Electronic Government: Towards New Forms of Authentication, Citizenship and Governance[1]

Miriam Lips (OII), John Taylor (Caledonian Business School & OII) & Joe Organ (OII)

1. Introduction

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. For a long time authentication procedures in government service provision were of course paper-based. The means of authentication, such as the passport, birth certificate or drivers licence, were used as an official proof of the individual holder's self-declared identity; the checking of that paper-based proof took place in face-to-face citizen-to-government relationships. With the arrival of digital technologies in our society, enabling the development of an 'e-government' service domain, it is clear that new forms of authentication are required for situations in which the digital citizen's identity must be checked as part of an assessment of service entitlement. Thus a citizen's assertion of identity is made digitally and, dependent on the service sought, measures are taken by government to authenticate that identity on-line. This process then allows for registration to the service arena, for an assessment of entitlement to the service and in some [as yet relatively few] cases for a transaction to be completed in this on-line environment. The process also allows for denial of access to service.

Against this backdrop, governments have been seeking new design possibilities for identity management, including authentication, to be used in higher level, including transactional, e-government service provision to citizens. The process of digital identification and authentication can, in principle, occur at any point on a continuum, from requiring 'fully revealed' personal data from the citizen at one end to a preference for pseudonimity or anonymity on the other; a process that does not necessarily require different security levels. The design options for the establishment of citizen identity and its authentication in e-government environments are numerous, therefore, and at present it remains far from clear where governments are settling. What is clear however is that new forms of identification and authentication processes in e-government are already suggesting fundamental redesign of service relationships with citizens compared to their face-to-face and paper-based counterparts.

In this paper we will argue that the introduction of identity management (IDM), including digital authentication, systems should not only been seen as requiring attention to *technical* design issues of the e-government service domain but as also requiring attention to wider and fundamental exploration and incorporation of *social* design issues that capture the changing relationships between government and citizen that these systems bring forward. In many cases the introduction of these new IDM systems comes together with much debate and fear about the surveillance of citizens and other privacy intrusions to be expected on a logical assessment of the technical characteristics of these new systems. From both government and citizen points of view it seems important therefore that design options reflect these concerns, incorporating as they do the respective political, managerial and democratic roles,

[1] This paper is grounded in empirical work derived from an ESRC-sponsored research project conducted by the authors and based at the Oxford Internet Institute (OII), entitled 'Personal Identification and Identity Management in New Modes of e-Government' (reference: RES-341-25-0028).

responsibilities and rights of all parties. The historical development of traditional IDM systems such as the passport lends further weight to this argument, showing as they do that, although their technical design features remain more or less the same through time, the political, managerial and democratic context and use of these systems is likely to shift markedly as social contexts and the perceived imperatives to which they give rise change.

2. IDM as a Technical Domain of Understanding

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).

The necessity for robust IDM in government service provision has become strongly recognised in the digital era both for security reasons and, more generally, to support the spread and successful uptake of e-Government (Hof, 2000; Davies, 2005, p.27; eEurope Action Plan 2005). We recognise too the multiple, digital relationships that the citizen has with government agencies, each supported by a form of IDM (Fishenden, 2005). For example, the citizen will often have 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. A consequence of this recognition is that integrated IDM solutions may increasingly be geared to creating a complete identity profile on the citizen (cf Prins & de Vries, 2003).

IDM issues in each of these service arenas and indeed from within a more strategic environment concerned with exploiting opportunities for integration, are largely and almost exclusively tackled from within a technical domain by experts with a dominant background in a technical discipline. Security and other related concepts like reliability, interoperability, single sign-on for users, and federated IDM can be observed as major topics and trends in current IDM discourse, for instance at conferences in this emerging domain. On this basis, varying IDM models are being explored for potential use by governments to create optimal IDM systems. The basis of these explorations appears limited however from a social scientific perspective. As social scientists it is hard to accommodate the view of some technical experts that human aspects are prohibiting optimal IDM systems and that “social engineering or other forms of manipulation”, such as in the case of identity theft, are needed to overcome these barriers to development (Fishenden, 2005). Equally, as social scientists, we observe organisations in digital environments asking customers to provide personal information which in many cases is excessive. In many cases of on-line transacting, for example, we find business firms as well as non-commercial organisations juxtaposing required data [indicated by an accompanying asterisk] and additional data that need not be supplied for the purposes of the specific transaction. Moreover, in many digital environments personal data is being collected from customers during e-service provision in digitally automated and therefore scarcely understood ways as for instance through the use of cookies, assigned IP addresses or automated observation of ‘click behaviour’. The digital basis of these different types of personal data promotes their easy collection, storage, updating and use.

The dominant information principle is identification of the citizen rather than the acceptance or encouragement of anonymity as the guiding principle. With anonymity as the guiding principle, the minimal collection of personal information by organisations is the norm. In the European FP6 project 'Privacy and Identity Management for Europe' (PRIME) technical solutions are being developed to meet this alternative principle of anonymity in various e-service relationships while, at the same time, offering optimal services provision to consumers. Offering personal data control to users rather than to service providing organisations and, at the same time, protecting the security of e-relationships through the use of encryption techniques, the Privacy Enhancing Technologies (PETs) being developed in PRIME will be usable in the near future in a range of applications in the fields, including e-government. PETS will enable a choice for users about the degree of anonymity they would like to have in service relationships, within the existent regulatory framework.[2] If these technologies become accepted in the European information society it may become clear that information management principles and practice will need to change accordingly. Paradoxically, one can argue that PETS are providing the prospect of continuity in the relationships of governments to citizens, many of which have been constructed historically on the principle that detailed IDM does not have to occur before service can be delivered and consumed as for example in national health care services. The following observations from interviewees in our current research illustrate the point:

"*For many years we have had a database holding personal information on our members, but we have never used it as management information. The fact that we now have a multifunctional smart card as a membership card does not change anything in this situation: it is just a card, which happens to provide a member with access to our services.*"

"*In our service provision we are dealing with patients, not customers. We do not need to know who they are; they can stay anonymous so far as we are concerned. We only need to know what the characteristics of their complaints are to deliver a good service*".

3. Information Management and IDM Innovations

It is clear that we still have design options in identity management, options with very different and fundamental implications for the collection, management and use of the personal information on citizens in their relationships with government. Alongside logical, systems building approaches, we take the view that empirical research must be conducted on the governmental and democratic implications of these options and that richer and widespread public debate should ensue so that there is wider awareness of the anticipated effects of new forms of personal information management in specific government contexts. Thus far we observe that a particular and partial debate is occurring though without the benefit of an empirical understanding of what is happening with flows of personal information between citizens and governments, and within government. The UK national ID card legislation[3] is a prime example of a strong debate occurring over the introduction of a new means of personal identification though one that has very little empirical basis to it. Moreover, critics have indicated the overemphasis in the public debate on the visible technical means 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,

[2] Governments will still have the possibility to obtain personal data of users if needed for a public interest purpose, such as for instance public safety.

[3] The proposed UK national identity card legislation is 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. 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.

2005, p.38; the UK House of Lords Constitution Select Committee[4]). Moreover some 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. 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.

This observation of overemphasis on the medium, together with lack of attention to the actual information flows surrounding that medium, seems to link to a more general point about the introduction of technical innovations through time. Together with the broader introduction of the open, decentralised Internet in our society various 'grand' ideas about resulting societal changes emerged [Brown and Duguid, 2000]. This new technology would bring citizen empowerment and perfect democracy, it would lead to paperless offices both physical and virtual, and it would reinforce powerful actors in becoming 'bigger brothers' than ever before. Interestingly, the emergence of new technologies in society in general seems to bring about oppositional ideas that turn out to be persistent through time. In many cases we can observe the strong impact of these ideas on societal debates surrounding the uptake of new ICTs, leading to situations in which, from their very first introduction, new ICTs are stuck in the middle of polarised normative debates based on the technological characteristics of the relevant ICT application – like in the case of the UK ID card legislation. Fed by one of the bigger visions such as big brother state, people seem to be convinced opponents from the very first introduction of plans to implement the new medium. According to Davies for instance the UK Government is rightfully dismissive of the conspiracy theorists who view technological change purely as a way of monitoring and disciplining citizens (Davies, 2005, p.2). However, scientists also seem often to take the technical characteristics as a starting point for societal effects, as with Michel Foucault's (1975) ideas about the panoptical state that is deemed consequential on technological opportunities, and David Lyon's ideas about the emerging surveillance state (1994; 200x), and Mark Poster, who claims that the quantitative advances in the technologies of surveillance result in a qualitative change in the microphysics of power. (Poster, 1990, p.93).

Both societal and scientific thinking about the introduction of new media appears to be strongly influenced by their technical characteristics. Put differently, technological determinism seems to be the dominant perspective through which assessments of the introduction of new technologies in society usually take place. Ciborra is one of the few authors who observes the dominance of a technical-scientific paradigm. Acknowledging the overly technical character of much thinking and writing about information systems in general he perceives current descriptions of the design, implementation, management, and use of ICTs in various organisations to be largely founded on notions of rationality, science, and method (Ciborra, 2002, p.1): *'Disciplines inspired by the paradigm of the Galileoan method such as ours* (ie information systems], *tend to disregard the fundamental role of the everyday life world of the agents, users, designers, managers, and the messiness and situatedness of their acting, while privileging the geometric worlds created by system methodologies. In such a way, one key element gets to be neglected: human existence, which represents the essential ingredient of what information is, of how the life world gets encountered, defined and described.' (Ciborra, 1998, p.9).* The example of the 'paperless office' vision shows us that, although when viewed logically and technically, we can see how we might be able to eliminate the use of paper, practise has turned out to be different so far. Similarly, identity

[4] The House of Lords Constitution Select Committee has suggested that the legislation should really have been titled the "National Identity Register Bill", rather than the "Identity Cards Bill" (Davies 2005).

management must not refer only to ID cards, or databases but a large infrastructure of personal information including authentication mechanisms, spanning public and private sectors and touching many aspects of modern life (Camp, 2003, p.7). Ciborra therefore suggests that we should move away from the scientific paradigm that he sees as predominant and move towards the exploration of new ICTs through a variety of conceptual lenses.

It is Ciborra's advice that we pursue further in this paper. The first empirical results of our research confirm the necessity of using other perspectives in addition to a technical one. Moreover the history of well-known, taken-for-granted authentication systems present in our society, such as the passport, shows us the importance of looking beyond the technology to find the richness of varying outcomes and implications surrounding the use of the passport through time.

4. Beyond the Technical Perspective – Insights from the history of the Passport.

The passport has become one of the most commonly used authentication systems in societies worldwide. Through time the process of personal identification related to the use of the passport has been largely constant. The passport holder shows his or her passport to the person officially recognised to check and verify the document carrier is the person shown in the information, including photograph, included in the document. How has this embeddedness of the passport in social practice come about? Why did governments start to use passports and in what ways have they come to be used?

In a historical journey through Europe throughout the 20th Century, the Dutch author Geert Mak vividly explains how Western-European bureaucracies have introduced the passport as an official public means for establishing the national identity of a citizen crossing national borders and how quickly this authentication process became common to all European citizens in the 20th Century. For instance the Austrian author Stefan Zweig admits to his readers in 1941: '*I still enjoy the stupefaction of young people when I tell them that, before 1915, I travelled to India and the United States without having a passport or even without ever having seen a passport*' (Stefan Zweig, 1941, in: G. Mak, 2004, p.42). Equally, a tourist guide published around the turn of the 20th Century did not consider a passport as a necessity for travelling citizens to have: "*however, often they are quite handy to establish the traveller's identity for getting access to museums on days when they are not open for the general public*" (Ibid).

With his historical analysis of the invention and evolution of passports and their uses in Europe and the United States since the French Revolution, Torpey (2000) shows the *révolution identificatoire* (following Noiriel) that has taken place in the public domain of nation states. Where the power to regulate citizens' movements used to belong to private institutions like the church, or market institutions at that time 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 passports or similar official national identification papers nation states have established the exclusive right to authorize 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 (ie under the old regime in France) were required to be in possession of a passport authorizing 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).

Passports took on a different use and meaning during a moment of crisis, the period of the French Revolution. As a consequence of the fact that a citizen's personal information derived from the municipal registration became part of the citizen's passport[5], the administrative bodies could check and verify the level of honesty of the traveller on the basis of his passport and, with that, watch the more dubious or foreign people who would need their particular attention (Torpey, 2000, p.34). Put differently, distinctions were now started to being made between true 'citizens' and 'non-citizens', also to look for traitors who would obviously belong to the alien, non-citizen category. Consequently passport controls to *enter* countries or districts became more extensive. In 1792, the French government 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 (Torpey, 2000, p.43-44).

Somewhat further in time, in the early 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[6] intermediairies 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.

Based on the same techniques and processes of identification and authentication through time, all these different national motives to require passport control finally came together in a situation in which international movements of people, particularly after the second World War, did become enormous. This then led to a global authentication system within which passports issued by the various national governments were recognised as official proof of a citizen's personal identity.

The history of the use of passports and their changing meaning in society shows us how important it is to look beyond their technical characteristics and, thereby, to make use of alternative perspectives in exploring the introduction and functioning of new identification 'technologies'. It also makes us aware of the importance to perceive the use of IDM systems

[5] The municipal registration contained personal information such as name, age, place of birth, previous domicile, occupation, and means of subsistence. Those citizens lacking the last mentioned category needed to indicate the name of a local resident who was prepared to vouch for them; people without either means of subsistence or a sponsor were to be registered as *gens sans aveu*; those who failed to indicate a previous domicile as *gens suspects*; and those shown to have made false declarations were to be identified as *gens malintentionnés*.

[6] The 1813 passport law in Prussia.

in an evolutionary way and for instance to look for punctuated equilibria (Baumgartner & Jones, 2003) in the historical evolution of ICTs, eg the periods of crisis during the history of the passport, as important moments where changes often may happen in the use of these technologies.

This discussion leads us to wonder to what extent these observations might be true for the digital age. Again, we present an empirical observation from our work as a further illustration:

"*We first needed to have the e-government application in which the IDM system is embedded, accepted by our politicians. Therefore it was a necessity that the application would comply with privacy and other government regulations. However, now that the application has been politically accepted and we have it up and running, we can do other things with it. Now we can look for ways to serve our customers better and develop longer lasting relationships with them, Customer Relationship Management that is. This may mean that we will use our database to provide regular customers with a discount or proactively provide them with information relevant to customers*"

What we have shown to this point in the development of our arguments about contemporary approaches in government to the 'problem' of identification and authentication is that the historical, analogue world has much to teach us both in terms of the ways in which scholars might best address their subject and about the ebbs and flows in the substantive, empirical world within which identity both has been and is being managed by government. Whilst there is a need to develop the technical field of IDM, there is a vital and urgent need to understand the social and political worlds within which these systems will be used. The lenses through which light flows on these systems need to be various if the nuanced understanding of them is to be forthcoming. The history of the passport as an identity management system in the analogue world clearly illustrates the power of social scientific and historical approaches to understanding IDM systems and to designing them in ways that are fit for purpose by modern government.

5. Different perspectives on on-line e-authentication policy designs

As we explained earlier, governments are beginning to think about the development of e-authentication within the context of their identity management solutions for e-government service provision. For the purpose of this paper we looked at two of these developing e-authentication policy designs: in the UK, the Government Gateway Project; and in The Netherlands, the DigiD initiative. More detailed descriptions of these two policy designs can be found in appendices A and B of this paper, respectively.

In addition to the predominant technical perspective, we use social scientific perspectives to examine these e-authentication case descriptions so as to illustrate how differently we can perceive them. This in turn leads us towards important differences in the implications for governments and citizens that emerge from these developments. To help us in so-doing we make use of perspectives derived in part from the classical lenses of an influential scholar in the field of public administration, Graham T. Allison. In his well-known book 'Essence of Decision: Explaining the Cuban Missile Crisis' (1971) he uses the Cuban Missile Crisis as a case study to illustrate how governmental decision making can be analysed and explained differently by using varying conceptual models. Besides the dominant conceptual model in public administration at that time, the so-called 'Rational Actor Model', which assumes that a decision making actor considers all options and takes rational actions to maximise utility, Allison constructs the ‘Organisational Process Model’ revealing the way in which organisational and bureaucratic factors place limits on government actions and often dictate the final outcome; and the ‘Governmental Politics Model’ showing the preferences and perceptions of specific actors involved in the Cuban missile crisis and the negotiation games leading to certain actions.

Similar to Allison we would like to look at these two e-authentication policy design models for on-line e-government using different lenses. We construct our lenses on the basis of a translation of not only Allison’s models but also his approach of adding alternative ways of seeing to the dominant perspective of that time. Interestingly, through a connection with the work of Ciborra, we may observe that Allison’s Rational Actor Model comes close to the technical scientific perspective on our e-authentication policy cases: similar notions of rationality, science, and method seem to be applicable to both Allison’s Rational Actor Model and the technical scientific perspective. We will take the technical perspective as our first lens, therefore. The second lens we use is also similar to Allison’s second perspective of the Organisational Process Model. Here we look at the two e-authentication policy designs from an Internal Government point of view. And finally in accordance with Allison’s third lens of the Governmental Politics Model we will use a more externally focused, actor–network perspective, a lens we refer to as External Governance and Citizenship.

What then can we see through these respective lenses when comparing the two e-authentication policy models? We will show that by looking through different lenses, and comparing these policy designs, varying details emerge with different implications for government, citizenship and citizen-government relationships.

- *Technical Lens*

Looking at and comparing the UK Government Gateway project and the Dutch DigiD-initiative from a technical point of view it is remarkable to see how similar these two national e-authentication policy designs are. Both policy initiatives entail a central Internet-based authentication facility through which citizens and businesses can access e-government services in these respective countries. Being ‘middleware’ solutions, both provide intermediary e-authentication services between citizens and government. Citizens can, in principle, access all e-government services from this single point of electronic access on the basis of only one user ID (or username in the Netherlands) and password, after having registered with the authentication service provider. In addition in the UK, the user will then need to provide ‘known facts’ for individual services that are being enrolled. Moreover enrolled citizens to Gateway services can make use of credit or debit cards under a secure payments function scheme.

At the government side universal security and authentication standards can be offered for clusters of e-government services that are acknowledged to have similar risk profiles. In doing so, different authentication levels have been established, each having its own security features and related authentication means; the Gateway project applies four different levels of authentication (0 - low to 3 – high), whereas DigiD supports three varying levels of trustworthiness (basic to high). In the UK for higher levels of authentication a user needs to be digitally certificated by a trusted third party supplier acknowledged under the ‘tScheme’; in the Netherlands, DigiD, not the user conducts verification of the authentication process with an authentication solution provider and feeds back the validation results to the individual e-government service providing organisation.

- Internal Government Lens

If we look comparatively at the Gateway and DigiD policy descriptions from an internal government point of view we observe more differences between the two policy designs than became visible through the technical lens. For instance the government organisation responsible for the development of the Gateway project is located in the heart of central government, the e-Government Unit of the Cabinet Office. Its policy aim is to develop a single channel for electronic transactions between citizen and UK central government. Also, in the past, responsibility for e-authentication and identity management in e-government service provision was lodged at the central level of UK government. The DigiD-initiative however was originally developed by a group of implementation agencies later replacing the existing Dutch national government's PKI-based e-authentication system. At present the DigiD-initiative is a joint policy responsibility of the Dutch Ministry of the Interior together with Ministers responsible for policy sectors concerned, implementation agencies and other governments. Operational responsibility for DigiD is with the Dutch national ICT implementation agency (ICTU) and the Dutch Taxation Office. Policy aim is to have only one authentication facility for e-government service provision in the Netherlands.

E-government services accessible through the Gateway are currently provided by eleven central government organisations and ten local government authorities. Authenticated services are offered directly through the Gateway website or programmatically via the individual government's website, putting the Gateway authentication facility in a more or less visible position. Moreover, although the Gateway holds 'known facts' for various e-government services, the relevant government organisation retains ownership and responsibility for the maintenance of these known facts.

In the Netherlands on the other hand many more local governments (17) and two Dutch government implementation agencies at the national administrative level are providing e-government services supported by the DigiD e-authentication facility. After having registered with DigiD citizens only need to reconfirm their DigiD password to be able to get direct, authenticated, access to e-government services. As a result of specific legislation at the Dutch national level it is allowed to use DigiD in e-government service provision where the unique taxation number or so-called A-number is required. The current development of DigiD only focuses on the Basic and Medium Levels of authentication whereas the third High Level of authentication (PKI) may be further developed in combination with the implementation of the eNIK, the foreseen electronic Dutch identity card. Although relatively expensive the use of the eNIK for this High Level of Authentication though would fit with the preference of the Dutch Parliament to have only one electronic identity card for all government services requiring authentication.

A similarity in both countries is that risk assessment has taken place to establish appropriate levels of authentication for clusters of e-government services. Following from this exercise has been the development of specific guidance for government organisations to assess the appropriate authentication level for a specific e-government service.

- External Governance and Citizenship Lens

When we apply a broader social scientific perspective to these two policy design descriptions, a lens of external governance and citizenship, we may observe even more distinct situations under development in both countries.

For instance if we look at the government organisations involved in the Gateway project and DigiD initiative respectively, and the relationships they have with their customers, we can observe differences in citizen – government relationship types involved in authenticated e-government service provision in both countries. Citizens for instance can have a relationship with a government organisation as ‘voluntary customer’, as an ‘obliged customer’, as a subject of the state and as a democratic participant. Participating UK central government departments like the Revenue and Customs department, the Department for Environment, Food and Rural Affairs, Department for Work and Pensions, Department of Trade and Industry, the Home Office, the UK Passport Service, and the Department for Constitutional Affairs have relationships with citizens which can be characterised differently, therefore, and especially when compared to the majority of Dutch government organisations involved in DigiD, namely the local governments, and the two other participating government agencies, the Taxation Office and the Social Insurance Bank. The UK Government Gateway project has a more limited scope for covering citizen-government relationships now that an alternative e-authentication facility has emerged that is tailored more towards e-government service provision by local authorities.

Moreover, varying types and sorts of the citizen’s personal information constitute the basis for e-government service provision within these relationships; in the UK Gateway project the ‘known facts’ which the citizen needs to provide to get access to e-government services even vary from service to service. The Gateway system then derives an ‘identifier’ from the validated known facts, to distinguish the citizen uniquely for that particular service. Further differences can be observed for the citizen’s enrolment to other services after having registered. Whereas the UK citizen needs to register for every individual Gateway service and, with that, supply a new set of known facts to the service providing organisation, the Dutch citizen only needs to register once for DigiD by providing his or her unique taxation number (a unique number used in the provision of a large variety of public services in the Netherlands nowadays), date of birth, postal code, and home number and by choosing a username and password. On the basis of these personal data the citizen’s home address can be constructed and verified in accordance with data known by a national register, the Dutch Municipal Data Base (GBA).

Also, citizens in each country are required to supply different types of personal information for each of the authentication levels created within the two policy settings. In doing so, different trusted third party providers are involved at varied authentication levels to validate the citizen’s trustworthiness. Based on the established level of trustworthiness and therefore appropriate level of authentication for a specific service, the Dutch citizen can determine what authentication means available at that level he or she would like to use. In the UK, recent internal policy documents that address government IDM in general and authentication in particular envisage the assignment of a “trust profile” to citizens who go on-line through the Gateway. Such trust profiles will be assigned in more or less refined ways [yet to be decided], though to include ‘high’, ‘medium’ and ‘low’ trust designations as a minimum. These trust profiles will be an outcome of third party authentication through the t-scheme where it is envisaged that Credit Reference Agency data will be the determinant of the level of assigned trust, in the first instance. The trust profile will be built up through time following successive entries through the Gateway and the authentication process.

Finally, differences can be observed in the identification of critical authentication and other identity management issues in both countries. For the Gateway project the UK government presented the following critical issues: the release of personal or commercially sensitive information against reliably verified authority only; service provision only to those entitled to receive it; clear communication to clients of the criteria for access to particular services; and, when it is under the government's control, the protection of clients against misuse of their authority. The Dutch government on the other hand presents a somewhat different interest with regard to citizen – government relationships and the role of these new forms of authentication in these relationships: citizens need to be certain that their data will only get to the place where these data belong, and also that one person cannot take the identity of somebody else; citizens logically would desire to be able to obtain easy, convenient access to whatever government organisation; citizens would desire from a modern government to re-use the information it already has; the government from a maintenance perspective would want to have unequivocal data of the citizen; and the government wants to check the identity of citizens in a safe and easy way.

6. Further analysis: implications for citizenship and governance

Looking through these lenses shows us that beyond the technical designs of newly available forms of authentication and identity management 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* standardisation of these new authentication and identity management systems for e-government service provision may appear to be an obvious development, other *social* factors of importance to the application and deployment of these systems seem to point in an opposite direction. In each of these countries we therefore may acknowledge the presence of similar technical e-authentication policy designs but with different implications for further development of the e-government service domain in terms of governance, citizen – government relationships and citizenship.

What the views through these respective lenses especially reveal to us is the influence of these new forms of authentication and identity management on the governance of citizen – government relationships. As a result of these authentication measures the nature of citizenship, which can be considered as a function of citizen –government relationships, in these two countries is changing. Similarly to Torpey's analysis of the history of the passport we may observe that borders between customers and non-customers of government organisations, 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 offer the same authentication forms the possibility for government to let people access its virtual territories, but also to keep people out of them. Analogously to the Prussian era where intermediairies 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, such as banks and credit reference agencies, to help government to check people upon their trustworthiness.

With these new digital forms of authentication and identity management we seem to have arrived into a new *révolution identificatoire* in the public domain, where a law of informational identity may soon replace the existing models of citizenship attribution in the analogue world, *ius soli* and *ius sanguinis*. We are 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 is still 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. Janus, the Roman God of Portals [how apposite in a paper that in part looks at government use of the Internet] faced simultaneously in two directions. So, Janus-like, we can see modern government facing towards ‘enlarging’ citizenship through offering new and enhanced experience of its services, on the one hand, whilst at the same time facing towards the security of the State, with its potential for ‘reducing’ the scope of citizenship through new restrictions on the individual’s private sphere, on the other [Taylor, Lips & Organ, 2005].

References

Allison, G. T., *Essence of Decision: Explaining the Cuban Missile Crisis*, 1971, Longman.

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

Brown, J.S. & P. Duguid, *The Social Life of Information*, 2000, Harvard Business School Press, Cambridge.

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

Camp, L.J., *Identity in Digital Government*, 2003, A Research Report of the Digital Government Civic ScenarioWorkshop, Kennedy School of Government, Harvard University, Cambridge, available at: http://www.ljean.com/files/identity.pdf

Ciborra, C.U., 'Crisis and foundations: an inquiry into the nature and limits of models and methods in the information systems discipline.'. in: *Journal of Strategic Information Systems*, 1998, vol. 7, pp.5-16

Ciborra, C.U., *The labyrinths of Information: Challenging the Wisdom of Systems*, 2002, Oxford University Press, Oxford / New York

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

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

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

Foucault, M., *Discipline and Punish: The Birth of the Prison*, 1977, New York, Pantheon.

Hof, S., 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, 2002, Springer-Verlag Berlin Heidelberg

Lyon, D., *The Electronic Eye: The Rise of the Surveillance Society*, 1994, University of Minnesota Press, Minneapolis

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

Mak, G., *In Europa. Reizen door de twintigste eeuw*, 2004, Atlas, Amsterdam/Antwerpen

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

Taylor, J.A., A.M.B. Lips & J. Organ, *Freedom with Information: Electronic Government, Information Intensity and Challenges to Citizenship*, paper presented at PAC Workshop on Freedom of Information, University of Durham, 4th-6th April, 2005

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

Wilson, T.D, Philosophical foundations and research relevance: issues for information research. A paper delivered at *CoLIS4 - Fourth International Conference on Conceptions of Library and Information Science: Emerging Frameworks and Method*, University of Washington, Seattle, USA, July 21 to 25, 2002

Appendix A: The UK Central Government's Gateway initiative

Policy context

The context within which the Government Gateway was developed was set in the UK central government's *Modernising Government* white paper, where a corporate ICT strategy was announced with the objective of achieving joined up working between different parts of government and providing new, efficient and convenient ways for citizens and businesses to communicate with government and to receive services (Cabinet Office,1999, p.45). This vision was taken forward by the Office of the e-Envoy[7] within the Cabinet Office, and was built around a holistic target of having 100% of government services available online by 2005. To achieve this target and attain joined up electronic service delivery, the Government Gateway project was developed to offer a single channel for electronic transactions between citizen and UK central government.

Following from the wider e-government strategy, the objectives of the Government Gateway can be described as follows (Cabinet Office, 1999, p.46; OeE, 2000, p.46):

- obviating the need for citizens to repeat the same information to different service providers using commercial open standards where possible
- making it easier and more efficient for citizens and businesses to use online public services
- provide universal security and authentication standards for online government transactions
- join up existing IT systems in departments to a single point of access (*ibid.*)

The authentication of users has been seen as crucial to unlocking the potential of online service delivery by joined up working through the Gateway. A policy document was published by the Office of the e-Envoy in 2002, which identified critical authentication and other identity management issues. The authentication policy document recognises that government must:

> - release personal or commercially sensitive information only against reliably verified authority
> - provide services and benefits only to those entitled to receive them
> - communicate clearly to clients the criteria for access to particular services
> - when it is under the government's control, protect clients against misuse of their authority. (OeE, 2002a, p.5).

The Gateway was officially launched in January 2001, and was located within the Office of the e-Envoy at the Cabinet Office. It was originally run as a pilot involving the Inland Revenue, Customs and Excise and the Department for Environment, Food and Rural Affairs (DEFRA), and included five services, only one of which was aimed at citizens rather than business, the electronic submission of self-assessment forms (NAO,2002a, p.30; NAO, 2002b, p.53). The Gateway was upgraded in July 2002 as it moved towards a fully-fledged system, to offer the service to other local government and central government organisations as well. Further upgrades occurred in later years as the Office of the e-Envoy looked for increasing departmental participants. Logistically, the Gateway is now being taken forward by

[7] The Office of the e-Envoy was closed in 2004 and replaced by the e-Government Unit within the Cabinet Office.

the e-Delivery Team within the Cabinet Office's recently created e-Government Unit. This team was created in June 2001 when the Government Gateway and UK Online teams merged into a single unit (eDT,2005c,p23).

As of summer 2005, the Revenue and Customs department, the Department for Environment, Food and Rural Affairs, Department for Work and Pensions, Department of Trade and Industry, the Home Office, the UK Passport Service, Department for Constitutional Affairs and four other central government organisations offer online services through the Gateway, as well as ten local government authorities (eDT, 2005b, p.4). The Revenue and Customs department operates 18 different services, ranging from several employer VAT transactions to the popular self-assessment online service. The Department for Environment, Food and Rural Affairs offer six services, aimed largely at agricultural businesses. The Department of Work and Pensions operates six services including claiming child benefit online, claiming for a Carer's Allowance and receiving real time Pension Forecasts. At the local government level council tax payments, payments of parking fines and other financial transactions are the most common services offered. Most of enrolments in the five years of the Gateway's existence have come through services offered by the former Inland Revenue department; over 6 million of the total of 6.3 million enrolments– many of which are business enrolments (eDT, 2005b, p.20).

An alternative to the Gateway portal has emerged that is tailored more towards local authorities, known as Government Connect. Whilst using portions of the Gateway architecture, this new service hopes to provide a toolkit with which local government councils can authenticate citizens to transact with different local government departments and potentially with other government organisations (ODPM, 2005, p.22).

Functioning of the Government Gateway

The following key features of the Gateway can be recognised (eDT,2005d, p.2):

- **Authentication and Authorisation** – to ensure that citizens are who they claim to be, and to determine rights of access to services
- **Single-Credentials** – citizens use a single user ID and password (or digital certificate) for use of all gateway routed services
- **Messaging –** electronic delivery of documents between citizens and government and between government services
- **Security –** offers high levels of security for transactions

Services are offered 'directly', i.e. through the Government Gateway website, or 'programmatically' via the websites of government organisations. The e-Delivery Team prefers programmatic access, as it reflects the favoured middleware role of the Gateway. Citizens would normally connect to the Gateway across the internet, but may not be aware that they are using the Government Gateway programmatically through a departmental website. The participating government organisations are required to install a Departmental Interface Service (DIS) within their own ICT systems to achieve compatibility with the Gateway. The procurement and use of this DIS system is the responsibility of the departments rather than the e-Delivery Team (eDT,2005d, p.2).

To use any Gateway service, a citizen would need to first register; for many Gateway services this entails providing a full name and email address and choosing an alphanumeric password (eDT,2005d, p.12). The user will then provide 'known facts' for the individual services that are being enrolled for. These 'known facts' vary from service to service within the Gateway. For instance for the most popular service, the Revenue Department's Self Assessment Service, the known facts are the Unique Tax Number and National Insurance Number or postcode, data already held on citizens within the department. Thus, when a citizen enrols of this service online, he or she will be required to enter these known facts, and they will be checked against existing data. The Gateway system then derives an 'identifier' from the validated Known Facts, to uniquely distinguish the citizen. The e-Delivery Team indicates that it is this derived identifier, rather than the original Known Facts, that are used to authenticate the citizen. The citizen who is using the service is not aware of this internal identifier used by the Gateway, only of his or her user name and password. Although the Gateway holds known facts information, the relevant government organisation retains ownership and responsibility of maintenance for them (*ibid.*,p2).

To be able to make use of services provided through the Gateway the citizen is given a 12 digit alphanumeric user name which can be used with a chosen password across all services offered. However, before most accounts can be activated, the e-Delivery Team first sends a PIN by post to the user's physical address, which is accompanied by a separate letter to confirm the user's ID. The correct postal address is not inputted by the citizen during enrolment; instead the Gateway system requests the address from the government organisation which is being enrolled on, via the DIS 'box' installed for such communication (eDT,2005g, p2-3). Name and Address details are printed along with an activation pin and then the address is deleted from the Gateway system once it has been used (*ibid*.,p3). Thus, this system is based on existing data held in government databases, and serves as additional verification of a citizen's identity at the point of enrolment. The activation PIN is another 12 digit alphanumeric password, which has to be used as a one off to inaugurate use of a specific service through the Gateway portal; the user has 28 days before this activation PIN expires. So far however, the Gateway has not succeeded in enabling citizens to automatically enrol on other Gateway routed services following successful registration with one. If other services are required, then a new set of Known Facts are collected and checked, and a new activation PIN has to be sent out and used in most cases.

In the process of enrolment the government organisations offering the service through the Gateway are required to set appropriate levels of authentication. To establish authentication levels the UK government prepared a guide known as the 'Registration and Authentication Framework', which has been based on risks carried by fraudulent use of services. The Registration and Authentication Framework provides four authentication levels, which determine the type of credential needed to use a service:

- **Level 0 –** no credential or authentication needed. Inherently, the Gateway is unlikely to be used to any great degree for services of this nature.
- **Level 1 –** user ID and password required to protect from minor inconvenience or loss to any party. The majority of citizen to government services will use this level of authentication, in contrast to business to government services.
- **Level 2 –** digital certificate required to protect from significant inconvenience or loss to any party. Users must prove identity to a trusted third party provider to obtain a certificate. In some cases however, user ID and password may be sufficient for Level 2.

•**Level 3 –** digital certificate plus biometric authentication is likely to be required to protect against substantial financial loss or risk to personal welfare and safety to any party. The Government Gateway does not currently support level 3 authentication.
(adapted from OeE,2002;eDT,2005g, p.8).

At present a channel for external, non-government organisations to be directly involved in the Government Gateway occurs in the cases where Digital Certificates are required as credentials for authentication rather than user names and passwords. Uses of Digital Certificates are usually required for business rather than citizen uses of the Gateway: for instance, certificates are used for Corporation and Employer Tax, export services, agricultural payments, where authentication levels are deemed to be higher. Digital Certificates are small pieces of encrypted software embedded in a smart card or hard drive of a PC (eDT,2005g,p8). Suppliers of digital certificates must have tScheme approval to be recognised by the government as a trusted supplier. The tScheme is a non-profit organisation owned by members which include Vodaphone, the Royal Mail, the Royal Bank of Scotland, Microsoft, IBM, Experian, Equifax, BT, Barclays Bank and other corporate entities (tScheme,2004). The tScheme was established at the time of the UK Electronic Communications bill in 2000 and enables industry to self-regulate in the development and use of secure electronic transactions (*ibid.*). In terms of Gateway services, at present, third party organisations are only involved in identity management processes as providers of such certificates.

For instance in the case of the Equifax system, to obtain a Digital Certificate, a user must enter an agreement with the provider and then submit basic and/or business details and pay for the certificate (typically £25). The user then has to engage in an interactive query, which consists of a questionnaire with answers that only the user should know, based on data held by the credit reference database held at Equifax. If this stage is passed, a certificate is issued and the user is invited to import the information onto a PC (Equifax,2005). The certificate is then used as an automatic form of authentication for Government Gateway services.

The Government Gateway also has a secure payments function, which allows citizens already enrolled to use credit or debit cards with Gateway services (eDT,2005d, p.52). The Passport Agency has been one of the government organisations to use this service for the online payment for new or replacement passports. As of April 2005, 116,000 out of the Gateway-wide total of 129,000 payments had been received for the Passport service (eDT,2000b, p24).

Recent internal policy documents that address government IDM in general and authentication in particular envisage the assignment of a “trust profile” to citizens who go on-line through the Gateway. Such trust profiles will be assigned in more or less refined ways [yet to be decided], though to include ‘high’, ‘medium’ and ‘low’ trust designations as a minimum. These trust profiles will be an outcome of third party authentication through the t-scheme where it is envisaged that Credit Reference Agency data will be the determinant of the level of assigned trust, in the first instance. The trust profile will be built up through time following successive entries through the Gateway and the authentication process.

Appendix B: The Dutch DigiD-initiative

Policy context

As stated in its ICT policy programme ‘Different Government’ the Dutch government wishes to take advantage of the opportunities offered by ICTs to improve the standard of service provision to the business community and the general public. To do so the following main points have been indicated:

- citizens and businesses need to provide certain personal data to the government only once;
- an electronic system will be established through which citizens and companies can authenticate themselves towards the government;
- both internally and externally, the government will use open standards for her communication;
- it is the objective of the Dutch Government to have 65% of government services provided via the Internet by 2007.

With that, it is the policy ambition of the Dutch government that transactions can be handled electronically instead of paper-based or at a physical counter. In the development of electronic handling of service transactions the Dutch government uses the following arguments:

- citizens and businesses need to be certain that their data will only get to the place where these data belong; also that one person cannot take the identity of somebody else;
- citizens and businesses logically would desire to be able to get access to whatever government organisation (and therefore do not need to remember a separate pin for each government service)
- citizens and businesses would desire from a modern government to re-use the information it already has (onetime data supply)
- the government from a maintenance perspective would want to have unequivocal data of the citizen or company.

For further development of e-government in the Netherlands ICT-facilities would need to be established in the following seven domains. Together these domains constitute a public electronic information infrastructure:

1. electronic access to government
2. electronic authentication
3. unified numbers for persons and companies
4. basic registries
5. electronic identification means (smartcards)
6. electronic information exchange
7. fast connections between government organisations

For development of the electronic authentication domain the Dutch government has expressed its desire to check the identity of citizens and businesses in a safe and easy way. Citizens and businesses in their turn need to rely upon the fact that their identities are not abused by others. Personal data need to be well protected therefore. To do business electronically with the government the Dutch government aims to have only one authentication facility (entrance code or card). The so-called DigiD-initiative (“Digital iDentity”) could be used for that purpose.[8]

In 2003, a group of six big Dutch national government agencies (the so-called ‘manifest group’), among them the Dutch Taxation Office, The Centre for Work and Income, The Council for Care Insurance, IB-Group, the Social Insurance Bank (SVB) and the Agency for Employees’ insurances (UWV) started with the development of a National Authentication Facility (NAV). At the same time the Dutch Ministry of the Interior commissioned the Dutch Foundation ICT Implementation Organisation (ICTU) to develop a comparable system. ICTU’s system offers both possibilities of electronic identification and electronic signature. In 2004, the NAV was adopted by the Dutch Ministry of the Interior as part of its own authentication initiave called Government Access Facility (OTV). Together with the Dutch Ministry of Economic Affairs both groups jointly continued their efforts to establish a Dutch Authentication Facility under the DigiD-initiative. The first version of DigiD was launched in October 2004. Since 2005 17 local governments have joined the DigiD initiative together with two Dutch government implementation agencies. The participating local governments usually offer their inhabitants the possibility for online application of summaries from the population register and licences. The Social Insurance Bank offers online application for child benefit or online changing of retirement data.

At present, the Dutch Ministry of the Interior together with Ministers responsible for policy sectors concerned, implementation agencies and other governments, are responsible for the implementation of e-authentication in the Netherlands. At this moment ICTU and the Dutch Taxation Office jointly supply DigiD to the general public. As a result of legislation at the national level (*Tijdelijk besluit nummergebruik OTV*) it is allowed to use DigiD in service provision where the unique taxation number or so-called A-number is required.

Functioning of the Dutch authentication system

The DigiD-initiative (“Digital iDentity”) is set up by the Dutch government as a central Internet-based facility to establish authentication for citizens and companies to public services offered by Dutch national and local governments. Aim of this initiative is to achieve uniformity in authentication for citizens and governments, for instance by means of creating one password for all Internet-based e-government service provision. Since 1st January 2005 citizens can consume electronic public services on the basis of only one username and password.

By means of ensuring that a user’s identity is adequately verified, DigiD functions as an intermediary to government, an Authentication Service Provider (ASP). The responsibility of the ASP is to validate the identity of the user and to feed back the validation results to the process owner or service providing organisation. On behalf of the process owner who established a specific authentication level the ASP conducts verification of the authentication process with an authentication solution provider, such as a bank, a smartcard owner or a certificate provider.

An ASP can make use of various types of authentication means. In the near future the Dutch government foresees that DigiD will function as an authentication portal for services provided

[8] Until September 2004 this initiative was actually called *Government Access Provision* (OTV).

by various government organisations and, with that, will prevent that every government organisation needs to develop, manage and maintain its own verification system.

DigiD supports different levels of authentication. A distinction has been made to three different levels of trustworthiness, namely Basic, Medium and High. These levels correspond with the security features and the migration of risks that can be achieved by authentication means available at that particular authentication level:

- Basic Level: combination of username or identification number and password;
- Medium Level: software certificates or methods used for Internet banking[9];
- High Level: PKI-standard; smartcard or electronic signature (as described in the Dutch Law on Electronic Signatures)

To support decision making on the appropriate means for authentication DigiD developed an Authentication Wizard. This tool incorporates a risk assessment and assists the process owner within a government organisation that wants to implement authentication for a certain service. Based on the established level of trustworthiness and therefore appropriate level of authentication for a specific service, the user can determine what authentication means available at that level he or she would like to make use of.

The current development of DigiD focuses on the Basic and Medium Levels of authentication. The third level of authentication, Public Key Infrastructure (PKI), may be further developed in combination with the implementation of the eNIK, the foreseen electronic Dutch identity card which contains an electronic signature. The implementation of this highest level of authentication in the citizen domain is relatively expensive however as a smartcard, for instance the eNIK, will be needed as its carrier. Moreover, the use of the eNIK for this High Level of Authentication would fit with the preference of the Dutch Parliament to have only one electronic identity card for all government services requiring authentication.

The DigiD-initiative will have two releases. The first release is focused on the citizen. DigiD issues a username and password to citizens, which will be a suitable security level for most electronic services in the Netherlands. With their DigiD account citizens are able to log in on web services supplied by the Dutch government.

Citizens only need to register once to be able to use DigiD. To register a citizen needs to go to the website of the government organisation participating in DigiD and click on a function to apply for DigiD. A screen opens automatically with a form where the citizen can fill in personal information such as his unique taxation number ("sofi"-number), date of birth, postal code, and home number. Additionally the citizen chooses a username with password. DigiD sends a personal activation code by regular mail to the home address as known by the Dutch Municipal Data Base (GBA). By filling in the code together with the username on the special screen at the participating government's website or through www.DigiD.nl the citizen's registration will be activated. The citizen again needs to reconfirm his password after which it can make use of an increasing number of electronic government services. For each service accessible through DigiD, after verification has taken place the government agency concerned can provide the requested service to the user.

[9] Under the condition that all banks in the Netherlands can participate.

For example, a citizen with a DigiD account may want to apply for a licence at the electronic service counter of his local government. He or she goes to the local government's website and clicks on the function of electronic licence application. A DigiD screen appears at which the citizen needs to fill in its username and password. The moment a citizen has access to his personal data known by DigiD, DigiD sends a cookie to the user. This cookie is removed automatically when the user shuts off his browser. After verification of these personal data by DigiD the citizen is able to submit his licence application electronically.

Since July 2004 the City of Enschede is using DigiD in a pilot project. Implementation of DigiD has been planned for the intake modules of the Dutch Centres for Work and Income (fall 2004), online tax application for citizens (from 2006 on) and for various services of the Social Insurance Bank (start 2005).

Scheduled for 2005, the second release of DigiD will be focused on companies. This second release will meet the security requirements of the Basic and Medium Levels of authentication. Application is planned for various Agriculture, Environment and Food Registrations (start 2005). From mid 2005 DigiD will be used as authentication means for the so-called Government Access Portal (*OTP*), a portal at which communication between businesses and government takes place. Moreover research will be conducted to further explore the potential use of DigiD for online tax application by entrepreneurs.

In the future DigiD will also provide access to government services via other means of authentication, such as challenge-response tokens, sms-authentication and PKI certificates.