Identity Management as Public Innovation: Looking Beyond ID Cards and Authentication systems[1]

Miriam Lips
Research Fellow, Oxford Internet Institute, University of Oxford, UK &
Associate Professor, Tilburg Institute for Law, Technology and Society, Tilburg University, The Netherlands
Email: miriam.lips@oii.ox.ac.uk and a.m.b.lips@uvt.nl

John A. Taylor
Professor of Government & Information Management,
Caledonian Business School, Glasgow &
Research Associate, Oxford Internet Institute, University of Oxford
Email: john.taylor@oii.ox.ac.uk and jta@gcal.ac.uk

Joe Organ
Research Fellow, Oxford Internet Institute, University of Oxford, UK
Email: joe.organ@oii.ox.ac.uk

Abstract:
Governments are introducing, managing and using digitised personal identification and authentication systems in their service relationships with citizens in addition to, and increasingly in replacement of, traditional forms of personal identification and authentication. An important question is to what extent these developments are causing innovation in the sense of a renewal of traditional institutions in the government domain. By presenting public debate with regard to the recently proposed UK national identity cards initiative we will show that a public administration perspective is needed to be able to detect more fundamental forms of innovation in government.

Key words: Identity Management, personal identification, authentication, e-government, ID card, passport

[1] Personal Identification and Identity Management in New Modes of E-Government. Ref: RES-341-25-0028', A.M.B. Lips, J.A.Taylor and J. Organ

1. Introduction

Governments around the world are introducing, managing and using digitised personal identification and authentication systems in addition to, and increasingly in replacement of, traditional forms of personal identification and authentication. Digitised personal identification systems can offer customer convenience; citizen mobility and empowerment; efficiency and/or effectiveness of public service provision, including joined-up government; and the enhancement of public safety and security, including general law enforcement. These systems therefore not only appear to enable the modernisation of government; they also enable government to fulfill its service providing functions, through its ability to authenticate personal identifiers provided by citizens in e-government relationships. Authentication, or the assurance that a person is who [s]he says [s]he is, is generally acknowledged as an essential requirement for the provision of many government services to citizens. Digitised personal identification and authentication systems thereby become the *sine qua non* of successful e-government. The innovative potential of these systems seems to be substantial, therefore; but is innovation in government actually happening as a result of the implementation and use of these systems, in what form and to what extent?

It is clear that e-ID, e-authentication and the broader field of Identity Management (IDM) can be observed as important topics emerging on national and international policy agendas, in e-government and other policy domains (eg EU Ministerial e-Government Declaration 2005). These concepts however are relatively new terms, whose meanings remain unsettled, at least from a social science perspective (Lips et al, 2005). In many countries the clarification and implementation of these concepts and their related personal identification and authentication systems has started only recently, leaving us without a clear perspective on what ultimately they will change or offer to governments. We observe in some countries that the introduction of these topics is surrounded by considerable public debate, indicating popular anticipation of a profound impact of new forms of personal identification and IDM on the machinery of government and its relationships with citizens. In the UK for instance the introduction of Identity Cards, *inter alia* an important component of the UK antiterrorist legislation, is causing heated public discussions about their pros and cons. In other countries, although with much less public attention or concern, comparable developments in the field of IDM are taking place in society. For instance, perceived as an eID best practice and copied by governments (eg Portugal) and even commercial organisations (eg Microsoft) the Belgian eID Card is being used in an increasing number of public and commercial services and has an uptake of at least 1.5 million, virtually without public debate.

Unquestionably these developments in the field of IDM will have some impact on the future management and organisation of electronic public service provision to citizens. The question is then if, and if so in what respect and to what extent, these developments are causing innovation in the sense of a renewal of traditional institutions. Are new forms of personal identification and IDM actually bringing about what Schumpeter (1942) has called a process of ‘creative destruction’, in this case of the traditional relationships including the information practices between government and citizens? Or are these developments merely conceptual innovations, ‘old wine in new bottles’, with limited

change implications for existing practices? Our main argument in this chapter will be that we need to make use of a public administration perspective, i.e. an *institutional* assessment of modernisation efforts in government, to be able to detect more fundamental forms of innovation in government as a result of the introduction of these digitised personal identification and authentication systems. At present, the two dominant perspectives regarding e-ID, e-authentication and IDM in general in the policy making arena are a technical design perspective based on the application of technical logic to complex public problem solving and a 'privacy-advocacy' point of view based on normative assumptions about the importance of privacy to human freedoms. Both perspectives can be acknowledged as *instrumental* assessments of the modernisation efforts related to the introduction of new digitised personal identification and authentication systems in public administration. We will further illustrate these perspectives on the basis of the recently proposed UK national identity cards initiative. But before we do so we will introduce the innovative potential related to emerging digital forms of identification, authentication and IDM.

2. New forms of identification, authentication and personal identity

Traditionally, personal identification of the citizen resides at the heart of many forms of government service delivery, from health services to policing, social services, housing and taxation, to cite some general examples. Historically and archetypically, such identification has been undertaken through manual form filling, coupled to the verification of personal identity through paper-based authentication processes. Through time authentication processes related to the use of paper-based authentication systems, such as the passport, have been largely constant. The passport holder shows his or her passport to the person officially recognised to check and verify that the document carrier is the person shown referred to through the information, including photograph, included in the document. Set within a traditional environment of trust, these authentication processes often have been supplemented by informal assessment of the citizen by the official, based upon their appearance of honesty or upon the official's knowledge of the citizen within the local community.

Within this archetype of personal identification of the citizen, public organisations delivering services to the public became vast repositories of stored paper records, gathered together as the proof of entitlement that was required before access to the service could be authorised. Moreover, the entitlement to service was realised through a form of administrative equity that saw citizens being 'handled' *seriatim*: the citizen claimant for service, for example, was included onto a waiting list, in line, and was provided service and thereby taken off that waiting list in the strict order in which the waiting list was entered. Furthermore, the service accessed by citizens was 'universal', deriving from the administrative equity principle of 'equality under the law' ie within any particular governmental jurisdiction (national, regional, local, functional), rights to the same service level were afforded to all citizens (Taylor et al, 2006).

Now, in the rapidly developing on-line activities of government new forms of personal identification are being used in which the identity of the citizen increasingly is being established through the gathering of personal or person-related information in electronic relationships rather than in face-to-face relationships between the citizen and government. Emerging within the digital era are three main ways of identifying a person operating within an electronic environment; accepting a self-declared statement of identity that draws upon details known by that person about who they are (eg a username, registration number, address details, password, PIN); accepting an item of identity the person physically possesses (eg a smartcard, electronic tag, mobile phone); scrutinising aspects of the physiological identity of the person (eg fingerprint, iris, face, DNA). Moreover these means of identification can be used in combination, as an affirmation of identity and as a step towards authentication of that identity (eg showing a credit card and supporting it with a PIN).

With the increasing use of these new forms of personal identification and authentication we can observe new types of 'personal data' being involved in citizen – government service relationships. In the abstract, these new types of personal data can be perceived in concentric circles at varying distances from the individual's core identity (Marx, 2003). The outermost circle is that of individual information which includes any data which can be linked to a person, for instance a license plate, email-address or click behaviour on the Internet; the most inner circle represents the individual's core identity based on biological ancestry and family relations. In between are concentric circles of private, intimate and sensitive information, followed by unique identification.

Combinations of different types of personal data are at the basis of new forms of e-government service provision. Examples of these new forms are personalised public service provision and Customer Relationship Management (CRM). Within these new forms of public service provision we may observe new and more complex ways of categorising, segmenting and grouping citizens that enable different modes, levels and paces of service provision to be implemented. With that, these developments offer possibilities to set aside the historically arrived at administrative logic of 'service by waiting list' derived from the policy norm of universalism and the legal principle of equality under the law (Taylor et al, 2006).

Moreover in the emerging electronic public service environment we recognise the multiple relationships that the citizen has with government agencies, each supported by an assembled form of a citizen's personal data (cf Fishenden, 2005). For example, the citizen has an Inland Revenue taxpayers identity, a Health Service patient identity, a Social Security identity as a contributor and claimant within the system, a drivers identity, and a resident identity within a public housing scheme. Traditionally, a separate citizen's identity profile was constructed, managed and used for each of these relationships. In the current digital environment it has become much easier in principle to create and manage an integrated identity profile on the citizen, for instance through the use of a unique number (eg social security number), or for the citizen to make use of a singular personal identification and authentication system to access a variety of government services. Potential IDM solutions such as these are being looked into by many governments around the world and, more specifically, practices in this last respect can already be found in for instance New Zealand, The Netherlands (DigiD-initiative), and the UK (Government Gateway Project).

3. Informational trends resulting from new identification technologies

These new modes, levels and paces of e-government service provision are developing on the basis of several general informational trends we may empirically observe (cf. Marx, 2003). We describe these trends below, without making any judgements about their nature or direction:

- an increasing use of digital forms of identification and authentication of personal data instead of physical forms;
- an increase of the ability to discover and track personal information in real time across physical barriers, locations and over time;
- an increasing integration of life activities with the generation of personal information (eg the use of credit cards or mobile phones);
- an increased blurring of lines between public and private places makes personal information more publicly available;
- an increased merging of previously compartmentalised personal data; and
- an expansion of ways of measuring and classifying citizens, with greater precision compared to traditional measures, such as paper-based methods.

These informational trends lead to different outcomes in society, which happen simultaneously and may be mutually contradictory. For instance, as a result of these informational trends an individual's ability to remain unnoticed and, after being noticed, to remain unidentified in society has declined significantly. In many cases we can observe a development towards the construction of (more) complete identity profiles on individuals (cf Prins & de Vries, 2003). This expanded ease of identity construction also has led to increased requirements of some form of identity validation in public and commercial activities. We can observe for instance a major expansion of laws, policies and procedures mandating that individuals provide personal information. Another related development is to more and more require personal identification with the heaviest possible means of identification, i.e. biometrics (Ibid). Arguments for using this far-reaching form of identification are often related to convenience (eg efficiency and increased speed of service delivery), combat of fraud or crime.

At the same time we may observe an increased freedom of choice for individuals to present their identity. Especially as a result of the expansion of impersonal, digital interaction, for instance supported by the Internet, an individual's personal identity is becoming relatively less unitary, homogeneous, fixed or enduring. Moreover in presenting the self, as indicated earlier, an individual is able to make use of new functional alternatives to his or her core identity. Different types of pseudonyms (eg email-address, phone number, credit card details, unique number) for instance can be used to present the self for various purposes in interactions with others. In doing so, but also through other available methods nowadays, an individual has increased possibilities to protect personal data that is more closely related to his or her core identity. As people play different roles in social processes (eg, as employee, citizen, customer, or family

member), each individual is in fact owner of many different identities, and is known to his environment under many different pseudonyms such as an e-mail address and GSM phone number. As Goffman has extensively shown, we cannot avoid conveying information about ourselves every moment that we are in the presence of others, but we may be able to affect the way in which those impressions are given to others (Goffman, 1971). Moreover, parallel to the observed expansion of lawful personal information requests, we can observe a significant expansion of laws, policies and management approaches that restrict and regulate the collection of personal information and its subsequent treatment.

4. Identity cards as a Technical Domain of Understanding

At present governments clearly have discovered these informational trends resulting from the availability of new technologies for detecting and validating personal information. Governments seem to have acknowledged these new identification and authentication technologies as contributors to information security and to increased confidence in the identity of individuals in electronic relationships therefore (Crompton, 2005). The implementation and use of these technologies in government service provision have become strongly recognised in the digital era, both for more optimal security provision and to support the spread and successful uptake of e-Government (Hof, 2002; Davies, 2005, p.27; eEurope Action Plan 2005). Generally, the introduction of a more robust form of IDM in citizen – government relationships is perceived as an essential solution for a variety of policy problems.

At present a prime example of the introduction of a new means of personal identification in government is the proposed UK national identity card legislation. The aims of the UK central government are to introduce a national identity card containing three biometric identifiers together with a national identity register acting as a central database in which a range of details about individuals will be stored. In the short term ID cards will be voluntary, though anyone renewing a passport or drivers' licence will automatically receive an ID card, and foreign visitors will have to obtain a biometric residence permit; in the longer term the ID card will become compulsory (Cragg Ross Dawson, 2004, p.1).

The UK government has defended its proposals for a variety of reasons, including prevention of benefit fraud, prevention of terrorism, prevention of identity theft and authentication in e-government services. Although the core policy objective is difficult to ascertain the location of the ID card legislation within the Home Office is believed to especially support the policy need to uphold security, law and international migration protocols (Davies, 2005, p.34). Research findings show that UK citizens are generally supportive of an ID card (Dutton et al, 2005, p.114; Home Office, 2003; Detica, 2004), or even consider their introduction as inevitable (Cragg Ross Dawson, 2004, p.6). This is in accordance with situations in other European countries where the implementation of ID cards did not cause strong public debate (eg Belgium, Austria, Finland).

In the UK context, however, critics have pointed to the overemphasis in the public debate on the visible, technical means of identification proposed by the UK government,

the ID card itself, and, with that, the lack of public attention for the more invisible aspect of how citizens' data will be handled by the UK government (eg Davies, 2005, p.38; the UK House of Lords Constitution Select Committee). Other critical voices point at seemingly unrealistic technical expectations of the ID card scheme, using arguments such as the fact that neither the major contractors nor the government have shown themselves capable of organising and implementing an outsourced IT scheme on this scale: no country has attempted to use biometrics technologies to register a population the size of the UK (The LSE, 2005); the proposed requirement for 100 per cent accuracy: has there ever been an identification system which is 100 per cent accurate? (Neville-Jones, 2005); trials of the card scheme have demonstrated that a substantial number of specific groups of the UK general population (eg disabled people) may not be able to enrol on biometrics based verification schemes (UK Passport Service Biometrics Enrolment Trial Report, 2005); from industry, '*a national ID card for the UK is overly ambitious, extremely expensive and will not be a panacea against terrorism or fraud, although it will make a company like mine very happy*' (Tavano[2], 2005); and, from a collective group of LSE academics, that the government proposals for a secure national identity system are too complex, technically unsafe, overly prescriptive, massively more costly than government is itself estimating and lack a foundation of public trust and confidence (The LSE, 2005, p.3).

This ID card debate illustrates the traditional way in which IDM issues have been tackled by governments so far. Optimal security, technical reliability, ID "theft[3]" and accuracy repeatedly have been important topics in public decision making about available personal identification and authentication systems at many occasions in the past. This debate therefore is not a new debate emerging in the current era, but can be observed for instance for the paper-based passport system on a regular basis in many national public decision making arenas. Interestingly, if we look at personal identification and authentication systems in practice, such as the use of the passport in authentication procedures, there have not been notable changes in this authentication system through time. Moreover this similarity in restricted, technically focused IDM topics may explain the current ease with which governments are trying to copy ID card systems or authentication systems from 'best practices' available in other countries. From a technical perspective new forms of personal identification, authentication and IDM can be perceived as improved technical means to be used in similar identification and authentication practices compared to the past. In terms of innovation these new means may bring about process innovation for governments, but their actual use in practice would need to demonstrate that type of innovation before it can be confirmed.

4. Identity cards as a Legal-Normative Domain of Understanding

[2] Biometrics specialist for Unisys, one of the companies considering bidding for contracts. Quoted in The Guardian, 21 October 2005

[3] ID theft as a concept has only emerged recently. The theft or fraudulent use of ID documents however exists for a long time.

Where a non-technical perspective is being used actively to approach the informational trends that we have noted here the perspective that is most common is 'legal-normative', one that derives especially from data protection legislation. The potential uses of identification and authentication technologies and their implications for individual citizens' privacy is often couched by privacy advocates in Orwellian big brother scenarios. They usually claim that a contradictory societal outcome of leaving more control to the individual over his or her personal information would be in accordance with legally defined civil rights and therefore a more appropriate scenario for which to strive. Privacy in this sense may be understood as the right to informational self-determination, i.e. individuals must be able to determine for themselves when, how, to what extent and for what purpose information about them is communicated to others.

We can observe the presence of this legal-normative perspective in the UK national identity card debate. A general conviction is that, with the introduction of an ID card, UK citizens are required to trade an element of their privacy for increased security (eg Davies, 2005, p.26). Proposals are for instance that personal details to be stored on the register will include three biometric identifiers, residence, former residences, and details of change of residence; moreover it will contain information about numbers allocated to the individual and official personal documents. For reasons of 'public interest' the Home Secretary would be able to pass on to other parties information kept on the national register, without the individual's consent and without the individual being entitled to know how his/her data is being used (Davies, 2005, p.35).

These proposals have convinced the LSE to comment that this legislation would conflict with data protection legislation, on the basis that the function of the register is too ill-defined (The LSE, 2005). Also several other critics, including the UK Information Commissioner, expressed concerns about the lack of clarification in the UK legislation proposals about the nature and extent of personal information which will be collected and retained, plus the reasons why such a large amount of information needs to be recorded as part of establishing an individual's identity (UK Information Commissioner, 2004). In addition, the centralisation of this information has been questioned, as alternative models for data storage could be chosen, such as for instance more data storage on the ID card and less data in the national register.

Proponents of this legal-normative perspective generally also try to explain that the dominant information principle in these government proposals is in keeping with the social norm attaching to identification of the citizen, rather than an alternative norm such as the acceptance or encouragement of anonymity. With anonymity as the guiding principle, the minimal collection of personal information by government would be the norm. However, with the current ease of collecting, managing and using of various types of personal information, the dominant information principle of individuals' identification seems to become widespread in the information society. A guiding principle of anonymity in the emerging information society appears to be far removed therefore, both empirically and normatively (Bailey, 2004).

Nonetheless, the developing IDM expert community in which information security specialists, (former) data protection commissioners, and privacy advocates can be recognised, has adopted more or less a set of laws for digital IDM, in which the principle of anonymity guides thinking. One illustration of this attention to anonymity is

to be found in the Seven Laws of Identity (Cameron, 2005[4]), which have been embraced by many IDM experts as IDM *principles* (see for instance a paper of the former Australian Federal Privacy Commissioner Malcolm Crompton, 2005):

1. *User Control and Consent*: Digital identity systems must only reveal information identifying a user with the user's consent;
2. *Limited Disclosure for Limited Use*: The solution which discloses the least identifying information and best limits its use is the most stable, long-term solution.
3. *The Law of Fewest Parties*: Digital identity systems must limit disclosure of identifying information to parties having a necessary and justifiable place in a given identity relationship.
4. *Directed Identity*: A universal identity metasystem must support both "omnidirectional" identifiers for use by public entities and "unidirectional" identifiers for private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.
5. *Pluralism of Operators and Technologies*: A universal identity metasystem must channel and enable the interworking of multiple identity technologies run by multiple identity providers.
6. *Human Integration*: A unifying identity metasystem must define the human user as a component integrated through protected and unambiguous human-machine communications.
7. *Consistent Experience Across Contexts*: A unifying identity metasystem must provide a simple consistent experience while enabling separation of contexts through multiple operators and technologies.

Interestingly, several of these 'laws' on identity can be recognised as similarly looking to the OECD's basic principles for the protection of personal data[5]. These laws therefore seem to propose to integrate the protection of civil rights in digital identity systems and to create what may be called 'privacy enhanced' IDM systems.

Through time we can observe that privacy and security values often have been balanced by governments with regard to the use of identification systems. The history of the use of the passport shows us that personal identification procedures mainly changed during moments of societal crisis, such as the French Revolution, the First World War and the Second World War (Torpey, 2000; Agar, 2003). Although the authentication system itself, the paper-based passport, more or less stayed the same through time, the frequency and intensity of its use, as well as the officials executing the authentication process usually changed during these periods of war. A similar effect can be observed in more recent times after the events of 9/11 and the London bombings.

[4] See http://www.identityblog.com

[5] See for instance the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Another general observation is that the introduction of new technologies in society, such as in the case of ID cards in the UK[6], inevitably raises public concerns, however muted they might actually be in public discourse, regarding individuals' privacy (see for instance Westin, 2003). The introduction of new identification technologies in itself cannot logically imply however that the monitoring and disciplining capabilities of these technologies will be used in practice and that privacy will be diminished *per se*. Our own research findings confirm this point of view by showing that new identification technologies can be introduced and used with few if any implications for individual privacy (Lips et al., 2005). From a legal-normative point of view new forms of personal identification, authentication and IDM can be perceived as new vehicles to re-open a continuous, more profound battle for improving civil rights. In terms of innovation the introduction of these new technologies can be perceived as conceptual innovation, as it moves the focus in governance away from more restricted concerns regarding individuals' privacy to a more comprehensive personal identity point of view which for instance simultaneously takes into account privacy and security values.

5. Identity cards as a Public Administration Domain of Understanding

"O*ne of the properties of effective digital innovation is that it is often rendered invisible to the public, while remaining a transformative social presence*"(Davies, 2005, p.1). What Davies seeks to indicate with this remark is the importance of looking beyond a new technology and its introduction and public use to be able to observe its innovative impact. We would like to add to this the importance of broadening the perspective and in so-doing looking behind the face value impressions of the technology. As ID cards in the UK have not been implemented thus far we would like to illustrate our point by focusing again on the history of the passport as an important predecessor of the ID card; two identification technologies with many characteristics in common.

If we look at the history of the passport we can observe what could be called a *révolution identificatoire* in the public domain of nation states (Torpey, 2000: following Noiriel). Whereas the power to regulate citizen movements used to belong to private institutions like the church, or market institutions like serfdom, national governments succeeded in increasingly gaining authority over activities in which a person's status of national citizenship needed to be confirmed. By issuing official national identification papers like the passport, nation states have established the exclusive right to authorise and regulate the movement of people. As identification papers evolved into an administrative expression of national citizenship, citizens have become dependent on nation states for the possession of an official "identity" which may significantly shape their access to various spaces and activities.

Interestingly the first passports and passport controls for that matter were not so much used to regulate citizens' access to spaces beyond their home country as we are used to today, but to *prevent* people from leaving their home territory. Consequently those citizens leaving their Kingdom (for instance under the old regime in France) were

[6] Interestingly the generally acknowledged successful eID in Belgium did not raise any public concerns at its introduction but had a socially accepted paper-based ID card predecessor since the 2nd World War.

required to be in possession of a passport authorising them to do so. The main purpose of these documentary requirements was to forestall any undesired migration to the cities, especially Paris (Torpey, 2000, p.21).

When geographically based citizen registrations were created and used for providing the personal details in passports, social distinctions started to be made between true 'citizens' and 'non-citizens', also to look for traitors who would obviously belong to the alien, non-citizen category. At that time the French government for instance decreed the establishment of civil status (*l'état civil*), which determined that an individual could only exist as a citizen once his or her identity had been registered by the municipal authorities, according to regulations that were the same throughout the national territory. Consequently passport controls to *enter* countries or districts became more extensive.

In the 19th century in Prussia, the practice could be found whereby incoming travellers were provided with a passport from the receiving state rather than by the state of the traveler's origin. These passports were no longer issued by local authorities but by higher-level officials. The foreigners and unknown persons circulating in the country were to be subjected to heightened scrutiny by the Prussian security forces, with the assistance of specific, legally defined[7] intermediaries like landowners, innkeepers and cart-drivers (Torpey, 2000, p.60). In the late 19th century a generally liberal attitude of governments toward freedom of movement could be observed; a development which was stopped in the 20th century by national government's desires to regulate immigration, also targeted to restrict immigration of specific national groups (eg USA) and to stimulate economic opportunities for their own citizens abroad (eg Italy), to be able to better protect their country for suspicious people in times of war (eg Germany, UK, France), or to have the possibility to track their own nationals for conscription into their armies (eg Germany). Generally in the 19th and 20th century we may observe a development towards two models for citizenship attribution and the related issuing of passports to citizens, namely on the basis of *ius soli* ("law of the soil") and *ius sanguinis* ("law of the blood") (see for instance Brubaker, 1992). The latter model had to do with the development of enhanced mobility of citizens beyond the state's territorial boundaries, especially for economic reasons, and the possibility for nation states therefore to continuously keep a relationship with citizens living abroad.

It is very interesting to see the changing meanings, uses, and values attached to a similar technical means and process for personal identification through time, the passport. Besides values which seem to be obviously related to a citizen's personal identity, eg security and privacy, we can observe ownership, public safety, service, economic, and international migration values being applied by those institutions issuing passports. This historical analysis also makes us aware of the importance to perceive the use of IDM systems in non-evolutionary ways. For instance to look for 'punctuated equilibria' (Baumgartner & Jones, 2002) in the evolution of identification systems, eg the periods of crisis during the history of the passport, as important moments where radical shifts happen in the use of these identity systems.

Moreover it provides us with several insights in shifts within and between public and private sector involvement in official identification and authentication processes, 'trusted third parties', such as city officials, higher level public officials, but also

[7] The 1813 passport law in Prussia.

landowners, innkeepers and cart-drivers. Together with the passport issuing institutions these 'trusted third parties' have played an important role in the attribution of citizens rights.

Insights like these may be of further importance when looking at current developments in IDM in e-government service provision. For instance, e-authentication systems for electronic public service relationships between government and citizens are being developed which introduce new 'trusted third parties' or intermediaries outside government, so-called 'authentication solution providers', to check citizens' identity for electronic services that require stronger authentication levels. Examples of these intermediaries are banks, telecommunication providers, software companies and credit reference agencies.

From a public administration perspective we can observe that the introduction and use of the passport has fundamentally changed the relationship between governments and citizens, and has led to alternative developments and designs in citizenship attribution. We can conclude therefore that at least this particular identification technology has caused a *révolution identificatoire* and, through that, institutional innovation in the public domain between governments and citizens. From an innovation point of view the question remains over what new forms of personal identification, authentication and IDM will occur.

6. Further analysis: implications for institutional innovation

Looking through these different perspectives shows us that beyond the technical designs of newly available forms of personal identification and authentication for e-government service provision, which appear to have remarkable similarities, a whole variety of nuances resulting from differently chosen or confronted governmental, managerial, and democratic design aspects come to the surface. Where *technical* or even *legal-normative* standardisation of these new identification and authentication systems for e-government service provision may appear to be an obvious development, other *public administration* factors of importance to the application and deployment of these systems seem to point in an opposite direction. In many countries we may acknowledge the presence of similar *instrumental* assessments of modernisation efforts through the introduction of IDM, namely technical or legal e-ID and e-authentication policy designs, but with different *institutional* implications for further development of the e-government service domain in terms of governance, citizen – government relationships and citizenship.

What the public administration perspective reveals to us is the profound influence these new forms of personal identification and authentication may have on the governance of citizen – government relationships. Institutional innovation, the renewal of traditional citizen –government relationships as a result of the creation and development of new information practices, appears to be happening as a result of the introduction of IDM in e-government. As a result of these identification and authentication measures the nature of citizenship, which can be considered as a function of citizen –government relationships, is changing. Similarly to the analysis of the passport's history we may observe that borders between customers and non-customers of government organisations;

identified or non-identified subjects of the state; authenticated citizens or non-authenticated citizens, are being reset as a result of these newly available forms of authentication and identity management in e-government relationships. Not only does the same authentication allow the possibility for government to provide people with access its virtual territories; it also allows governments to keep people out of them. Analogously to the Prussian era where intermediaries like landowners, innkeepers and cart-drivers supported the government in the checking and validation of a person's identity, new trusted third parties are emerging in the e-government domains in these countries to help government to check people upon their trustworthiness.

With these new digital forms of personal identification, authentication and identity management we seem to have arrived into a new *révolution identificatoire* in the public domain, where a law of informational identity, a so-called *ius informationis*, may soon replace the existing models of citizenship attribution in the analogue world, *ius soli* and *ius sanguinis*. We are now seeing the reworking of information on and about the citizen-as-consumer so as to classify, to "sort", the citizen in ways that enable the segmentation of the service being provided (Lyon, 2003). Citizen sorting opens the possibility that these forms of remote checking and validation will shape access to service in a variety of ways largely hidden to the end consumer, breaking down the historic eligibility of the citizen to service consumption, based on a universal access conception of citizenship.

What will happen in eras of crises with the application of this newly developing model of citizenship attribution remains to be seen. Whilst there is this chief concern with enhancing e-government service provision to entitled, trusted citizens, there is, nonetheless, recognition that the security agenda of modern government is adding to a climate wherein the identification of the citizen is seen as of paramount importance. If services to the citizen are to be provided effectively, then identity issues come to the fore. If enhanced personal and State security is paramount then, once more, the means of identifying individual citizens becomes of crucial importance.

References

Agar, J. (2003), *The Government Machine: a Revolutionary History of the Computer*, The MIT Press.

Bailey, D. (2004), *The Open Society Paradox: why the 21st century calls for more openness – not less*, Virginia, Potomac Books.

Baumgartner, F. & B. Jones (eds) (2002), *Policy Dynamics*, Chicago, University of Chicago Press

Brubaker, R. (1992), *Citizenship and Nationhood in France and Germany*, Harvard University Press, Cambridge

Cragg Ross Dawson (2004), *Public perceptions of ID cards. Qualitative Research Report*, COI Ref: 262 151.

Crompton, M. (2005), *Trust, Identity and Connected Government*, paper presented for The Evolution of e-Government: from Policy to Practice, a forum for the Research, Development and Evaluation Commission, Taipei, 24 June 2005.

Davies, W. (2005), *Modernising with purpose: a manifesto for a digital Britain*, Institute for Public Policy Research, London, UK.

Detica (2004), *National Identity Cards: The View of the British Public*, April 2004

Dutton, W.H., C. di Gennaro & A. Millwood Hargrave (2005), *The Internet in Britain : The Oxford Internet Survey (OxIS)*, May 2005, Oxford Internet Institute, University of Oxford.

EU Ministerial Declaration on e-Government, 24 November 2005, Manchester, Ministerial eGovernment Conference 2005 Transforming Public Services, available at: http://www.egov2005conference.gov.uk/documents/proceedings/pdf/051124declaration.pdf

European Commission (2005), eEurope Action Plan 2005, available at: http://europa.eu.int/information_society/eeurope/2005/all_about/action_plan/index_en.htm

Fishenden, J. (2005), *eID: Identity Management in an Online World*, paper presented at the 5th European Conference on e-Government, June 2005, Antwerpen, Belgium.

Goffman, E. (1971), *Relations in public; microstudies of the public order*, New York, Free Press.

Hof, S. (2002), Arguments for a Holistic and Open Approach to Secure e-Government, in: R. Traunmüller and K. Lenk (Eds.), *EGOV 2002*, LNCS 2456, pp.464-467, Springer-Verlag, Berlin/Heidelberg

Home Office (2003), *Identity Cards – A Summary of Findings from the Consultation Exercise on Entitlement cards and Identity Fraud*, Cm 6019.

Lips, A.M.B., J.A. Taylor and J. Organ (2005), *Electronic Government: Towards New Forms of Authentication, Citizenship and Governance*, paper contribution to the Oxford Internet Institute's Cybersecurity Conference, 8-10 September 2005

Lyon, D. (ed.) (2003), *Surveillance & Social Sorting: privacy, risk and digital discrimination*, Routledge, London & New York.

Marx, G.T. (2003), *Varieties of Personal Information as Influences on Attitudes Toward Surveillance*, Paper prepared for a Conference on 'The New Politics of Surveillance and Visibility', available at http://web.mit.edu/gtmarx/www/vancouver.html

Neville-Jones, Dame P former chair of QinetiQ. Reported on 18/10/05 by silicon.com, 'Lack of "balls" in Whitehall will hinder ID cards' Will Sturgeon http://www.silicon.com/publicsector/0,3800010403,39153447,00.htm

Prins, J.E.J., & M. de Vries (2003), *ID or not to be? Naar een doordacht stelsel voor digitale identificatie*, Rathenau Institute, The Hague, The Netherlands

Schumpeter, J.A. (1942), *Capitalism, Socialism and Democracy*

Taylor, J.A., A.M.B. Lips, and J. Organ (2006), 'Freedom with Information: Electronic Government, Information Intensity and Challenges to Citizenship' in: R. Chapman and M. Hunt (eds.) , *Freedom of Information: perspectives on open government in a theoretical and practical context*, Aldershot, Ashgate, in press.

The LSE (2005), *The Identity Project. An Assessment of the UK Identity Cards Bill & its implications*, The LSE Identity Project Interim Report, March 2005

Torpey, J. (2000), *The Invention of the Passport: Surveillance, Citizenship and the State*, Cambridge University Press, Cambridge, UK.

UK Information Commissioner press release, 'Information Commissioner publishes concern on identity cards', 30 July 2004.

'UK Passport Service Biometrics Enrolment Trial Report' May 2005 - http://www.passport.gov.uk/downloads/UKPSBiometrics_Enrolment_Trial_Report.pdf

Westin, A.F. (2003), 'Social and Political Dimensions of Privacy', in: *Journal of Social Issues*, Vol.59, No.2, pp. 431-453.