

# Key Technologies for Identity Management

Report for  
“Foresight: Horizon Scanning Centre  
Workshop on Identity Management”

Michael Huth  
Quantitative Analysis and Decision Science  
[imperial.ac.uk/quads](http://imperial.ac.uk/quads)

Imperial College London

February 1, 2007 <sup>1</sup>

## 1 Introduction

“The human experience of identity has two elements: a sense of belonging and a sense of being separate.”  
Salvador Minuchin, family therapist, 1974.

This quote not only captures psychological identities but also digital ones: digital credentials can certify the sameness of identities, but they also can express relationships with other identities.

### 1.1 Central concepts

*Subjects* or entities (e.g. you, HP, Microsoft Word, or the machine named `marina.doc.ic.ac.uk`) are agents that can make requests to access a resource (e.g. cross a border, access files from Orange, copy a file, or connect to the machine named `shell1.doc.ic.ac.uk`).

Subjects get access by claiming an identity. E.g. you may attempt to cross the border by claiming to have the identity specified on your passport.

*Identities* collate data in the form of attributes, traits or preferences of a subject. E.g. a passport contains a photo id, height, eye colour, may contain fingerprint ids but does not contain data on characteristic behaviour or likely preferences of a subject.

- *Traits* are inherent, e.g. the characteristics of your left or right eye's iris.
- *Attributes* are acquired and transient, e.g. holding a valid driver's license or a certain visa status.
- *Preferences* often occur in service industries, e.g. whether you prefer to sit in row three of your local cinema.

---

<sup>1</sup>This is an amended version of the report and takes into account comments and discussions made during the workshop.

A crucial function of identity systems is to authorize/deny the access of subjects to resources.

*Credentials* are the principal means of laying claim to an identity, e.g. biometrics, passwords, and X.509 certificates are credentials to claim a physical identity, ownership of an account, and possession of a public encryption key (respectively).

**SCENARIO:** <sup>2</sup> You have just moved to East London and want to rent a DVD from that video rental store in your new high street. The store owner does not know you personally so she asks you for several credentials before you can open an account with her. Since the United Kingdom currently has no universally accepted identity card, she is likely to ask you for “a” photo id (e.g. from your employer) and two recent bills (e.g. from a utility company or local council) showing the local address at which you claim to live. Saying that she is satisfied with these credentials means that she authenticated them. If so, she will then open an account for you that will authorize you to rent up to five DVDs at the same time, provided that your account balance is positive.

This example shows key elements of identity management; we mention here authentication, authorization, and policies that depend on proper authentication to regulate such authorization.

According to Philip Windley, identities can be classified into tiers:

1. *Abstract identity*: timeless and unconditional traits or features of a subject, e.g. eye color
2. *Shared Identity*: attributes assigned to subjects by other subjects, e.g. your employee id card — which is *shared* between you and your employer and is temporary in nature
3. *Abstracted Identity*: used to identify groups, e.g. the group of owners of Oyster cards that are currently valid in zones 1 and 2

Tier 3 identities are useful — e.g. data mining customer behaviour, or proof of legal age when entering a night club — but intrinsically limited for identity management, e.g. unsolicited phone calls to the owner of the phone line to propose a change of service provider.

Tier 2 identities are the domain in which digital identities operate.

Tier 1 identities are the basis for biometrics and, for that, deserve attention and have value in identity management systems.

*This report will cover abstract (tier 1), shared (tier 2), and abstracted (tier 3) identities.*

## 1.2 Identity management systems

(Digital) identities need to be managed. Particular technologies and products that support (digital) identities therefore need to be seen in a holistic manner as operating within an overall system, an *identity management system* (IMS). As a corollary, any technology such as biometrics can only be a solution within an IMS, and what such a technology solves or whether it is indeed a solution depends on the IMS in which it operates.

All IMSs follow or subsume, in essence, the following life cycle:

Provision → Propagation → Usage → Maintenance → (Propagation or Deprovision)

where

- provisioning: creates and initializes identity records
- propagation: stores or sends identity records to required locations or devices
- usage: is self-evident, e.g. authenticating a fingerprint for laptop access
- maintenance: concerns *change management* of identity attributes or associated resources

---

<sup>2</sup>Scenarios may be in part, or total, fictitious but are meant to kick-start the reflection and discussion of such technologies in their societal and economic context.

- deprovisioning: removes identities from IMS

Key technologies for identity management should therefore be assessed (with respect to reliability, cost, effectiveness, realizability, etc.) within such a life cycle. Such an analysis will then vary from IMS to IMS.

## 2 Key Technologies for Identity Management

### 2.1 Authentication Technologies

*Authentication* is the process of checking the validity of credentials, e.g. checking whether a passport has indeed been issued by Her Majesty's Government and, if so, whether this passport has not been tampered with.

A proper understanding of a particular authentication task requires knowledge of its context and scope. For example, authenticating that a passport was issued by the proper authorities is only part of the authentication process at border control points, since one also needs to ensure that the bearer of the passport is its legitimate owner, not wanted by Interpol, etc.

Authentication is a vital component of *authorization technologies*, which need to authenticate subjects prior to their authorization to access a resource. Immigration officers check the authenticity of passports before they authorize travelers to enter the baggage claim area.

#### 2.1.1 Biometrics

**DEFINITION:** Uses biological or behavioural traits to uniquely identify a person or animal with high probability, either against a pool of subjects or with respect to a set of credentials for a subject.

**EXAMPLES:** Handwritten signatures, voice, retinal maps, iris characteristics, fingerprints, palm prints.

**SCENARIO:** Tens of thousands of football fans' faces were scanned secretly as they entered the stadium for Super Bowl XXXV, the face recognition software produced probable matches with faces of known criminals in a police control room.

**OUTLOOK:** PDAs and Laptops with built-in fingerprint recognition for access can be bought already. Such biometric means will be embraced by users if they are in control of their life-cycle.

Use of biometrics similar to that in the scenario will gain importance in controlling and monitoring public spaces such as airports, public transport, and public events.

Use of biometrics for identification as a reliable check of credentials should also gain significance. Typically requires "reading" of biological trait from person at site of check, since the presentation of a *digital* biometric reading is just another credential.

Biometrics of animals will become economically viable and interesting in the long term, e.g. to identify animals that are used for breeding, racing or laboratory testing.

Biometrics may also identify a specific behaviour (as opposed to an individual). This could have uses in automated monitoring of CCTV systems, e.g. to detect assaults or threat levels of crowds.

**ANALYSIS:** Biometrics has a high probability of uniquely identifying an individual so it can be used for *identification* not just for the authentication of credentials that a person offers. In particular, it is useful for *negative* identification: criminals may steal your National Insurance Card and use it as a credential to claim your identity; but if credentials are then checked against biometrics of the claimant at the locus of authorization, such fraud will be detected.

The strength of biometrics (unique identification of person) is also their weakness. E.g. once a fingerprint of Cliff has been obtained, that print can be placed on a suitable carrier material and then be used to access a laptop secured by this biometric until, and if, the access system is reconfigured to another biometric or fingerprint. This weakness suggests to use biometrics within a two-factor authentication system (discussed below).

Terminology is important in any discussion of biometrics. One needs to distinguish between the use of biometrics for enrollment (in the provisioning phase) and for verification (in the authentication phase of an IMS):

- Enrollment: a biometric identifies a person uniquely within the entire enrolled population of the IMS, called *one-to-many* matching.
- Verification: process of matching a person's claimed biometric identity with the one stored during enrollment, called *one-to-one* matching.

Accurate enrollment processes are typically more challenging than reliable verification of biometrics.

**WHAT TO WATCH:** Success of existing iris scan schemes for crossing UK borders without passports. Cost issues. Not a silver bullet but just a means of authentication and identification within a holistic identity management system. Fairness issues (e.g. palm or finger prints of polydactyl people). Use of biometrics in schools and similar institutions with controlled gateways (as opposed to securing a large campus perimeter). Legal considerations, e.g. intellectual property rights on personal biometric readings?

**KEY PLAYERS:** Government. Business.

**KEY ISSUES:** Exclusion and Inequalities. Privacy. Ownership. Trust and Culture. Criminality. Internet.

### 2.1.2 Two-Factor Authentication

**DEFINITION:** Authentication based on two *independent* (rather than one) credentials (both must be approved).

**EXAMPLES:** ATM card and PIN. Username and password? Touch card and password.

**SCENARIO:** Klaus logs into his bank account with the Deutsche Bank through a secure browser session. This login always requires entering a secret customer number and selected digits of his 6-digit password. Thereafter Klaus can access statements of his various sub-accounts, as well as lists of recent transactions, etc. Whenever he wishes to transfer money to another account, he needs to enter a *one-time password* to authenticate that transaction further. Klaus receives a stack of such passwords through regular postal mail and receives a new stack of passwords whenever the previous one has nearly run out or has expired — similar to how cheque books are being delivered by most UK banks.

**OUTLOOK:** Hand-held tokens will increasingly be used in connection with two- or multi-factor authentication. There is great scope in the nature of hand-held tokens (e.g. electronic versus non-electronic). Such tokens require more complex identity management processes so the respective IMSs need to reflect this and cope with it.

**ANALYSIS:** Hand-held tokens that can be used only once provide much stronger security and constitute a significant obstacle to sophisticated and organized criminals who want to commit online identity fraud. The example of postal, one-time passwords in the scenario above is just one way in which to achieve this.

Another one is a (not necessarily smart) card that can be read on a computing device prior to financial transactions that require additional authentication. An issue is here whether this requires a separate card reader or whether a simple touch function is supported by the off-the-shelf computing device. A tamper-proof hand-held token can store a long-term secret (e.g. a digital signature on a smart card) and has therefore the advantage of being reusable without any further mechanisms. This advantage is also a disadvantage since a thief of this card will be able to use it, whereas one-time hand-held tokens can be used only once (whether stolen or not).

With companies such as Microsoft and Intel moving into the design of platforms that are based on identity management from the ground up, it is likely that future off-the-shelf computing devices will have such reading facilities based on slot penetration or touch. This will then leverage token-held authentication for financial transactions.

Use of passwords in conjunction with usernames is *not* two-factor authentication since the username may be public knowledge or easily reconstructed. Two-factor and multi-factor authentication means that the factors are independent. Getting three out of five security questions right with your bank clerk is *not* multi-factor authentication as all questions and answers can from the same factor: knowledge about account state.

Despite of its social problems (hard to remember more than eight passwords, social engineering, etc.), the username/password form of authentication will stay with us for a long time. Expect it to be strengthened increasingly with third factor of authentication, e.g. biometrics, whenever appropriate.

**WHAT TO WATCH:** How/whether customers take on one-time passwords for sensitive financial transactions. This is the standard approach for online banking in Germany, where consumers seem to be more weary of fraud than in the United Kingdom. Use of one-time tokens (with bar codes) as authenticated travel tickets, as discussed further below. Convergence/combination of password- and token-based access control in the future.

**KEY PLAYERS:** Business. Individual.

**KEY ISSUES:** Trust and Culture. Attitudes to Risk. Criminality. Internet.

## 2.2 Authorization Technologies

Authorization is the process of issuing, granting, denying or revoking an entitlement to a subject for use of a resource. This process is based on authenticating, and then mapping, identities onto entitlements. Two examples:

1. Set of credentials and procedures that governments use to then authorize the payment of benefits.
2. After having approached the reception of Alcatel-Lucent in Isle, Illinois, with one of its Distinguished Technical Members of Staff (who then and there claimed that you were his visitor) and having had a copy of your passport made at the reception, you received a visitor's pass that authorized you to access the building but obliged you to always be accompanied by an Alcatel-Lucent employee.

### 2.2.1 Role-Based Access Control

**DEFINITION:** Systems that control the access to resources based on access-control policies, where the policies don't authorize access based on a subject's identity but on a subject's *role*.

**EXAMPLES:** Company office policies. Access control of secret government information. Buying liquor?

**SCENARIO:** All office employees of a company have access to that company's intranet through networked PCs and user accounts. Company policy is that all non-managerial staff can use that network connection to access sites beyond their intranet before 9am and after 5pm. All managerial staff can access external sites at all times. Pamela has been working as a sales analyst for that company with great success in the past three years. As a non-manager, her access to that web is restricted during regular working hours. Deservedly, she will be promoted next Monday, when she *will* be able to access external sites at any time simple because her role attribute then will have changed in the IMS. No creation of a new user account or change of policy is necessary to achieve this.

**OUTLOOK:** Role-based access control will be the increased model of choice for managing access control, as the access to resources is largely determined by the role a subject is playing within a system. Role-based access control is a lively topic in academia with good foundations and robust proof-of-concept implementations. Challenges remain for ubiquitous systems and fully mobile subjects and resources.

**ANALYSIS:** The scenario above should make clear the key advantage of role-based access control over access control that states for each subject, resource, and action an authorization. So instead of explicitly saying "Joshua is granted the right to modify file foo.doc" (and saying similar things for other individuals and files), one can simply say "All company partners have the right to modify all Word documents." This coarser level of granularity allows for more flexibility and scalability in the life cycle of an IMS and speeds up the authorization process as it only requires that a subject or resource is authenticated to have the required role.

Many roles are comprised of a group of subjects. As such, roles are abstracted (tier 3) identities and may play a role in determining the proper balance between authentication and privacy. For example, the group of individuals that has legal age to buy liquor should be able to exercise that right based on that role only, and not on more specific information such as their actual age.

**WHAT TO WATCH:** Convergence and combination with Digital Rights Management systems (discussed next). Increased use of role-identifying email addresses. Different roles as different digital personas.

**KEY PLAYERS:** Individuals. Business. Government.

**KEY ISSUES:** Exclusion and Inequalities. Ownership. Trust and Culture. Internet.

### 2.2.2 Digital Rights Management Systems (DRM)

**DEFINITION:** Framework for controlling circumstances under which a digital resource can be used, possibly independent of location of resource. Such control typically depends on the context or history of such access.

**EXAMPLES:** Fairplay (as used for iTunes). Zone codes for DVDs.

**SCENARIO:** <sup>3</sup> Jens makes a legal copy of his new CD on his account of the family PC and enjoys listening to that copy while working online. His wife Hanna likes to knit and uses her account on the family PC to access a web-site that shares knitting patterns. She downloads some patterns and is then asked whether she wants to share her patterns stored on the PC's hard drive. She agrees and these patterns are uploaded. This permission, however, allows remote programs from other hosts to access all music files on the family PC, or worse, to install a server program for music sharing on that PC — both due to the absence of a DRM system. Weeks later Jens receives a hefty fine from the law department of a big records company, resulting from the unsolicited installation of such programs.

**OUTLOOK:** DRMs will gain importance in areas that require context-dependent and dynamically evolving authorization control. We mention the UK Ministry of Defence and its recent interest in DRMs as a technology that can describe what exactly subjects in the field can do under which circumstances to what resources. This is likely to be explored in the US/UK Information Technology Alliance.

The fine-grained control of DRMs is also vital for opportunistic alliances in the commercial world, when companies want to share resources for tactical or strategic ends within specified logical and temporal boundaries.

**ANALYSIS:** DRMs are much more than an attempt of media companies to protect their intellectual property rights. DRMs go beyond traditional access control technologies. For example, a DRM could not merely specify who has access to your National Insurance Number but it could state who can do what with it under which circumstances. This yields a much more fine-grained control of resources but is also harder to implement.

DRMs also have to strike a balance between the usage constraints attached to a digital right, and the value of such a right as perceived by its consumer. If Fairplay would not allow you to make copies of a tune on up to four computers, the value of that tune would decrease and you would not be willing to pay the current asking price.

DRMs entail management burdens. For example, if one of your PCs is stolen, breaks or is sold off, then there should be a process by which you can get back the entitlement to the iTunes copies stored on that PC.

DRMs are configured with respect to currently anticipated behaviour and so may be at odds with future behavioural culture. For example, making DVDs playable only within certain zones of the world makes assumptions that may erode in the coming age of a global economy with global economic and skills-based migration, travel and mobility.

DRMs may offer an exiting tool for the empowerment of subjects through consumer/citizen-centric DRMs that could help with maintaining the delicate balance between privacy (in the sense of controlling access to, and flow of, personal information) and the desire to interact in the market place and the cultural commons.

---

<sup>3</sup>This more or less happened a while back in Denmark.

**WHAT TO WATCH:** Whether and how the military embraces DRMs. DRMs for document work flow within organizations (within context of future computing platforms that integrate identity management from the ground upwards). Whether market forces will strike the right balance between the level of enforcement of DRMs and the value to customers in the multi-media domain. Whether consumer/citizen-centric DRMs will catch on.

**KEY PLAYERS:** Government. Business.

**KEY ISSUES:** Exclusion and Inequalities. Privacy. Ownership. Trust and Culture. Criminality. Internet.

## 2.3 Directories and their Meta and Virtual Versions

**DEFINITION:** Directories are centrally managed repositories for *retrieving* structured information that can be supplied to distributed applications. Unlike databases, directories have more retrievals than updates.

**EXAMPLES:** Password files. Access control lists. Windows Registry.

**SCENARIO:** A server who guards the access to computer accounts on a local area network receives the hash (a digital fingerprint) of a password from a client with claimed user name `foo`. The server has superuser privileges that enable it to read a password file that centrally stores hashes of legitimate passwords bound to their user names. The server checks whether that file contains an entry for `foo` and grants access only if such an entry exists and its hash matches the one supplied by the client.

**OUTLOOK:** Directories may seem like straightforward entities to create and maintain, but they are an important aspect of smoothly running IMSs. Their virtual and meta versions have growing significance.

**ANALYSIS:** Directories are most often *directory services*, which are *network-aware* directories. The stored information is not necessarily about people (as one would expect in the directory `imperial.ac.uk`), but can be about devices or abstract concepts. Examples of this are

- Domain Name Server (DNS), distributed service for resolving hierarchically organized symbolic domain names, such as `marina.doc.ic.ac.uk`, to Internet Protocol (IP) addresses
- X.500, a family of ISO/ITU specification standards, notably X.509 which specifies the public-key infrastructure that operates as the foundation for the use of many forms of digital certificates within an IMS
- Lightweight Directory Access Protocol (LDAP), simplified interface for use of X.500 compliant services

Within organizations there is pressure to aggregate information as the maintenance of fragmented identification records causes problems — we mention the difficulty of maintaining consistency of data (e.g. credit checks) and the need of different government agencies to share information reliably and accurately. The aggregation of such data, and the manner in which this is done, will be two key needs and drivers of future IMSs. There are four principal architectures for directories that aggregate information:

1. single, centrally managed data repository
2. single, centrally managed *meta-directory* that must be synchronized with all other directories of the organization (e.g. to ensure consistency)
3. single *virtual directory*, that does not synchronize but presents a single and integrated view of data retrieved from various directories
4. federated directories, we discuss federated IMSs below

Given the history of how separate government agencies have built their own directories, virtual (or federated) directories should work better for a coordinated government directory than “plain old” directories or meta-directories. Synchronization scales perhaps well in theory, but rarely does so in practice (problems with interoperabilities of data models, communication latency, local sources of inconsistencies, etc.). Realistic virtual directories need to live with, i.e. manage, data inconsistencies.

**WHAT TO WATCH:** Off-the-shelf frameworks for the creation and maintenance of virtual and meta-directories. Growing use of virtual directories within commercial organizations.

**KEY PLAYERS:** Business.

**KEY ISSUES:** Privacy. Ownership. Internet.

## 2.4 Identity Management Systems and Architectures

**DEFINITION:** An IMS architecture is the result of a systematic and structured analysis of how to conceive and carry out identity management in an IMS.

**EXAMPLES:** Four-tiered architecture (User Interface, Business Processes, Database Management System, IMS), e.g. as promoted by StrongAuth, Inc.

**SCENARIO:** A small startup company hires consultants to analyze anticipated identity-related tasks within planned business processes in order to determine a suitable IMS and its management processes. Such an analysis will comprise *process architectures*, *data architectures*, *policies*, and *interoperability frameworks* — to name a few.

**OUTLOOK:** There is no doubt that this will become more important in the future. Good architectural patterns will emerge as best practices. Capability Maturity Model<sup>®</sup> Integration, as used today in improving and maintaining software development processes, may then be developed for identity management within given architectures.

**ANALYSIS:** This topic may seem very abstract but the value of architectural principles is as compelling here as it is in the construction business. This thesis has been soundly proved in the world of software engineering, where such principles enabled much of today’s enterprise software frameworks.

**WHAT TO WATCH:** Whether identity management becomes core business of specialized consultancy agencies. Work on standards in this area. Whether commercial IMS suppliers will publish their proprietary IMS architectures. Whether future IMSs will have legal requirement to show “due architectural process”.

**KEY PLAYERS:** Business.

**KEY ISSUES:** Culture. Internet.

## 2.5 Federated Identity

**DEFINITION:** Best understood as a software architecture with low coupling between heterogenous IMSs (owned by different organizations). The coupling provides for well defined and contained sharing of information.

**EXAMPLES:** The Microsoft/IBM alliance and its WS-\* set of web security specifications. Organization for the Advancement of Structured Information Standards (OASIS) and its drive to create e-business standards. Liberty Alliance, which consists of 170+ companies and develops standards for federated IMSs.

**SCENARIO:** British Airways has been in a strategic alliance with other airlines, driven by the need of competitiveness and the fact that such alliances dominate the market place. BA thinks that the current alliance is stable at its core in the medium term and wishes to federate its IMSs with its partners. This will streamline many business processes that cross the boundaries of individual airlines and will simplify existing services (e.g. lost baggage), and even drive new business ideas (e.g. an alliance-branded frequent flyer card).

**OUTLOOK:** Federation of IMSs will become very important in the business world. Such federation of IMSs should also occur, to varying degrees of coupling, between government agencies (e.g. those of the United Kingdom) and governments (e.g. those of the European Union).

**ANALYSIS:** Federation of IMSs is driven by the need to streamline and share identity-related activities across different organizations. The challenges are plenty as such alliances may be temporary in nature, and may have to be established or deprovisioned quickly. The statement made by Home Secretary John Reid to Parliament on 10 January 2007 about foreign convictions is a good illustration of what happens when no federated infrastructure for IMSs exists. The recent agreement of EU member states to share more information about criminal records is to be welcomed, but will only pay off if the information flow is properly conceived and managed. Federation of IMSs may offer great value here.

**WHAT TO WATCH:** The success of companies such as PingID and SXIP, and whether new competitors appear that offer frameworks for federated IMSs. Whether governments will embrace such technology and its ensuing architectures and standards, given their increased pressure to act based upon information that is hosted only in part in their own proprietary IMSs.

**KEY PLAYERS:** Government. Business.

**KEY ISSUES:** Exclusion and Inequalities. Privacy. Ownership. Trust and Culture. Environment. Demographics. Criminality. Internet.

## 2.6 Risk and Trust Management Systems

**DEFINITION:** Manage key aspects of trust in terms of perceived or known risk. Ability to revise risk and to exhibit adaptive behaviour based on such risk.

**EXAMPLES:** Risk assessment tools in the financial services industry. IMSs that dynamically adapt to different threat levels (e.g. contingency planning).

**SCENARIO:** (1) A standard personal loan application and its risk assessment based on a completed application form. (2) How a National Identity Registry would cope with a human pandemic of the avian flu.

**OUTLOOK:** Increased importance in IMSs. Increased need for automation of risk assessment, risk revision, and risk-based event scheduling.

**ANALYSIS:** The financial services industry, notably in trading and investment, has pioneered automated risk management within IT systems. This knowledge and technology needs to be transferred and adapted to future IMSs. For example, if two companies want to connect parts of their IMSs they will only commit to this because each one of them already completed a satisfactory but possibly extensive risk analysis. Automating such extensive analyses is challenging but adds reliability and decreases costs.

**WHAT TO WATCH:** Web services and their evolving negotiation capabilities. Increased need for IMSs to adapt to dynamic risk contexts.

**KEY PLAYERS:** Business. Government.

**KEY ISSUES:** Ownership. Trust and Culture. Attitudes to Risk. Internet.

## 2.7 Anonymity, E-Cash, and E-Voting

### 2.7.1 E-Cash

**DEFINITION:** Money that is exchanged in electronic form. This can be electronic manifestations of real currencies (e.g. money accumulated by an avatar in the online game Second Life) or virtual money (e.g. for trading favours among friends online).

**EXAMPLES:** Electronic Funds Transfer. Octopus card (Hong Kong). Interac network (Canada).

**SCENARIO:** Duncan has an Oyster card with twelve months of valid travel in zones 1 and 2 but also regularly uploads credit on that Oyster card for trips outside zones 1-2 (e.g. to Heathrow airport). This has the advantage that such longer trips are charged at cheaper rates, and he only has to upload his card every once in a while and so he need not worry about extra tickets for each such trip. Duncan would be happy to use his card also for buying snacks within the London Underground Network or tickets for other Railway Networks; but he would prefer to use his credit/debit card or cash for other purchases made in London (dinner, theatre, shopping, etc.).

**OUTLOOK:** Growing significance of E-Cash due to its convenience. Attractive for regional (e.g. Oyster card) and global (e.g. Starbucks card) schemes.

**ANALYSIS:** Credit is stored *on* an E-Cash card so this differs from credit/debit cards that store only credentials and where credit is stored in databases of banks or credit companies. This difference makes the former “cash”.

There is no intrinsic reason why the bearer of an E-cash card needs to be authenticated or in fact bound to that card in any real sense (e.g. when the card stores his name). So E-Cash can be as anonymous as ordinary cash (which is not completely anonymous as serial numbers can be traced and may be recorded at various points within the work flow from the printing press to the customer ATMs).

For security and commercial reasons it may be better to replace anonymity with *pseudonymity*, where each card has a unique ID (that could perhaps be linked to the initial owner of the card in an audit). This would still give enough privacy in legal spending behaviour.

David Chaum holds patents on anonymity control that providers of financial services are reluctant to implement in E-Cash services. There is a friction between the commercial value of knowing the spending behaviour of individuals and the desire of individuals to spend anonymously or even pseudonymously, if so desired.

If authenticated financial transactions become the norm even for small transactions, they paying with cash may be perceived as a “suspicious act”, in the same way as it is today if large sums are being paid in cash. Predominance of id-traceable E-Cash will raise serious privacy issues. This connects to the discussion above on consumer/citizen-centric DRMs.

**WHAT TO WATCH:** Whether E-Cash will tend to blur the boundaries to credit/debit cards in that it may require checks with central databases (e.g. for credit checks or security checks). Whether E-Cash will allow room for anonymity or pseudonymity. Whether consumer-centric DRMs will interact with E-Cash schemes.

**KEY PLAYERS:** Business. Government.

**KEY ISSUES:** Exclusion and Inequalities. Privacy. Ownership. Trust and Culture. Criminality. Internet.

### 2.7.2 E-Voting

**DEFINITION:** E-Voting means the provision, conduction, or auditing of an election — in part or in total — by electronic means.

**EXAMPLES:** Electronic voting machines. Voting on agenda items of stockholder meeting via the internet. Web-hosted systems for administering political petitions. Electronic Committee or Panel Meetings.

**SCENARIO:** As a registered voter, you receive mail from your local council containing a paper slip with a bar code identifying you *and* your right to vote in the next council election. You can use that slip in a variety of ways:

- add that slip into the envelope of your postal vote as a credential for your vote; the bar code is encrypted with a threshold scheme of  $k > 0$  trustees so your real identity can be bound to this vote only if all  $k$  trustees collude against you
- present that slip to the local election officer at your borough's voting location; the election officer scans the slip and verifies that you have the right to vote in that borough on that day, in addition to asking you your name and address (which she checks against her registrar and your National Identity Card); the slip will be stored for possible audits and ought not be connectable to the vote you completed in the voting booth
- visit the local election web-site and enter your vote through a secure session, where the slip is scanned on your PC in the process and its bar code passed on to the web server; authentication and prevention of link to real identity work as in the first item (assuming the web-page is accessed through an *anonymizer*)

**OUTLOOK:** Electronic voting machines are increasingly used in the USA, replacing traditional mechanical voting booths. E-Voting is already being used by professional bodies such as the IEEE and by pension funds such as the CREF-TIAA in the USA; *but such schemes currently don't offer anonymous votes — E-voting requires reliable implementations of anonymity.*

**ANALYSIS:** Full-scale electronic voting systems and their proof-of-concept implementations already exist in academic research. They are unlikely to replace fully traditional means of voting but provide a useful additional way in which subjects can cast their vote. More specifically, technology components and concepts from such E-Voting systems could be used in existing voting processes to great advantage, as illustrated by the scenario.

Bar codes that represent a credential for access to a resource can also be produced and printed on the subject's own computing infrastructure. E.g. customers of British Airways and EasyJet may check in online (subject to certain constraints), print out a boarding pass at home, and present it with their passport upon check-in. This is a powerful enabler for customer satisfaction (through a sense of control and short-cutting of work flow). Imagine the benefit if railway customers can print their tickets at home (including a printout of digital credentials) and won't have to pick them up at the station (either at a counter or through dedicated terminals, e.g. as is the case in King's Cross Station) or wait for them in the mail.

There is a larger picture here: E-Governance, which is not just about an organization having a web-based interface through which it offers services, but about managing data and processes (work flow) within IT systems such that different stake holders (e.g. civil servants as "producers" and private citizens as "consumers") have customized views and access to such systems. This applies to commercial organizations and public agencies alike.

**WHAT TO WATCH:** Encrypted and digitally signed certificates that provide sufficient information about the subject and the access privileges embodied in that certificate, e.g. bar codes. These certificates will be increasingly important as (one-time) hand-held tokens. Opportunities for improving authentication to combat election fraud. Trend of increased E-Voting in US elections at all levels (local, state, federal, and primaries), and therefore an increased pressure on IMSs to allow for contained but robust anonymity.

**KEY PLAYERS:** Government. Business.

**KEY ISSUES:** Privacy. Ownership. Trust and Culture. Attitudes to Risk. Internet.

## 2.8 Interoperability Standards

**DEFINITION:** Interoperability standards specify how important data or processes should be implemented so that other systems can understand and process them, if so desired.

**EXAMPLES:** Security Assertion Markup Language (SAML), Service Provisioning Markup Language (SPML), eXtensible Access Control Markup Language (XACML).

**SCENARIO:** Two companies want to connect together parts of their IMSs. They both have used the standard XACML to describe their internal access control policies, so they both have the tools to process such policy specifications whenever they decide to share them, e.g. in an initial negotiation phase.

**OUTLOOK:** Some of these standards will prevail, others may not be widely adopted (e.g. XACML). But the intent of these standards and their direction are right; so either these actual standards or some mutations thereof will become a lingua franca for the information security and other aspects of inter-operating IMSs.

**ANALYSIS:** These standards are very detailed and beyond the scope of this report. But they are all based on the eXtensible Markup Language (XML) so XML technologies will be important drivers here.

**WHAT TO WATCH:** Adoption rate of various standards in industry and the public sector. Growth and adaption rate of XML technologies.

**KEY PLAYERS:** Business.

**KEY ISSUES:** Ownership. Internet.

## 2.9 User-Friendly Solutions

**DEFINITION:** User-Friendly Solutions to Identity Management satisfy basic attributes of user interface design, as understood in software engineering: ease to learn, recoverable, having low ambiguity, etc.

**EXAMPLES:** Single-Sign-On, Identity-based encryption. Self-service password reset services. *Free* rural or urban wide area wireless networks. *Free* local area wireless access at prominent “public” spaces (railway stations, airports, etc.).

**SCENARIO:** Angie has just connected to her university’s Virtual Private Network (VPN) from her laptop, using a publicly accessible (i.e. free) wireless connection at the international airport in Vienna. With a single instance of a three-factor authentication she signs on to this VPN and can now access her email, go to internal web-pages for entering course-work marks, check on the current applications for her new research assistant position in the respective folder in the HR division of her college, and download publications from external sites for which her university has valid license agreements — without having to re-authenticate herself locally or externally.

**OUTLOOK:** Users will always want simple solutions but technical constraints may force some complexity on them. Users, if in control of that choice, will migrate to systems that they perceive to be simple but effective. Growing autonomy and involvement of subjects in management of IMSs and their role therein; self-serviced password reset services are a first example of this.

**ANALYSIS:** User interface design principles and their validation techniques are fairly mature and are obviously of use in the design and analysis of IMSs. For example, how easy is it for individuals to correct wrongly specified attributes in a given IMS? How easy is it to swap the supplier of your home utility? The latter has to do with interoperability standards, among other things. Most easy solutions sound too good to be true or compensate for simplicity with a daunting level of complexity “under the hood” (e.g. the mathematics of hierarchical identity-based encryption). But simplicity is a highly desirable goal as it is a competitive edge and increases the likelihood of correct interaction with an IMS. In addition, “user-friendly” solutions go beyond friendly interfaces, e.g. as in consumer/citizen-centric IMS processes.

**WHAT TO WATCH:** Identity-based encryption. VPNs becoming the norm for private and public sector IMS backbones. Google’s promise to offer San Francisco residents and visitors a free 300 kilobits per second connection anywhere in that city. Similar moves in urban (e.g. London) and rural (e.g. Southern Irak) areas.

**KEY PLAYERS:** Individuals. Government. Business.

**KEY ISSUES:** Ownership. Trust and Culture. Criminality. Internet.

## 2.10 Regionally/Globally Unique Identifiers

**DEFINITION:** Means of identifying subject/resource uniquely, either within a well specified region or worldwide.

**EXAMPLES:** Oyster cards. Radio Frequency Identification Devices (RFIDs). Universally Unique Identifiers (UUIDs). The Digital Object Identifier System (DOI).

**SCENARIO:** Duncan travels to Tokyo for a short but well deserved city break. His Oyster card has a universally unique identifier (UUID) on it and Duncan naturally carries that card with him upon arrival in Tokyo as it is needed for his initial and final part of the trip in London. To his astonishment he finds out that London and Tokyo Transport have a trade agreement honoring each others' cards on the other network. This is being made possible by the UUID technology and the interoperability standards for these touch cards. Duncan is relieved that he won't have to purchase a ticket in Tokyo (his Japanese is pretty poor), but still has a hard time to read the Japanese letters for station and train names.

**OUTLOOK:** Regional identities (as in "I am a Sussex man") may map onto regional IMSs. E.g. RMV is a regional transport network that spans Frankfurt, Mainz, Wiesbaden, Darmstadt, Giessen, etc. in Germany. Agreements with the German national railway service provider Deutsche Bundesbahn, as well as with some boundary regions and their transport systems, exist. "Think globally, act locally" can be turned into regional IMSs that have global meaning and form strategic relationships with other regional IMSs.

**ANALYSIS:** Regional identifiers uniquely identify a subject or resource within a specified region; e.g. at present an Oyster card won't be recognized in the Tokyo tube. Universally unique identifiers are guaranteed to be unique worldwide, e.g. URIs (uniform resource indicators) — of which URLs of the worldwide web are an example — are expected to be globally unique. For if not, two DHL customers may look at the same tracking information although these customers want to track different deliveries.

There could be function and mission creep with such identifiers. The fictitious scenario above shows a benign function creep in that the global uniqueness of a regional card can be exploited to enhance its service capabilities.

Such creep could also be perceived as a threat: If RFIDs contain UUIDs, then they could be tracked anywhere, and not just within their initial scope, e.g. the logistic flow from the distributors to Tesco warehouses, supermarkets, and up to their cashier points may not stop when customers leave; items may be recognized overseas, and by organizations other than Tesco or its affiliates.

There is an issue of the range of detectability. Citizens may feel comfortable with a chip on their biometric passports if that chip can only be read in the range of centimeters and with opened passport. Citizens are likely to feel uncomfortable with RFIDs implanted into their clothing that could be detected during a leisurely stroll in Victoria Park.

**WHAT TO WATCH:** Cost issues of RFIDs. Standards for, and interoperability of, RFIDs. Convergence of standards for UUIDs. Public perception of UUIDs and their scope and range of detection.

**KEY PLAYERS:** Individuals. Government. Business.

**KEY ISSUES:** Exclusion and Inequalities. Privacy. Ownership. Trust and Culture. Environment. Demographics. Criminality. Internet.

## 2.11 Pie-in-the-sky technologies

- *Quantum-computing based digital identities*: If quantum computers can be build for more than a few quantum bits, then large integers can be factored efficiently. So all *existing* public-key encryption based on RSA, in particular RSA digital signatures and certificates, can be broken. But quantum computing offers new solutions, e.g. encryption that can only be broken in flawed implementations or by breaking the laws of quantum physics. This can be a very disruptive technology, not only in terms of breaking legacy codes, but even more so in the erosion of trust into any treaties or legal documents that would have been signed with digital signatures based on such then-breakable encryption.
- *Adaptive behaviour*: Important in ad-hoc formed networks, e.g. car platooning on motor-ways. Identity-related entitlements need to adapt to changing roles within such networks, e.g. a follower in a platoon may decide to become the leader of a newly formed platoon. More generally, IMSs need to be able to adapt to different levels of threat, e.g. in contingency planning of major environmental disasters.
- *Computer Forensics*: Ever-increasing importance in criminal investigations. Serious and well developed science and technology. Question of whether increased logging of information on computer devices can help with future potential forensic tasks (this is standard practice in some financial trading companies). This should be seen within the context of future IMSs and their privacy issues.
- *Nanotechnology*: Offers opportunities for “molecular steneography”, the almost undetectable identity tra-  
cability for chemicals, fluids, and general consumer goods.

### 3 References

*Automated Highways and Vehicles for Increased Capacity and Safety*

Delta Scan: The Future of Science and Technology, 2005-2055  
[humanitieslab.stanford.edu/2/432](http://humanitieslab.stanford.edu/2/432)

*Broadband Networks Available Anywhere, anytime*

Delta Scan: The Future of Science and Technology, 2005-2055  
[humanitieslab.stanford.edu/2/293](http://humanitieslab.stanford.edu/2/293)

*New Technologies for Cooperation*

Delta Scan: The Future of Science and Technology, 2005-2055  
[humanitieslab.stanford.edu/2/349](http://humanitieslab.stanford.edu/2/349)

*Quantum Computing Breakthroughs*

Delta Scan: The Future of Science and Technology, 2005-2055  
[humanitieslab.stanford.edu/2/287](http://humanitieslab.stanford.edu/2/287)

*The Rise of Proactive and Context-Aware Computing*

Delta Scan: The Future of Science and Technology, 2005-2055  
[humanitieslab.stanford.edu/2/340](http://humanitieslab.stanford.edu/2/340)

*Tracking Physical Objects Made Easy with RFID*

Delta Scan: The Future of Science and Technology, 2005-2055  
[humanitieslab.stanford.edu/2/297](http://humanitieslab.stanford.edu/2/297)

### 4 Recommended Reading

Philip J. Windley, *Digital Identity*, O'Reilly Media, Inc., 2005.

### 5 Acknowledgements

The introduction and the presentation of some key technologies were in part inspired by Windley's excellent book mentioned as recommended reading. The participants of the workshop are thanked for their lively, often passionate, and always very informed discussion of these subjects. I have tried to incorporate their insights and feedback into this amended report to the best of my ability, and within the given space requirements.