The National ID Card
- The Crosby Report on challenges and opportunities in Identity Assurance
- The Data Sharing Review

The National Identity Scheme (the ID Card)

David Blunkett, when Home Secretary in November 2004, stated that:

"A national ID cards scheme will provide a `**gold standard**` for protecting individuals from the modern day crime of identity theft, protecting public services for those who are properly entitled to them, and helping us tackle crime, terrorism, and illegal immigration and working".

"The Register is about proving people's identity, but to a level that shows whether they are entitled to particular services. Services are a function of circumstances that relate to a person's identity – the footprint of who they are"…Des Browne – 25 January 2005".

The Identity and Passport Service (IPS) delivery plans that Identity Cards will start to be issued to foreign nationals this year (2008) and UK workers in sensitive roles and locations next year.

"The Scheme will be available to people over 16 years old who legally reside or work in the UK. Specifically, it includes biometric visas, enhanced passports (for all ages) and identity cards, including those cards issued to foreign nationals in the form of biometric immigration documents. The Scheme is supported by legislation, including the Identity Cards Act 2006, which provides important statutory safeguards regarding the collection, retention and oversight of information necessary for the operation of the National Identity Register and the issue of identity documents issued under the powers of the Act."

[3] No reproduction without the express permission of the author

The IPS delivery plan recognises the importance of effective identity management as:

"The means for people to prove their identity is fundamental to a functioning society. This is important not only to counter identity fraud and its effects (crime, terrorism and illegal immigration and working) but to make all our lives easier. More frequently than before we have to prove who we are to people who do not know us: for example when we apply for jobs, use public services, travel abroad, and open bank accounts. These two related objectives, public protection and ease of day to day life, are at the heart of the Scheme."

The Crosby Report

Sir James Crosby and his team was engaged by the Chancellor (now Prime Minister Gordon Brown) to consider how the public and private sectors might work together in identity (ID) management for their mutual benefit and that of citizens and consumers. Their report summarises the issues at the beginning:

Identity "is the new money"

"There is nothing new in the importance of being able to prove our identity. The first passports were issued almost 600 years ago. But today, as our lives become more peripatetic and our dealings more rarely face to face, it is ever more important for each and every one of us to be able to assert our identity with ease and confidence." …Crosby summary

It's the consumer's identity

"At an early stage, we recognised that consumers constitute the common ground between the public and private sectors. And our focus switched from "ID management" to "ID assurance". The expression "ID management" suggests data sharing and database consolidation, concepts which principally serve the interests of the owner of the database, for example the Government or the banks. Whereas we think of "ID assurance" as a consumer-led concept, a process that meets an important consumer need without necessarily providing any spin-off benefits to the owner of any database. This distinction is fundamental. An ID system built primarily to deliver high levels of assurance for consumers and to command their trust has little in common with one inspired mainly by the ambitions of its owner. In the case of the former, consumers will extend use both across the population and in terms of applications such as travel and banking. While almost inevitably the opposite is true for systems principally designed to save costs and to transfer or share data.
The importance of ID systems extends well beyond commercial transactions. In practice, the quality of such systems determines the extent to which many desirable social goals, including border controls and restricting employment to those entitled to work, can be achieved. Indeed, an ID system will only help fulfil national security goals if it achieves mass take up and usage.
If citizens don't use a system regularly, it will be capable of providing very limited data for national security agencies. Thus, even the achievement of security objectives relies on consumers' active participation."

It was interesting that the Crosby report was commissioned by the Treasury at the same time as the ID Card Programme was approaching its procurement phase and takes an alternative approach to assuring identity, very much that of the EU sponsored case study above. It also makes the assumption that a passport is an assured identity, for many it is; for some, myself included, it is merely one of the many credentials necessary to achieve an assured identity and is not the gold standard in itself that many in IPS would see it. I will return to the challenge of assuring identity and the use of collateral sources or what are known as 'breeder documents' later in this paper.

The Data Sharing Review

This review was set up by the Prime Minister who invited Dr Mark Walport, Director of the Wellcome Trust, and Richard Thomas, the Information Commissioner, to conduct a review into the use and sharing of personal information in the public and private sectors.

"The terms of reference of the review are as follows:

- Consider whether there should be any changes to the way the Data Protection Act 1998 operates in the UK and the options for implementing any such changes;

- Provide recommendations on the powers and sanctions available to the regulator and courts in the legislation governing data sharing and data protection; and
- Provide recommendations on how a data-sharing policy should be developed in a way that ensures proper transparency, scrutiny and accountability.

The recommendations will seek to take account of technological advances and to strike a balance that ensures appropriate privacy and other safeguards for individuals and society, whilst enabling the sharing of information to protect the public, increase transparency, enhance public service delivery and, where possible, reduce the burden on business."

One could ask why this is included here where I am discussing identity, its management and how that extends to an e-ID. Essentially Data Handling in the context of the review is very much complementary to the identity debate. The spate of data losses in the public and corporate sectors that prompted the review are also about identity and on how information regarding the credentials and attributes of personal data are shared and safeguarded. The report is, therefore, in my view by extension very much about attributes and credentials of identity hence its inclusion.

Back to basics in identity

Regardless of whether we support the present UK Government National Identity Card Scheme and its underlying database, the National Identity Register (NIR) as either a political or a privacy issue, identity is recognised as a pivotal credential in modern life and our interaction within wider society for business or pleasure.

Yet there are few standards and even less common understanding of what makes up the components of an identity and the credentials that support assertions of identity. For almost time immemorial it has been assumed that 'You are who your papers say you are', with little challenge outside the intelligence and police community to prove the assertion. It has become established practice that the possession of photographic identity, especially a passport and a driving licence equates to 'good identity'.

It is only now, with increased dependence on the multitude of transactions on the internet and with increasing levels of electronic fraud that some of us are pressing for an in depth examination of what constitutes 'good identity'. This benchmark standard ought to be in a graduated scale of assurance depending on the appropriate level of use and associated guarantee of dependability.
At National level it follows, therefore, that there has to be a high degree of rigour in the baseline level of application and enrolment onto the National Identity Register. The standards for Verification, Authentication and Authorisation by those charged with investigating and awarding assured identity at both Public and Private level must follow established best practice in Identity Management. It would also be useful if these standards were universally acknowledged and adopted for the sake of consistency; at present there is no such benchmark.

In any case what is "Good"? There needs to be a variety of differing levels that work up in a graduated scale of assuredness. There will be occasions when certain affirmations or credentials of identity will prove to be "fit for purpose" i.e. identity credentials required for the issue of a local library ticket at the lowest scale ranging up to sufficiently robust process for an assured National Identity (an absolute certification). The processes and procedures in present used to issue National Insurance numbers, driving licences and even passports are based on policies, processes and procedures that were never, in themselves, intended to be standards of assured identity, regardless of what these various departments would have us believe! At the same time, we need to guard against unnecessary "gold plating" of our demands for evidence of identity. What is certain is that we can establish the level of acceptability of an individual's identity before this can be used as the method of establishing and `binding` that identity for use on an ID card.

What about fraud? I have caused great consternation in the past by posing the question "what is an acceptable level of fraud against our accepted standards of good or best ID"? It is naturally enough a question that all wish to duck or go away but it will not and must be faced head on. No system is perfect. An identity has a value and as such will inevitably be the target of those who wish to steal or appropriate its credentials for their own purposes. The Threat Spectrum ranges from fraud by criminals, sometimes on a large scale, through to threats to national security by terrorists using alternative identity to bypass detection by law enforcement agencies.

Identity is a token, a key, to goods and services and a secure Identity card. The approved e-ID must be that which conveys in a data/graphical/pictorial form a true representation of the Identity of the individual being presented which can be authenticated and verified. This might be by a commercial organisation based on a credit reference check or by the government NIR. I would add a comment here and a note of caution that sometimes much overweight is placed on a system founded on credit reference – which was originally predicated on one's ability to pay and not on whom one is.

Identity can be seen as the distinct personality of an individual regarded as a persisting entity, the individual characteristics by which a person is recognised or known. The integrity of the process that determines and awards the granting of an identity as opposed to an identity claimed by personal affirmation is an entirely different thing. Yet the distinction is not widely recognised. For example knowing the PIN number of a credit or bankers card is NOT proof of identity – it is only a risk mitigation mechanism linked with a finite risk (cash) limit. It is fine in certain circumstances but falls far short of assurance levels for other requirements.

The present 'best practice benchmark' in common commercial use to determine proof of identity such as combinations of:

- A utility bill
- Picture driving licence
- Passport

The above are deemed sufficient to prove identity but are open to abuse. The test is down to appropriateness, for what purpose is the test of identity required and what are the risks associated or business impact of getting it wrong?

Where are we legally? Anyone could claim to be anyone else in isolation without consequences of any sort. This was changed by the recent introduction of the National Identity Cards Bill (when?) where the possession of another's identity can be deemed an offence. It is only when one person claims to be another in the commission of a commercial transaction or where they are purporting to be somebody else in a commercial transaction that a problem arises That is, the legal system only cares that Fred Smith is claiming to be Mary Jones when he tries to assert her identity fraudulently for some purpose. In other words, authentication of identity is only necessary when an authorisation event, or attempted authorisation event, follows.

Components and definitions of Identity

It is useful to include here some definitions of identity components

- **Entity** a being, a place or a thing
- **Identifying Characteristics** are biometrics and other unique characteristics associated with an entity
- **Primary Identifying (or "Root") Documents** link an identifier with an entity often by association with an identifying characteristic such as a biometric.
- **Secondary Identifying Documents** are standard documents referencing identifiers(such as a utility bill, bank statement)
- **Identifiers** are names, numbers, titles meant to identify an entity.
- **Identification** A document that purports to be issued by an authority that has *established* the identity of an entity.
- **Identity** A set of identifiers associated with an entity.

The elements of Identity are generally agreed to be:

- Attributed
- Biographical
- Biometric

Attributed

These are the components of a person's identity that are given at birth i.e.:

- Full Name
- Date and place of birth
- Both parents names and addresses where applicable

Biographical

These are the components that are built up over time and are the most time consuming and difficult to falsify by all but the most professional or dedicated efforts.
They cover certain life events and how a person interacts with structured society. This is why credit reference agencies are such devotees of address registration to build up a pattern of biographical information that is attributable to a certain 'claimed identity' (remembering that without surety in linking biometric information with biographical it is still easy to assume another previously established identity record or part of it).

Biometric

Biometric components are considered to be the unique physical characteristics of an individual such as fingerprints, iris/retina pattern or DNA, that can be used to strongly bind an individual to a previously established identity. It should also be noted that there is a debate about the absolute or relative uniqueness of biometrics. This is not dancing on the head of a pin but a question of statistical probabilities of uniqueness to many millions of a degree.

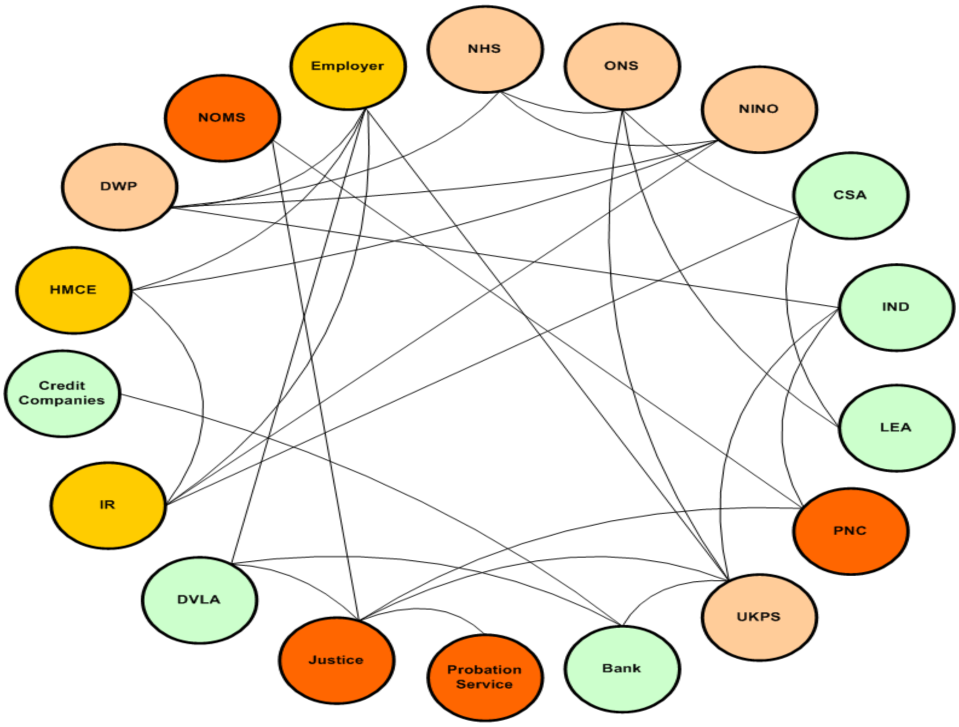
Biometrics used for identity purposes can only bind an individual to an established biographical identity and should not be used to establish identity, unless awarded at birth by for instance taking DNA and immediately linking that to a biographical identity. This has been recommended by the Lord Chief Justice. Biometrics can also be used to link an individual to previously obtained biometrics in different contexts, but even then cannot establish identity in themselves.

There are some fundamental identity questions still to be considered

- "Who do you claim to be?"
- "Whom do you wish to be known as?"

Proof of Identity is to an extent judgemental although increasingly this is rules based using intelligent computer applications. I am always wary of completely computer based analysis engines that remove the final decision from an operator. Biographical checks need to be incremental and depends on levels of rigour appropriate to the use that the identity and e-ID are to be placed i.e. are they to be used as authorisation to highly secure facilities and networks or very high value financial transactions? There is also a need to be aware of 'breeder documents'. The diagram bellow illustrates how various agencies could share information.

For example, a self assertion credential that is used as 'proof' of identity' by John Smith to a local council by asserting that illustratively he lives at '3 Acacia Avenue' to register to vote on a local electoral register (sadly one of the lowest requirements of proof of identity). This subsequent entry with very low levels of proof is then shared in good faith amongst other agencies that have no reason to doubt the legitimacy of the entry. Where a check, automated or manual is made that requires a number of points of reference these are made and the checks may well validate that John Smith does live and is registered to vote at the address in question. However, it often happens that a single item of data is 'bred' across databases without further checks and is in fact of very low corroborative value and so the level of trust ought to be correspondingly low.



The breeder document cycle of shared assertion (ECA copyright)

Biographical documentation for identity purposes ought to be validated. Variations of assertion could be as varied as follows:

- Self assertion
- Unofficial breeder – self assertion
- 3rd Party Assertion - my mother says I am who I am
- Official 3rd Party Assertion – lawyer
- Credit Agency – record transaction in a name/address
- Demographic database check
- Unvalidated documentation
- Unvalidated official document with visual image
- Validated Official document
- Validated Official breeder document
- In person proofing – assertion of false identity but provision of biometric data

Going into more detail when profiling secure identity possession, knowledge and characteristics of information can all be used to reach an award of identity again depending on the level of assuredness or trust required. Establishing and maintaining a CHAIN OF TRUST i.e. what the individual possesses -.physical and biometric characteristics, gait, height, DNA, fingerprint, facial recognition features, IRIS and vein footprint etc is important in these circumstances. This is especially valuable where an e-ID is to be used for high value transactions.

Identity Crime

The components of Identity Crime were defined by the UK Identity Fraud Committee in 2005 as:

A false identity can be created where a fictitious (invented) identity is created or an existing (genuine) identity has been altered to create a fictitious identity.

True Identity Theft is itself rare and the term is a misnomer, generally what is experienced is “impersonation” commonly using a form of e-ID. Identity theft is, therefore, a generic term for Identity Impersonation, creating a False Identity or committing Identity Fraud by impersonation or in legal terms fraud by using? a false instrument to gain a pecuniary advantage. Most of us call it theft! This occurs when sufficient information about an identity is obtained to facilitate Identity Fraud, irrespective of whether the victim is alive or dead. Identity fraud in the case of deceased persons is normally, but not exclusively, found in establishing a false identity by the application for a birth certificate of a baby or deceased adult. This type of identity fraud was popularised as 'Day of the Jackal Fraud'.

Identity Fraud occurs when a False Identity or someone else's identity details are used to support unlawful activity or when someone avoids an obligation or liability by falsely claiming that they were victims of Identity Fraud.

Social engineering can be described as the practice of impersonating or using a remote enquiry to elicit identity and personal information. This information is subsequently used to gather further key elements of identity in order to impersonate in kind, by illusion or actual data, a person whom they are not for financial or other gain. It is a key component of identity impersonation or fraud.

At the individual level a citizen may claim an identity and for most low value transactions for identity purposes that is proof enough. Their ability to prove, by the bonding of documentary assertions *beyond reasonable doubt*, that they are who they claim to be is by the supply of documentary evidence and the provision of biometrics
The supply of initial and continuous official biographical documentation (paper or electronic) fused to an individual identity using biometrics, provides a strong link between an individual and the claimed and recorded identity on an assured database such as the National Identity Card Register (NIR).   The commonly made assertion is that biometrics provided and stored on the NIR can be used to verify and authenticate to a previously established and claimed identity to a higher level of assurance.

Verification of identity can also prove challenging and problematic. The statement that "I am who I claim to be" can usually be checked against a single established identity. More in depth checks can be made using a number of reference sites (but being aware of breeder document claims) and against unique characteristics, such as biometrics, where the identity is located using unique information such as a reference number or name on a national or international assured database. This usually requires a search against a database of previously established identities with a unique matching characteristic to locate one entry.

In turn, governments initiate standards, create regulations and issue mandates, that aim to protect this information and help secure assets. By layering security technologies across different applications and resources, governments and large commercial Identity Management Systems are managing their processes and leveraging a variety of technologies in order to create secure environments. By using a layered security strategy, these agencies hope to avoid single points of failure and voids that leave gaps in security. These strategies often are different for every government entity.

In developing and implementing a government-focused layered security model, many countries have created systems of trust to protect borders and citizens' information via e-Passport technology or e-ID's. Whilst implementations may vary across the globe, the primary objective is identical: authenticate both citizens and the validity of e-Passports and e-ID's through technology and a strategic, secure infrastructure.

Summary, where does all this leave us?

Without a method of assured Identity, certainly biographical, we can adopt a persona, transfer that identity by assertion alone to electronic form and operate on the internet and elsewhere with several forms of "identity". Only where there is a strong method of awarding and binding an identity (an 'assured or certified identity') to a person is there any real prospect that a person is likely to be, within reasonable bounds, who they claim to be.

Why should this bother us at all? A large proportion of the internet community regularly assume a cloaked identity or persona as standard practice. Pseudonyms are common but they are also alternative forms of e-ID and are entirely unregulated. Individuals also have other names or forms of assumed e-ID (identity) on different systems; web based dating agencies, social networking sites such as Facebook, internet gaming sites, internet chat rooms and on virtual reality sites such as Third World etc. We do not consider all of these forms of 'assumed e-Ids' as unusual or suspicious, but they are without regulation and we can basically call ourselves what we like. It is but a short step to the same culture permitting e-ID mechanisms to give paedophiles and criminals huge opportunities to operate and assume identities for other nefarious reasons quite unintended by the well meaning administrators of electronic sites and systems For example the prevalence of West African and Russian based identity fraud scams on dating sites, which raise millions of dollars for organised crime and terrorist organisations) It is this unintended consequence that has such implications for the unregulated use of identity and especially e-ID.

Some unintended consequences

The widespread adoption and use of cross border e-ID schemes nationally, within the EU, between the USA and internationally will carry unintended consequences. In March this year the European Data Protection Supervisor, Peter Hustinx, flagged his concerns that the EU plans, for its outer border controlled biometric-based system, may have significant privacy implications. He commented that:

"It is very regrettable that the EDPS has not been consulted in the preparation of the communications or in the course of the impact assessment of the first communication. The national data protection authorities have not been consulted either. This gives the overall impression that this aspect was considered less relevant by the European Commission than purely technical aspects."

And that:

"Several of the envisaged measures entail the processing of vast amounts of data, involving the collection, consultation and possible sharing or pooling of these data. A lack of data protection safeguards does not only mean that these individuals might suffer unduly from those measures, but also that the measures will be less effective, or even counter-productive, by diminishing public trust in government action."

This fascination with 'technical solutions' without a full understanding of what is required when considering identity and e-ID and all the options and implications of a selected solution option reinforces my earlier point.

Summary

I can think of no better summary of our present predicament than the summarised by the Prime Minister in his speech on Liberty on 25th October 2007

"In previous centuries people's identities were protected in the only ways people knew how - with the requirement to register at the time of birth, marriage and death. Today we have the benefit not just of the fingerprint technology of the last century but advances in biometric technology in this, that can protect individuals and society against crime, fraud, illegal immigration and terrorism - and protect for each and every individual our own identity.

"And on those occasions where we already have to identify ourselves - when we open a bank account or withdraw money, pay for something, cross borders or register with a GP - citizens themselves are recognising that it is in their interests to have a modern and secure means of identification which better protects against crime, fraud and illegal immigration and also protects each of them as individuals, their property but also their privacy." **Extracts from the Prime Minister's speech on Liberty – 25 October 2007**

This is why the fundamentals of Identity are so important to us all.

About the author

Tony founded Electronic Commerce Associates www.ecalimited.co.uk on leaving the Army in 1998. He has been widely interested in national and international efforts to rationalise Identity Proofing and Verification with key interest in the implications for Corporate and Government Identity Management, its Integrity, Security and Privacy issues and on Data and Control Centre design and operation.

A fellow of the British Computer Society, an experienced CLAS Security consultant and qualified UK Government Security Accreditor; Tony is a regular speaker and authority on a wide area of associated issues. He has huge experience in the practical and useful application of Security Policy, Physical and Technical Security Measures, Corporate Business Assurance, Business Continuity and Disaster Recovery. He has 40 years experience in the practical application of system and network architecture, appropriate security policy, business assurance and continuity, and data and control centres for military, government and corporate application.

An Expert Witness for Cyber Assurance and security issues in the International Court of Arbitration, Chairman of The ECA Group and ECA International. He directed the overall business assurance challenges for the UK Government Trusted Borders Programme, and was previously head of the Resilience, Security and Fraud prevention team for the UK National ID Card Programme. From August 2004 to April 2007 he was head of the Resilience, Security and Fraud prevention team for the Home Office ID Card Programme. In this role he lobbied hard to establish the requirement for an entirely fresh approach to Risk Management on holding personal biographical and biometric data together with assurance principles for remote authentication, an enhanced security vetting standard for the Identity and Passport Agency. His team were instrumental in establishing benchmark standards for identity management and enforcement policy with close co-operation with legal-law enforcement and National Security Authorities on compliance issues with relevant legislation and enforcement powers.