IDENTITY MANAGEMENT IN INFORMATION AGE GOVERNMENT
EXPLORING CONCEPTS, DEFINITIONS, APPROACHES AND SOLUTIONS

June 2008

Miriam Lips with assistance of Chiky Pang
Victoria University of Wellington

1 Introduction

Governments throughout the world are introducing digital Identity Management (IDM) systems into their E-Government service relationships with citizens. These new IDM systems are being managed and used in addition to, and increasingly to replace, traditional forms of IDM in citizen – government relationships. As government agencies are moving into the 'transaction stage' of E-Government, it becomes clear that IDM more and more belongs to the core of national and international E-Government policy agendas (e.g. SSC, 2006; EU Ministerial E-Government Declaration 2005).

With that, new questions arise as to how core IDM concepts like 'identity', 'identification', and 'identity management' can be redefined for their deployment in emerging E-Government environments. At the same time however, the continuing use of traditional paper-based and face-to-face public service arrangements and, with that, the use of traditional IDM means, requires not only a redefinition of these concepts for new digitised public service environments, but also a reconsideration of the broader IDM concept for an emerging situation in public service provision of 'converged IDM': a situation in which traditional IDM and new digital IDM are being used, managed and governed by government in separated, integrated and shared ways.

While a proper definition of IDM seems to be essential for transactional government, activities in both industry and academia indicate that we are still on a discovery tour of how to reconceptualise and design ways in which we can be, or should be, managing our identity. Simultaneously, various governments around the world have started their own journey in reconceptualising, designing and introducing new e-authentication solutions in E-Government relationships.

This review of state of the art scholarly thinking and writing in the area of IDM in government is aimed to help the New Zealand government defining what IDM is, or can be, for next generation government. We explored how academics nowadays conceptualise, define and approach IDM and related concepts in a broader sense, in both traditional and new digital public service environments that is. We did this on the basis of available academic literature as well as professional literature of acknowledged thought leaders from industry.

Moreover, in order to further explore what might be a useful working definition of IDM in government at this stage, we investigated e-authentication applications in six other jurisdictions, namely Singapore, Hong Kong, Australia, the UK, Ireland and Austria. In our investigation, we focused on the relationships government has with individuals (rather than businesses for instance). The study of e-authentication solutions is based on website and policy document analysis. An analysis of these e-authentication solutions is provided in section 7 of this report, with a full overview presented in Annex I.

Our research question is the following:

What could be a useful working definition of Identity Management in government at present?

a) *What are conceptualisations, definitions and approaches of IDM in government according to academic literature?*

b) *Which e-authentication solutions have been developed in other jurisdictions?*

2 Current Conceptions of Identity Management in government

2.1. Current Identity Management definitions

The term 'Identity Management' (IDM) has become widely used, both in practice and in academia. And yet, a commonly accepted meaning for the term is lacking so far (Bamford, 2007; OII, 2007; Crompton, 2004). This lack of a common understanding can be explained by the fact that IDM is a relatively new term which meaning is not entirely settled. We are still on a journey of discovery towards the meaning of IDM in the emerging information age, both from an academic and a practitioners' point of view.

A quick scan of available academic literature indicates that the relatively new term 'Identity Management' is strongly related to processes in emerging digital environments so far. Moreover, current IDM conceptions do not reflect, or relate to, the unique role government has in our society. IDM seems to be mainly understood as a technical means which serves many and varied purposes, issues, and even organisations. These assumptions seem to be appropriate when looking at various working definitions being proposed for IDM, such as:

"*the set of business processes, and a supporting infrastructure for the creation, maintenance, and use of digital identities*" (The Burton Group, 2003 in: Scorer, 2007, p.43)

"*the management of identity-related information … is simply the digital authentication and certification of identity-related information, with its biggest use in access management*" (Brands, 2002a, p.81).

"*a set of data management systems and practices to increase confidence in the identity of individuals where appropriate"* (Crompton, 2004, p.1);

"*a process of representing and recognising entities as digital identities in computer networks*" (Jøsang, Fabre, Hay, Dalziel, & Pope, 2005, p.99);

A recent OECD-paper reminds us however that 'identity' is both a "real world" concept and a digital artefact, and that IDM in these two environments may entail different forms therefore (OECD, 2007). For instance, the representation of personal identity in emerging digital environments takes place on a different footing compared to identification processes in the traditional physical world. Although attempts to define IDM appear to be restricted to digital environments, it is not to say that IDM only takes place in digital environments. With continuing activities of individuals in

both worlds it is most likely that a convergence between digital identity and physical identity will take place (cf. Greenwood, 2007).

Moreover, the narrow focus on digital IDM in these definitions seems to ignore the fact that people continue to have a relationship with government in the physical world, in which IDM already has, and will continue to have, a certain role. In fact, citizens usually have multiple relationships with government agencies, each supported by a form of IDM (Fishenden, 2005). For example, the citizen will often have an Inland Revenue taxpayer's relationship, a Health Service patient relationship, a Border Control relationship as an international traveller, a Social Benefit relationship as a contributor and claimant within the system, a driver's relationship, and a resident relationship within a public housing scheme. The IDM system currently available to government is, at best, a patchwork of different – sometimes inconsistent – processes, practices and rules of law (cf. The National Electronic Commerce Coordinating Council, 2002).

Furthermore, traditionally, due to the collective interest society has in government, government needs to make sure that it serves its citizens, and will continue to do so, in equal ways. An overview of traditional principles of administrative equivalence in public service provision to citizens is summarised below (Lips et al, 2006). The introduction of transactional E-Government service provision and, with that, the introduction and use of new forms of IDM, should not make a difference for government in the execution of these principles. Some literature however suggests that the use of new IDM will make a difference, often without individuals being aware of it (e.g. Taylor et al, 2007; Murakami-Wood et al, 2006).

TABLE 1: Traditional Principles of Administrative Equivalence in Public Service Provision to Citizens (Lips et al, 2006)

Administrative Equivalence Principle	Details
Access rights to services	Equal service access for all citizens within any particular governmental jurisdiction (national, regional, local, functional)
Procedure	Equal and fair treatment during the service process
Entitlement to a specific standard of service	Equal service outcome for similarly assessed cases, in accordance with legally embedded norms

The unique role of government in IDM and, with that, the complexity of introducing IDM systems in citizen – government relationships, also comes through when looking comparatively to IDM cultures in various countries (e.g. Caplan, 2001). For instance, research in different European regions indicates that trust in government, also as an expression of social, cultural and historical values, determines the use, or non-use, of specific IDM solutions to a substantial extent (PRIME, 2004). McKenzie et al (2008) come to a similar conclusion in stating that culture and history strongly affect the nature of the IDM system that might be acceptable to citizens in particular circumstances, with trust in government being a key determining factor.

Examples of cultural and historical impact on IDM approaches are the legal ban on unifying numbers in German government, due to Germany's Nazi history; and the administrative use of two last names in Spain, family names of the father and mother, respectively. Another example of cultural differences in Europe is the fact that the introduction of ID cards is heavily debated in some countries (e.g. the UK), whereas in other countries the introduction and use of ID cards is not at all an issue (e.g. Belgium, Finland). Moreover, cultural conceptions of legitimate IDM may change over time, as can be observed in, for example, the Netherlands, where a law was adopted recently to extent the use of the fiscal number to other public service areas and, with that, to rename the fiscal number as a 'citizen service number'.

These considerations imply that government would want to make use of an IDM definition which:

- covers IDM activities in both the physical and digital world in a holistic and consistent way;
- meets traditional administrative principles like equity, etc; and,
- takes into account social, cultural and historical values.

To be able to discuss what converged IDM may look like, we will explore the nature and forms of IDM before the term was invented, i.e. IDM in the physical world.

2.2 IDM in citizen – government relationships in the physical world

There is not much academic literature available on IDM in citizen - government relationships in the physical world. This lack of attention may be explained by the fact that, traditionally in the physical world, the management of an individual's identity in citizen – government relationships involve more or less standardised procedures. Presenting themselves for identification purposes, individuals usually are scrutinised on the basis of personal recognition in face-to-face interactions at a service counter for instance, or, in the case of paper-based identification processes, submit their personal identification documents to the inspecting public official.

With that, it is interesting to note that for a long time the ways in which individuals represented themselves in identification processes did not change much. Historically, community development and related social interactions were on a small enough scale to base IDM activities on personal recognition and trust (Camp, 2003). Traditionally in Maori-culture, representation for identification purposes is done orally with individuals identifying themselves with their whakapapa (Meredith, 2008). The whakapapa not only includes the naming and order of genealogies of an individual, but also the spiritual, mythological and human stories that represent the genealogical backbone.[1]

In the development and expansion of the bureaucratic society, identification processes were extended to paper-based forms, introducing the need for individuals to submit

[1] In: Whakapapa Maori. Structure, Terminology and Usage, available at: http://maaori.com/whakapapa/whakpap2.htm#Introduction

paper-based proof of identity for representation purposes. Gradually, the most commonly accepted paper-based proofs of identity in many societies, so-called 'Trusted Identifiers', became the passport, birth certificate or driver's licence (Camp, 2003).

Generally in most countries, during the 20th century, we can observe a strong expansion of identification practices in citizen – government relationships. The evolution of particularly social citizenship rights and entitlements (e.g. benefits, education, public health) saw the number of separate public services provided to citizens expanded enormously, and a 'silo-structured' government with separate public counters for each public service domain emerge. Moreover, a further explanation offered for the expansion of identification practices has been the phenomenon of an increasingly mobile society. Increased international mobility of individuals led in turn to the establishment of a globally acknowledged, universal means of personal identification, the passport (Torpey, 2000). Remarkably, throughout time, the process of 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.

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* 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 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 (Noiriel, 2001).

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 (i.e. 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).

The history of the use of passports and their changing meaning in society shows us how important it is to look beyond technical characteristics in exploring the use of IDM in citizen – government relationships. Whilst there is a need to develop the technical field of IDM, there is a vital and urgent need to understand the social, cultural and political worlds within which these systems are used.

From this overview we may conclude that IDM in the physical world is much more focused on processes of *identification* by public officials, rather than on processes of an individual's *representation* in relationships with government (Lips et al, 2006). For

instance in paper-based public service provision, human assessment is the decisive factor in IDM: a public official assesses and decides upon an individual's paper-based request for access to a public service. Administrative assessments arising from an individual's request to access a particular public service take place on the basis of a single set of administrative norms and values within the governmental jurisdiction concerned. In cases where administrative norms leave room for discretion a civil servant seeks to apply existing administrative values based upon the notion of administrative equivalence as far as possible, e.g. through considering case law on the matter (Snellen, 1998).

Within this administrative system, a final assessment of a citizen's request for access to a public service can take considerable time. The various documents concerned are normally stored by the service-providing organisation in a personal file as 'proof of entitlement' to the specific public service. In many cases citizens need to queue until an official is able to bring one citizen's case to a close and start a new one. Usually these personal files are kept for a certain time period, again securing an element of administrative equivalence. Thus each individual service relationship is underpinned by a citizen's personal file and such information management is undertaken separately within each service-providing organisation. Public service providing organisations have turned thereby into vast repositories of stored paper records containing fragmented forms of information related to a citizen's identity.

Enlarging paper-based regimes of citizen identification and representation in an increasing variety of administrative processes have introduced a central tension to IDM practices when compared to earlier identification practices based on 'face to face' identification. Emerging from this document-based citizen – government relationship, a citizen does not fully own or control his or her personal administrative identity any longer (Caplan, 2001). Systems have been created to store and retrieve information about an individual's eligibility, leading to the emergence of generic categories of identity information on the individual: familiar personal details such as name, address, and date of birth.

We may conclude from this that, in the physical world, IDM in public service provision depends upon judgements and assessments made by public officials on the basis of generic categories of identity information. These generic categories of identity information have been acknowledged by government agencies as authoritative sources of identity information on the citizen, usually collected from, or supported with, official identification documents.

2.3 From paper-based to digital Identity Management

As people increasingly make use of digital environments, such as E-Government or E-Commerce, the need for reliable digital IDM becomes more and more urgent. However, replicating IDM approaches and means we have in face-to-face or paper-based environments does not appear to be an option. Digital IDM takes place in different environments and, with that, on a different footing, than we have been used to in the past (Lips et al, 2006). Digital IDM is about the *informational* representation of an individual, rather than a physical or paper-based representation, in a relationship or activity (Lips, 2007). Transactional E-Government relationships with individuals

are *information* dependent, therefore. In order to arrive at effective digital IDM solutions for government, we need to know more about what these new IDM means do to an individual's informational representation in digital environments.

Marx observes the following informational trends in society as a result of the introduction of new identification systems (Marx, 2003):

- 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;
- an expansion of ways of measuring and classifying citizens, with greater precision compared to traditional measures, such as paper-based methods; and
- an increasing use of digital forms of identification and authentication of personal data instead of physical forms.

Camp adds the following informational trends as a result of introducing IDM systems in E-Government relationships (Camp, 2003, p.7-8):

- information can flow freely, compared to information in face-to-face and paper-based transactions within the confines of a physical locale and relatively closed networks;
- information can be copied and stored at almost no expense;
- transactions become information dependent, with current identification systems relying on the confirmation of an individual's information;
- transactional histories become more detailed and easily available to many; and
- trust depends on transactional history reports rather than on personal recognition.

These informational trends can lead to different outcomes, which may 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 has declined significantly; at the same time however we may observe an increased freedom of choice for individuals to represent themselves, such as the use of different types of pseudonyms (e.g. email-address, phone number, credit card details) in interactions with others.

Generally, these informational trends pose new questions about how governments design their relationships with citizens. The shift towards digital IDM not only requires government to explore newly available digital IDM systems and reconsider IDM solutions available in the physical world, but also to reassess benefits and costs related to the use of IDM more in general, such as the protection of human rights (e.g. privacy protection, freedom of speech), the enforcement of responsibility (e.g. liability and responsibility of actions) and the enhancement of user and societal capabilities (e.g. reduction of coordination and transaction costs) (FIDIS, 2005).

3 Digital Identity Management perspectives

Although individuals are increasingly represented in multiple ways, namely in information systems, in official documents, and in face-to-face settings, scholarly efforts are almost exclusively focused on system-based forms of an individual's representation, also called 'digital IDM'. Usually in scholarly efforts, digital IDM is not related to government specifically but focuses more generally on the relationship between an individual and an organisation. In the next three paragraphs we will further explore what perspectives scholars take to approach IDM (section 3), how they conceptualise and define core IDM concepts (section 4), and what IDM system models and tools they acknowledge (section 5). A summarising analysis of dominant scholarly understanding of IDM is provided in section 6.

In academia, two dominant IDM perspectives can be distinguished in research activities. Several scholars focus on the emerging societal trend towards increased identification of the individual. According to this perspective, IDM is utilised as a business strategy to maximise the collection and use of identity information related to individuals (e.g. customers). Other scholars are exploring and advocating an opposite IDM perspective of minimising the collection and use of identity information related to an individual. The latter perspective appears to be the most dominant in designing IDM solutions. A summary of the two different IDM perspectives will be provided below.

3.1 Identity Management as maximising the collection and use of identity information

Facilitated by the availability of new ICTs, scholars point at a general trend in society of increased identification of the individual, often referred to as '*surveillance*' (e.g. Lyon, 2003; Gandy, 1989). Most scholars perceive this increasing amount of surveillance, especially the ability to gather an individual's identity information secretly and involuntarily, as a major societal concern (Danna & Gandy, 2002; Marx, 1999a & 2004; Lyon, 2003; Gandy, 1989). For instance, Clarke focuses on a specific form of what he calls 'data surveillance', i.e. the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons (Clarke, 1997). As he considers forms of data surveillance to be intrusive and threatening to an individual's privacy, Clarke urges for developing effective controls over data surveillance techniques, through implementing informational privacy policies (Clarke, 1988 & 2003).

According to scholars, this societal trend of maximising the collection and use of identity information is both taking place in the private sector, where data mining systems and practices increasingly are being used as a surveillance technique to facilitate the identification and classification of customers into distinct groups or segments (Gandy, 1989); and in the public sector, where the increasing practice of surveillance provided through CCTV cameras or ID cards, for example, lead to the social sorting of citizens on the basis of newly available identity information (Lyon, 2003; Murakami-Wood et al, 2006).

3.2 Identity Management as minimising the collection and use of identity information

Most scholars perceive anonymity and pseudonymity at the basis of an alternative information management paradigm for organisations, which they acknowledge as a realistic alternative to the currently dominant paradigm in society of increased identification of individuals (e.g. PRIME-project[2]; FIDIS-project[3]; Clarke, 1997; Gilbert, Kerr & McGill, 2006). In their view, an alternative information paradigm can be achieved through for instance incorporating anonymity and pseudonymity into IDM systems and providing individual users with complete control over transactions requests as well as the transmission of their identity information (e.g. Crompton, 2005 & 2006; Hansen et al., 2004; Royer, 2007). An example of such privacy-enhanced IDM systems would be the use of so-called 'partial identities' in online transactions. With that, a potential IDM definition could be *managing an individual's various partial identities and pseudonyms*. (Hansen et al., 2004; Pfitzmann & Hansen, 2006)

A core issue for providing 'secure' IDM to users is about whom I can trust and who will trust me (Clippinger, 2007). Governments may want to establish trust through coerced identity information disclosure and authentication, such as through issuing national ID cards. An alternative IDM approach however would be to design an open identity system, which architecturally would support the principles of equality of individual rights and provide for a highly decentralised and open governance model (Clippinger, 2007, p.188).

Scholars perceive a particular need to apply anonymising technologies now that the ability for automated systems to collect, store and disseminate personal information has significantly increased. These information systems may gather personal information for one purpose, but if used for another purpose they may create serious implications for safeguarding an individual's information privacy (Gilbert, Kerr & McGill, 2006). Similarly, Nissenbaum perceives the value of anonymity as the possibility of acting or participating digitally while remaining out of reach – i.e. being unreachable in the physical world. She believes an individual's 'unreachability' is the key element if a society is to place high value in transactions and expressions protected by anonymity (Nissenbaum, 2003). According to Clippinger, in order to protect an individual's identity from unwanted surveillance by governments, corporations or any other party, the real test for society will be to have authenticated anonymity, meaning that a trusted community network authenticates only that amount of information required to complete a transaction or participate in an organisation (Clippinger, 2007, p.188-189)

Acknowledging minimal personal information disclosure as a fundamental value for organising digital IDM, Microsoft's Identity Management Architect Kim Cameron has developed several IDM system design principles. His '7 Laws of Identity' have been widely acknowledged, both in academia and in practice:

2 https://www.prime-project.eu/

3 http://www.fidis.net/

1. User Control and Consent – Technical identity systems must only reveal information identifying a user with the user's consent.

2. Minimal Disclosure for a Constrained Use – The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution. The 'least identifying information' concept should apply for both claims and information least likely to identify a given individual across multiple contexts.

3. Justifiable Parties – Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4. Directed Identity – A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5. Pluralism of Operators and Technologies – A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers. The universal identity meta-system must not be another monolith, it must be polycentric (federation implies this), and also polymorphic. This will allow the identity ecology to emerge, evolve and self-organise.

6. Human Integration – The universal identity meta-system must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks. The identity system must extend to and integrate the human user, profoundly changing the user's experience so it becomes predictable and unambiguous enough to allow for informed decisions.

7. Consistent Experience Across Contexts – The unifying identity meta-system must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies. As users, we need to see our various identities as part of an integrated world which none the less respects our need for independent contexts. (Cameron, 2006[4])

4 Core concepts and definitions related to digital Identity Management

Several scholars are working on the conceptualisation and definition of core concepts for digital IDM, in some cases with an ambition to contribute to the design of future IDM systems. Substantial research activities in that respect are taking place in the European Union, where large subsidised research consortia are working under the FP6 Network of Excellence 'the Future of Identity in the Information Society' (FIDIS) and the FP6 R&D Project 'Privacy and Identity Management for Europe' (PRIME).

[4] http://www.identityblog.com/?p=354

Exploring the spectrum between on the one hand core or full 'identity' and on the other hand full 'anonymity', academic experts seem to agree that IDM involves the following core concepts: identity, identification, authentication, anonymity, pseudonymity, (un-)observability, and (un-)tracability. An overview of how scholars conceptualise and define each of these terms will be presented in the following sections.

4.1 Identity

Academic experts have invested considerable efforts in exploring to what extent and how digital identity may be different compared to physical identity. Greenwood (2007) introduces a useful typology for different forms of identity in relationships with government:

1. Digital identity (e.g. username, IP, email address);
2. Physical identity (e.g. passport, drivers license, birth certificate); and
3. Dual or "converged identity", a combination of digital and physical identity (e.g. a 'chipped' person or animal, biometric passport) (Greenwood, 2007, p.5).

Several scholars argue that, now that people increasingly are operating in digital environments, individuals have a growing amount of digital identities used to identify themselves in relationship with other entities (e.g. Clarke, 1994; Pfitzmann, 2007). Whereas, in the physical world, identity is considered to entail a rather comprehensive set of individual characteristics by which a person is recognised or known, in the digital world on the other hand an identity can be a rather simple subset of identity information (e.g. an email-address) (OECD, 2007). Moreover in the digital world, even a role-based identity can be defined as an identity, which may be used by a group of individuals who share the same role concurrently or in turns, for example (Clarke, 2008).

As an expression of digital identity, most scholars utilise the concept of *identity information*, i.e. data relating to a person. Moreover, an individual can represent a subset of identity information, which is often referred to by the concept of *partial identity*. *Identity attributes* are used to express the contents of partial identities or digital identities (OECD, 2007).

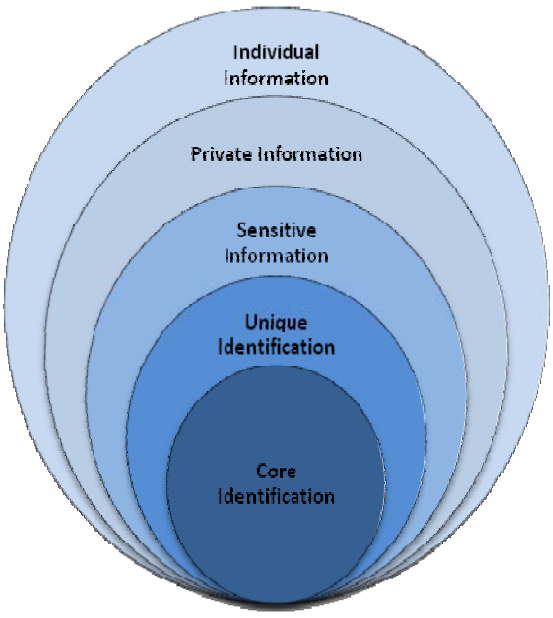
Unlike physical identity, digital identities are typically distributed in different forms and related to different locations (Norlin & Durand, 2002). For instance, identity can be defined as "*any subset of attributes of an individual which sufficiently identifies this individual within any set of individuals*" (Pfitzmann & Hansen, 2006, p.28). Usually an individual does not know all of her identities. Moreover, these identities may change as the person's attributes change. Consequently, aiming at developing a universal definition of identity and/or an "identity provider" is very hard, if not impossible (Pfitzmann, 2007).

Several authors present a layered conception of digital identity. For instance, Hayat, Posch & Rössler use the idea of a unique identity in relationship to digital identity. They define unique identity as the "*designation of a specific person by means of one or more features enabling that data subject to be unmistakably distinguished from all other data subjects*." Moreover, they utilise the concept of a 'recurring identity', understood as the "*designation of a specific person in a way which, while not ensuring unique identity, enables this person to be recognised by reference to a previous event, such as an earlier submission*" (Hayat, Posch, & Rössler, 2005, p.5).

Durand distinguishes three categories or 'Tiers' of Identity (Durand, 2002; in: FIDIS, 2005, p.31):

1. T1: the personal or inner and timely identity – this is the true personal identity that is owned and controlled entirely by the person;
2. T2: the corporate or assigned identity – this identity relates to a particular context (e.g. a business relationship) and represents a temporary assigned or issued characteristic for the person, such as a job title, phone number, email-address; and
3. T3: the marketing or 'abstracted or aggregated' identity – this identity corresponds to a result of profiling or filtering performed on a given set of an individual's characteristics (e.g. a high income customer, middle-aged, male and playing golf).

Marx uses an integrated vision on what he calls 'identity knowledge': i.e. varying types of personal information. He visualises the relationship between different types of personal information as a set of concentric circles (Marx, 2003):



In Marx' model of identity knowledge, the outermost circle is that of individual information which includes any data or category which can be attached to a person. For this concentric circle, the individual need not be personally known. Moreover, an individual does not need to be aware of the data linked to him. The next circle

consists of private information that is not automatically available and only revealed under compelled disclosure enforced by law. Each individual controls the identity knowledge that he or she regards as sensitive information, selectively revealing this information to people they trust and feel close to. Unique and core identifications create a unique identity that is attached to an individual, either jointly or individually. Traditionally, unique identity tended to be synonymous with a core identity based on biological ancestry.

Some researchers make a distinction between components, rather than layers, of identity. For instance, FIDIS-researchers distinguish the following four components that contribute towards the identity of a person (FIDIS, 2006, p.15):

1) Socio-demographic characteristics: e.g. gender, age, ethnic group, household size, employment status;
2) Benefit sought: the benefits desired from pursuing certain behaviour, including the underlying motivation. This component focuses on common values and attitudes across cultural groups;
3) Lifestyle adopted: options made regarding travel patterns, consumption of certain types of goods and services, for instance;
4) Behaviour exhibited: this component focuses on data resulting from the known history of an individual's actions in a relationship. Examples are shopping behaviour, tax compliance and contributions to political, religious or charitable groups.

Moreover, several scholars perceive the social context as a determinant factor for identity. From this relativist perspective, identity is granted and modulated by an individual's roles, relationships, and reputations in a variety of social networks (Clippinger, 2005). Based on a subjective interpretation of digital identity, Blakley *et al* distinguish the following properties (OECD, 2007, p.26):

- *Identity is social* – To engage in social interactions people need something that persists and that can be used as a basis for recognition of others;

- *Identity is subjective* – different people attribute different characteristics to an individual, constructing different identities for him.

- *Identity is valuable* – by building a history of a person's past actions, exchange of identity information creates social capital and enables transactions that would not be possible without identity;

- *Identity is referential* – an identity is not a person, it is only a reference to a person.

- *Identity is composite* – while some information is provided voluntarily by the individual, other information about him is developed by others without the person's involvement;

- *Identity is consequential* – because identity tells of a person's past actions, the decision to exchange identity information carries consequences;

- *Identity is dynamic* – identity information is always changing;

- *Identity is contextual* – people have different identities that they may wish to keep entirely separate. Keeping identities separate allowes a person to have more autonomy;

- *Identity is equivocal* – the process of identification is inherently error-prone.

4.2 Identification

IDM conceptualisations not only have an 'identity dimension', i.e. a set of characteristics representing a person, they also have an 'identification dimension', that is a set of terms, concepts and mechanisms that relate to the disclosure of identity information and the use of this information (FIDIS, 2005, p.26). Generally, the term 'identification' describes the process of ensuring a person is who he or she claims to be (Crompton, 2004). Identification in digital environments can be defined as *the association of data with a particular human being*: an identified record or transaction is one in which the data can be readily related to a particular individual (Clarke, 1994, p.8). FIDIS-researchers utilise the following definition for identification, which may cover identification in both physical and digital environments: *the set of approaches and mechanisms that intervene in the course of an interaction and which are very broadly related to the disclosure of identity information* (FIDIS, 2005, p.36).

Many authors utilise the concept of an *identifier* to indicate an information item that can be used to provide some level of authentication for a person (OECD, 2007; FIDIS, 2005). Identification occurs when a person or entity compares the identifiers of another person or entity, with a set of identifiers that the person or entity has previously recorded, and finds a match between the two (Harper, 2006). Generally, scholars distinguish the following four broad categories of identifiers (e.g. Harper, 2006; FIDIS, 2005; Anrig et al, 2004):

- Something that you are – characteristics that are inherent in a person or attached to an individual's physical body, e.g. DNA, fingerprints, voice signatures;

- Something you do – characteristics that relate to the behaviour of an individual, e.g. click behaviour in a digital environment, attitudes in a specific social context;

- Something you know – the characteristic of having some distinct knowledge, usually knowledge that few others have, e.g. passwords, mother's maiden name etc;

- Something you have – the characteristic of possessing some distinct item, these identifiers are often called "tokens", e.g. smart cards, software tokens like digital certificates, keys.

Harper (2006) introduces a fifth category of identifiers:

- Something you are assigned to – identifiers that are socially defined for the person, these identifiers are associated with people but not inherent or attached, e.g. name, addresses, titles, social security number, etc.

Scholars seem to agree that these categories of identifiers differ in their usability and their reliability.

Moreover, scholars point out that identification can be used for interventions in the following contexts (FIDIS, 2005, p.36-37):

- access control to restricted resources or areas – this control comprises two different aspects: authentication of the individual and access management;

- exploitation of identity information – allowing access to relevant information so that the impact of the interaction can be increased (e.g. customisation of services, diagnostic services, direct marketing);

- monitoring to enable accountability – the ability to record and audit the actions of a person (e.g. for supporting transactions, developing an individual's reputation).

Another distinction made by scholars is that identification can happen explicitly or implicitly (FIDIS, 2005, p.38-39):

- Explicit identification relates to processes in which the person is aware, and even participates in identification. Examples of explicit identification mechanisms are passwords, ID cards, biometric elements, business cards, introduction of the individual by another person in a social process;

- Implicit (or inferred) identification relates to processes that are used to authenticate the person and obtain the identity information without this person being aware, relying upon a series of available information from which the identity information is inferred or extracted. This can include identifiers attached to the person (e.g. visual appearance, IP number, RFID), or traces of characteristics that can be captured and analysed.

4.3 Authentication

Authentication relates to the verification of the individual's identity, ensuring he or she is the person he or she claims to be (FIDIS, 2005; van der Ploeg, 1999). Several authors describe authentication as *the process of checking a claim or assertion made by the person about their identity*, such as confirming that a person making a bank transaction is indeed the account owner (e.g. Crompton, 2004; Greenwood, 2007). In comparison, Clarke defines authentication as *the process of testing an assertion in order to establish a level of confidence in the assertion's reliability* (Clarke, 2008).

Identity verification can be done on the basis of one or more identifiers. Moreover, verification is not restricted by the two individuals or entities involved in the identification process, but can be done through the use of a (trusted) third party, such as a certification authority.

Alternatively, Greenwood restricts the definition of an individual's identity to what is *authenticated* in relationship to that person: once the individual's identity has been established through authenticating the claims made by that person, the person's authority is what his or her authenticated identity is allowed to do (Greenwood, 2007).

4.4 Anonymity

On the spectrum of identifiability versus non-identifiability, scholars define the polar value of identity as 'anonymity'. According to some scholars, full anonymity exists when an individual cannot be identified on any of the dimensions of identity information (e.g. Marx, 1999b). Also, anonymity can mean being unacknowledged, as well as being undefined (Clarke, 2002). The term can be applied to an individual, but also to other entities or subjects like data or transactions. For instance, defined transactions or records are anonymous when data cannot be associated with a particular individual, either from the data itself, or by combining the transaction with other data (Clarke, 1997). A practical example of anonymity is an individual connecting to a website.

Pfitzmann & Hansen use the following definition of anonymity:
"*Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set*" (Pfitzmann & Hansen, 2006, p.7). The anonymity set is the set of all possible subjects, for example individuals, organisations, senders, or recipients.

An individual's ability to remain anonymous is also explained from a more active perception of the individual's behavioural attitude in a certain relationship:
"Anonymity arises from withholding identifiers to prevent a usable identification from occurring. A person who has withheld identifiers from others is anonymous to them" (Harper, 2006).

Scholars distinguish between the following levels of control of anonymity (Claessens et al, 2003, in: FIDIS, 2005, p.42):

- Unconditional anonymity (no revocation possible);
- User-controlled conditional anonymity – in some cases a user could wish to revoke his anonymity: for example, a patient could ask for his medical records which have been stored in a medical database. For so-doing he would need to prove his identity;
- Trustee-controlled conditional anonymity – in some cases anonymity may be revocable by third parties under specific conditions (e.g. combating terrorism)

A few scholars indicate that anonymity should not be seen or treated as a synonym to privacy. However, anonymity can be perceived as a specific means by which

individuals may attain a degree of privacy (Gilbert et al, 2006; Crompton, 2002; Clarke, 1997).

4.5 Pseudonymity

As anonymity may prevent any useful two-way communication between parties, several authors perceive pseudonymity as a more realistic alternative for digital IDM solutions. A 'pseudonym' can be used as an identifier in certain relationships (e.g. Windley, 2005). Consequently, the term 'pseudonym' can be defined as "*an identifier of a subject other than one of the subject's real names*" (Pfitzmann & Hansen, 2006, p.19). An example of a pseudonym is the fictional name of a TradeMe vendor or buyer who wants to transact without disclosing his or her identity. Similarly, a pseudonymous record or transaction is one that cannot, in the normal course of events, be associated with a particular individual (Clarke, 1997).

More in general, pseudonymity is considered to represent a particular indirect mechanism that helps protecting the identity of the person in the conduct of some activity (FIDIS, 2005).

Clarke suggests two specific techniques which can provide pseudonymity in an online transaction:

- the authentication of eligibility rather than identity;
- the authentication of identity without recording it (Clarke, 1999).

4.6 Unlinkability and unobservability

Related to the polar value of anonymity and again focused on developing alternative solutions for digital IDM, academics also have introduced the concepts of unlinkability and unobservability.

Unlinkability of two or more information items (e.g. subjects, messages, events, actions) means that, within a digital IDM system, these information items are no more or no less related than they are related concerning a-priori knowledge (Pfitzmann & Hansen, 2006). An example of an unlinkable item is an anonymous message. A further distinction is made between 'absolute unlinkability', i.e. no determination of a link between uses; and 'relative unlinkability', i.e. no change of knowledge about a link between uses (FIDIS, 2005, p.40).

Unobservability is the state of information items of interest being indistinguishable from any information item of interest at all (Pfitzmann & Hansen, 2006). A similar concept is untraceability. The definition of the antonym 'traceability' is the possibility to trace communication between application components and as such acquire private information (FIDIS, 2005, p.41). It refers to the ability to obtain information about communicating parties by observing the communication context (e.g. through an IP address).

Unobservability is stronger than unlinkability, as it protects the contents of an operation, and even its existence. An example of an unobservable item is a secret message for which other parties cannot be aware of its existence.

5 Identity Management systems

Most scholars appear to be quite critical about available IDM systems and products. Several authors for instance point at the fragmentation of current digital IDM systems and the need for standardisation and international cooperation therefore (e.g. Greenwood, 2007; Durand, 2003). Some however argue that, due to political, organisational and economic complexities, developing standards and accreditation schemes for institutional-level interoperability appears to be far more difficult than developing technical standards (Backhouse, 2006; Backhouse, Hsu, & McDonnell, 2003).

Several authors indicate that many of the fundamental technologies for IDM systems are actually very well known and well understood. The following key IDM technology tools can be distinguished (Birch, 2007, p.4-5):

- *Public Key Infrastructure (PKI)* – this technology tool provides a mechanism for binding cryptographic keys (used to encrypt and to digitally sign messages) to other identity attributes (e.g. age, date of birth) to form 'key certificates' and for transporting those certificates around the internet;

- *Directories* – these tools are needed to give access to identity information and credentials;

- *Smart cards* – this tool provides a convenient mechanism for binding identity information to individuals with appropriate authentication, so that when an identity is used, other people can be certain that its rightful owner is present;

- *Biometrics* – there are many different biometric tools, ranging from iris scan and fingerprinting to body odour and face analyses. These are at varying degrees of maturity and appropriate for different uses, but standardisation is proceeding.

Some authors point at shortcomings of current IDM systems and products. For instance, Brands claims that digital IDM products have fundamental design flaws, as they rely on technology that was invented several decades ago: these technologies were never intended to serve as the basis of current access control and information authentication (Brands, 2002b). In his view, in shifting from physical to digital environments and introducing digital identity, physical trust domains are replaced by logical trust domains. Consequently, security must be tied to the identity information itself, rather than to the perimeter of its repository as with most IDM products (Brands, 2002a).

Not surprisingly therefore perhaps is that several scholars are closely involved in IDM system development. For instance, in line with Cameron's 7 Laws of Identity, IDM

solutions are being developed in the European FP6 project 'Privacy and Identity Management for Europe' (PRIME) to meet the alternative information management paradigm of anonymity in various e-service relationships while, at the same time, offering optimal services provision to consumers. PRIME aims to develop a working prototype of a privacy-enhancing IDM system. Offering identity information 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.[5]

Another IDM solution is being developed in the so-called 'Higgins' project[6], to which CA, Google, IBM, Novell, Oracle, Parity and Serena are contributing. Higgins is an open source Internet identity framework designed to integrate identity, profile, and social relationship information across multiple sites, applications, and devices. At the heart of Higgins is the so-called 'i-card': a graphical way to refer to a collection of identity information that a user might wish to send to a website or program. Higgins uses i-cards to unify and standardize identity interactions regardless of the underlying protocol or data source. The scope of Higgins is the following[7]:

1. Provide a consistent user experience based on i-cards for the management and release of identity data;
2. Empower users with more convenience and control over personal information distributed across external information silos;
3. Provide an API and data model for the virtual integration and federation of identity and security information from a wide variety of sources;
4. Provide plug-in adapters to enable existing data sources including directories, communications systems, collaboration systems and databases each using differing protocols and schemas to be integrated into the framework;
5. Provide a social relationship data integration framework that enables these relationships to be persistent and reusable across application boundaries.

A third example of an IDM solution is the U-Prove Technology developed by Brands' firm Credentica and recently acquired by Microsoft. Based on the assumption that security can be enhanced by protecting privacy, U-prove is an encryption and authentication system that allows individuals to disclose minimal personal information in digital transactions. The U-Prove Technology makes use of an ID token, i.e. a special kind of digital certificate that allows for minimal selective information disclosure. Moreover, the tokens are loaded with cryptographic protections that make them resistant to forms of ID-fraud or theft Although the tokens can store all kinds of information selected by users, they leave no unwanted data trails

[5] 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.

[6] http://www.eclipse.org/higgins/about.php

[7] http://en.wikipedia.org/wiki/Higgins_project#Scope

and permit both anonymity and pseudonymity, as neither the people who create the tokens nor those who accept them can track and correlate their use.

In general, scholars seem to agree towards the emergence of three different models for designing IDM systems (e.g. OII, 2007; OECD, 2007):

- Organisation-centric IDM: centralised, cross-domain IDM. The organisation keeps and manages personal information on the user, also across sectors; for example, different sub-sectors in government are allowed to synchronise a user's identifiers.

- User-centric IDM: the user has control over his/her own personal information; he or she also is the only party who knows the links between different personal information accounts.

- Federated IDM: involves the assembled identity of a user's personal information stored across multiple IDM systems. Authentication of the user takes place across multiple systems and organisations on the basis of mutual trust: the user authenticates himself to his primary domain and then his primary domain authenticates the user to all the other domains in the federation. This way, the user sets up only one account and logs on only once.

Although all three models could provide so-called 'single sign-on' to the user, i.e. a capability wherein the user is required to authenticate himself only once for multiple transactions, each model carries different implications in terms of control over the sharing of personal information (OII, 2007). Some authors indicate that the specific context, in which the need for IDM systems is considered, should be an important factor in the selection process for an appropriate model (Greenwood, 2007). We will discuss each of the models more in detail below.

5.1 Organisation-centric Identity Management

Organisation-centric IDM is based on the logic of being able to assign and control identities, according to hierarchically managed rules. Within this centralised IDM type, it is possible to create a single core identity for each individual, and establish other correlating identities based on centrally mandated rules (Greenwood, 2007). Many commercially available IDM systems prefer this centralised model, where a single identity service provider manages users' identities on their behalf, allowing for efficient management of identity and access, and less user support (Hansen et al., 2004).

Scholars have raised several concerns with this model, including the fact that the individuals identified by this system are not in charge of their identity within the system (e.g. The National Electronic Commerce Coordinating Council, 2002); the high concentration of data content and trail could increase the system provider's security risks (Hansen et al., 2004); and the likeliness of errors within large-scale databases, which imposes risks to personal privacy and victimisation of innocent people through no fault of their own (Schneier, 2007; Clement et al., 2001).

5.2 User-centric Identity Management

Although there is still much confusion about what user-centric IDM means in practice, scholars appear to agree upon a perspective of providing users with (more) control over the management of their personal information, respecting individual liberties and civil rights like privacy and ownership of personal information. According to Blakley (OECD, 2007), user-centric IDM systems provide users more control of their identities by allowing them to choose identity providers independently of service providers. The goal of a user-centric IDM system is to enable the creation of identity providers who operate in the user's interest. User-centric IDM systems incorporate the following three components:

1. Identity Providers - to store user account and profile information and authenticate users;
2. Relying Parties – to enable service providers to accept 'claims' about users from identity providers (i.e. having an authentication dialog with the user);
3. Identity Selectors – to allow users to choose which identity provider to use with (and what information to disclose to) a particular service provider (OECD, 2007, pp.44-45)

Scholars believe that user-centric IDM could emulate the complex levels of identity disclosure that exist in the physical world. When used in different combinations with federated and organisation-centric models, the user-centric model could offer a continuum of choices to suit various information-sharing needs and data protection requirements (OII, 2007). However, some scholars perceive a user-centric IDM model of individually managed identities, tokens and authorisations, to be more susceptible to identity fraud crimes (The National Electronic Commerce Coordinating Council, 2002). Consequently, within the user-centric model, individuals will have to accept responsibility for their informational privacy, as no agency can guarantee its protection for them (Hansen et al., 2004).

5.3 Federated Identity Management

Similar to the user-centric IDM model, the disclosure of personal information under a federated IDM model is contingent on relationships. Federated IDM is focused on autonomous groups, based on the logic of being able to remain independent of other identity schemes used by other groups, or the desire to maintain a primary and exclusive relationship with identified individuals (Windley, 2005). This also provides the setting for federated identity ownership and decision making, when groups determine that it is beneficial to adopt a common identity scheme. In contrast to users providing permission for the release of their personal information, the permission to release personal information in the federated model is determined amongst all parties involved, the so-called 'circle of trust'. Rules for sharing personal information among federation partners are typically defined by business partner agreements, although the terms of these agreements may be influenced by laws and regulations (OECD, 2007). In the absence of a relationship permitting the release of a user's personal information

from the identity provider that stored it to the service provider that sought it for a transaction, the user has no meaning to the service provider (OII, 2007).

As an international consortium, the Liberty Alliance Project Group aims to establish an open standard for federated network identity through open technical specifications. Their specification for federated network identity services will provide simplified sign-on capabilities for all network devices, permissions-based attribute sharing to provide users with choice and control over the use and disclosure of their personal information, and a commonly accepted platform and mechanism for building and managing identity-based web services based on open industry standards (Varney & Hogan & Hartson, 2003).

According to the Liberty Alliance Project Group, the adoption of federated IDM will bring several benefits to the public sector, including improved alliances both within and between government organisations, through interoperability with autonomy; faster response time for critical communications, cost avoidance, cost reduction and increased operational efficiencies; stronger security and risk management; interoperability; and decreased development time (Liberty Alliance Project, 2004).

6 Academic conceptualisations of IDM

Considering this overview of current scholarly thinking on IDM, although definitions of IDM are still many and varied, academics seem to agree on definitions for most of the core IDM concepts. The dominant focus of academia however has been on the conceptualisation of digital IDM so far. Moreover, the focus has been almost exclusively on technical aspects: on the design of IDM more in general, rather than on the application and use of IDM in the context of citizen – government relationships for instance. Moreover, the study of what is happening with and to IDM in citizen – government relationships in the physical world, also increasingly in combination with digital forms of IDM, appears to be more or less neglected. As a result, what a broader definition of ‘converged identity management’ in the public sector may entail, has not received much scholarly attention so far.

Interestingly, the technologies used for digital IDM products are usually well known and well understood for a few decades (cf. Birch, 2007; Brands, 2002a). The history of the use of the same identification technology during several centuries, i.e. the passport, shows us how important it is to consider the application and use of IDM solutions in a specific context: we need to know more about how IDM technologies are applied and used in citizen – government relationships to be able to decide upon a useful working definition of IDM in government. This is further confirmed by the scholarly assumption that the social context is a determinant factor for identity.

With the social context almost completely absent in current scholarly thinking on IDM, it may not be surprising that discrepancy between current academic view points mainly exists with regard to the definition of the most fundamental concept of IDM, i.e. identity. Compared to the representation of identity in the physical world, scholars agree on the assumption that ‘identity’ is differently represented in digital environments, and that therefore ‘identification’ takes place on a different footing.

Especially in digital environments, the multiplicity of identity information and layers of identity has been acknowledged by most scholars.

Although scholars generally are not (empirically) focused on the social context in which IDM activities occur, most of them share a certain ideology about what is needed in society. For instance, most scholars acknowledge the need for three, what could be called paradigm shifts in society: they are in favour of changing the perceived societal trend of increased identification; they are supportive of an alternative information management paradigm of minimising personal data collection; and they are in favour of user-centric models of IDM. Based on these ideological viewpoints, the European PRIME-project, the Higgins initiative, and Credentica's U-Prove Technology solution are all good examples of scholars developing their own preferred IDM solution for the emerging information society.

7 Current e-Authentication solutions in other jurisdictions

In order to investigate how digital IDM can be understood in the context of citizen – government relationships more specifically, we explored the ways in which other jurisdictions have adopted e-authentication solutions. The study of these e-authentication solutions was restricted to website and policy document analysis. We looked at the following six jurisdictions:

- two jurisdictions with fundamentally different public management systems compared to New Zealand, namely Singapore and Hong Kong;
- two jurisdictions with similar public management systems to New Zealand, namely Australia and the UK; and
- two jurisdictions which do not have fundamentally different public management systems compared to New Zealand but have prominent e-authentication solutions, namely Ireland and Austria.

An overview of the various e-authentication solutions and their embeddings in the respective E-Government related strategies of these jurisdictions can be found in Annex I of this report.

Comparing these national e-authentication solutions, we can observe that they differ quite substantially from each other, although similar IDM models, technologies and concepts are being used.

For instance, both Singapore and Hong Kong have adopted an organisation-centric e-authentication solution, including their national ID card as a key element. Singapore however does not use the ID card itself as an e-IDM tool, but makes use of the national ID card number as an important national unique identifier for authentication purposes. Although national ID cards are compulsory for citizens in both countries, Singaporeans are not obliged to make use of the e-authentication solution provided by government. Similarly, although SingPass is the default authentication scheme for E-Government service provisions in Singapore, individual agencies have an option to decide for other e-authentication means.

Hong Kong and Austria are both using a smart card as a substantial element of their IDM infrastructure, with Hong Kong introducing a smart card enabled ID card as a replacement of the existing ID card system. Using the SMARTICS system in combination with PKI as a single national IDM means for all purposes, Hong Kong has decided to store several sets of personal information on the card, including biometric templates and digital certificates. The Austrian Citizen card on the other hand provides for minimal personal information storage on the card, making use of high security standards combined with a strong protection of personal information.

Unlike e-authentication solutions in other jurisdictions, the Austrian Citizen card increasingly has become a concept, rather than a smart card, with individuals having several device options for how they want to make use of their electronic ID document including e-signature. Moreover, not only is the Austrian Citizen card used for e-authentication in public service provision but also in services offered by private sector organisations.

Quite the opposite from jurisdictions like Hong Kong and Austria, the Australian Federal Government has adopted decentralised e-authentication solutions in providing non-obligatory guidelines to individual agencies for assessing the suitability of available authentication mechanisms; final e-authentication solutions are dependent on the take-up of individual agencies. The AGAFI framework aims to promote consistency and interoperability across the Australian government so that individuals can expect similar e-authentication processes with similar assurance levels across government.

Both Australia and the UK offer a staged solution approach in determining the type of credential needed to use an online service, ranging from 'light touch' to 'heavy touch' e-authentication. The choice for a certain level of e-authentication depends on the extent of, and risks associated with, personal information exchanges in E-Government service provision to individuals. Similar to Australia, the UK Central Government's e-authentication solution is non-obligatory for central government agencies and dependent therefore on their buy-in into the e-authentication scheme. However, the UK offers centralised registration for e-authentication services, as is the case in Ireland, Austria, Singapore and Hong Kong.

Although the Austrian government partners with the private sector in offering e-authentication services, the authentication process itself continues to be conducted within the Austrian public sector, making use of authoritative data collected and maintained by government. Under its tScheme, the UK central government partly has handed over this process to the private sector, which is quite a fundamental change compared to traditional IDM responsibilities and activities of government in the physical world for instance. Moreover, the trust profiling of citizens conducted by private sector organisations like credit reference agencies, can be perceived as a moving away from traditional administrative equity principles in public service provision.

E-authentication solutions with a strong focus on privacy protection of individuals are provided in Austria and Ireland. Austria's user-centric solution is based on the information management principle of minimal personal data exchange or pseudonymity, with the Austrian Data Protection Commission in a key

implementation role as the SourcePIN registration authority. Ireland's federated solution offers users not only a single point of access to online public services, but also provides options to create different service accounts where they can change their personal details or have their personal details permanently removed from the portal's database of registered users. The Irish solution differs quite substantially from the Hong Kong solution for instance, where SMARTICS card holders are allowed to view personal data stored on the chip but are not allowed to change them.

It is also interesting to note that most jurisdictions perceive the generic authoritative data categories from IDM solutions in the physical world (e.g. name, address, date of birth) of continuing importance in the digital world, with some jurisdictions using a physical world mailing address as part of their e-authentication solution (e.g. Singapore, UK). Moreover, most jurisdictions utilise a multi-channel approach in offering public services to individuals, which implies that citizens have a choice in how they want to consume public services. Also, the importance of cultural and historical values as determinant factors for IDM solutions can be perceived in the relatively easy adoption of the new ID card in Hong Kong or in the decentralised IDM-solution in Australia, for example.

8 Working definition of Identity Management in government

From developments in academia and in practice we may conclude that, when we consider IDM in the context of government and its relationships with individuals in both the digital and physical world, there is no common understanding of core IDM concepts like 'identity', 'identification' and 'identity management'. Moreover, there is no clear development towards a preferred IDM model, technology or approach in the practical application of IDM in E-Government service relationships.

Interestingly however, although substantial progress is being made by government in adopting digital IDM solutions for E-Government service provision, these digital IDM solutions are not completely replacing physical world IDM solutions or public service relationships with individuals so far. Consequently, what 'identity' or 'identification' is in E-Government service provision today, is not completely different from what they are in public service provision in face-to-face or paper-based relationships. For instance, generic categories of personal information used by governments as authoritative data in the physical world, such as name, address, or date of birth, continue to be part of governments' IDM solutions in the digital world.

Moreover, individuals continue to have their unique self in the physical world, which becomes increasingly related to new and different 'identity attributes' when individuals represent themselves in E-Government service relationships. As we can observe from IDM developments in other jurisdictions, new identity attributes of individuals in E-Government service relationships often are imputed by government (e.g. unique number, a SourcePIN). As a result, individuals have a growing amount of identities and identity information in their relationships with government, also distributed in many and varied forms.

Consequently, what is different in the broader sense of IDM in public service relationships with individuals is that IDM is increasingly about the *informational representation* of an individual. Simultaneously, also due to the adoption of new IDM systems, human assessment of how to deal with personal information provided in public service relationships decreases. These developments stress the importance for government to decide what, and if so how, identity information will be collected, stored and used, especially also considering the asymmetric information relationships which could develop as a result of introducing and applying new IDM systems.

As a result, a useful working definition for government of IDM in public service relationships between government and individuals appears to be *the representation, collection, storage and use of identity information.* Related to this working definition, in order to establish trust in emerging E-Government service relationships and depending on social, cultural and historical values, government will need to decide on what information management paradigm to adopt for future IDM: towards maximising, or minimising, the collection, storage and use of individuals' identity information. Government will also need to decide upon the governance of identity information, especially if there are more parties involved in IDM activities, such as government agencies but also private sector organisations perhaps. And, last but not least, government will need to be transparent about its IDM design options and choices towards society, not only to further enhance trust of individual users of emerging E-Government transactional services, but also to further stimulate user-centric decision making about the preferred service channel in dealing with government.

References

Anrig, B., E. Benoist & D.O. Jaquet-Chiffellet (2004), *Virtual? Identity*, paper delivered within the scope of the European project Future of Identity in the Information Society (FIDIS), available at http://www.vip.ch/papers/virtual_identity.pdf

Backhouse, J. (2006). Interoperability of identity and identity management systems. *Datenschutz und Datensicherheit-DuD, 30*(9), 568-570.

Backhouse, J., Hsu, C., & McDonnell, A. (2003). Toward public-key infrastructure interoperability. *Communications of the ACM, 46*(6), 98-100.

Bamford, J. (2007). Identity Management: Achieving Data Protection Compliance and Inspiring Public Confidence, *Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing*: Oxford Internet Institute.

Birch, D.G.W. (2007), 'The Identity Vision', in: D.G.W. Birch (ed), *Digital Identity Management: Perspectives on the Technological, Business and Social Implications*, Gower, UK, pp.3-8.

Birch, D.G.W. (ed) (2007), *Digital Identity Management: Perspectives on the Technological, Business and Social Implications*, Gower, UK

Brands, S. (2002a). Secure Access Management: Trends, Drivers and Solutions. *Information Security Technical Report, 7*(3), 81-94.

Brands, S. (2002b). A technical overview of digital credentials. from https://www.sics.se/~lra/thesis/library/brands02technical.pdf

Cameron, K. (2006). The Laws of Identity. *Microsoft Web Services Technical Articles*, from http://msdn.microsoft.com/en-us/library/ms996456.aspx

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

Caplan, J. (2001). "This or That Particular Person": Protocols of Identification in Nineteenth-Century Europe, in: J. Caplan & J. Torpey (eds) Documenting Individual Identity. The Development of State Practices in the Modern World, Princeton: Princeton University Press, pp.49-66.

Caplan, J. & J. Torpey (eds) (2001). *Documenting Individual Identity. The Development of State Practices in the Modern World*, Princeton: Princeton University Press

Clarke, R. (1988). Information Technology and Dataveillance. in *Communications of the ACM, 37*(5).

Clarke, R. (1994). Human Identification in Information Systems: Management Challenges and Public Policy Issues. *Information Technology & People, 7*(4), 6-37.

Clarke, R. (1997). Introduction to Dataveillance and Information Privacy, and Definitions of Terms. from http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

Clarke, R. (1999). *Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice*. Paper presented at the User Identification & Privacy Protection Conference.

Clarke, R. (2002). *The Mythology of Consumer Identity Authentication*. Paper presented at the 24th International Conference of Data Protection & Privacy Commissioners.

Clarke, R. (2003). *Dataveillance - 15 Years On*. Paper presented at the Privacy Issues Forum, New Zealand Privacy Commissioner.

Clarke, R. (2008). *(Id)Entities (Mis)Management: The Mythologies underlying the Business Failures*. Paper presented at the Managing Identity in New Zealand, Identity Conference 2008.

Clement, A., Stalder, F., Johnson, J., & Guerra, R. (2001). National Identification Schemes (NIDS) and the Fight Against Terrorism: Frequently Asked Questions. *Computer Professionals for Social Responsibility, Palo Alto-CA, versión, 1*.

Clippinger, J. (2005). Identity, Reputation and Social Currency. *John H. Clippinger's Blog* Retrieved 20 February, 2008, from http://onthecommons.org/node/723

Clippinger, J. H. (2007). *A Crowd of One: The Future of Individual Identity*: Public Affairs.

Crompton, M. (2002). *Under the Gaze, Privacy Identity and New Technology*. Paper presented at the Union Internationale des Advocats (International Association of Lawyers) 75th Anniversary Congress.

Crompton, M. (2004). *Proof of ID Required? Getting Identity Management Right.* Paper presented at the Australian IT Security Forum, 30 March 2004.

Crompton, M. (2005), '*Trust, Identity and Connected Government*'. 24 June 2005, paper presented at the Forum for the Research, Development and Evaluation Commission "The Evolution of e-Government – From Policy to Practice", Tapeï.

Crompton, M. (2006). *The Revolution of RFID - Challenges and Options for Action: a consumer perspective*. Paper presented at the CeBIT 2006.

Danna, A., & Gandy, O. (2002). All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining. *Journal of Business Ethics, 40*(4), 373-386.

Durand, A. (2003,). Three Phases of Identity Infrastructure Adoption, January 23, 2003. Retrieved March 2008, 2008, from http://discuss.andredurand.com/stories/storyReader$343

Future of IDentity in the Information Society Project (2005) WP2, D2.1. *Inventory of Topics and Clusters*, 21 September 2005, available at http://www.fidis.net/resources/deliverables/identity-of-identity/#c1755

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

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

Gandy, O. (1989). The Surveillance Society: Information Technology and Bureaucratic Social Control. *Journal of Communication, 39*(3), 61-76.

Gilbert, D., Kerr, I. R., & McGill, J. (2006). The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers. *Criminal Law Quarterly, 51*(4), 469.

Greenwood, D. (2007). *The context for Identity Management Architectures and Trust Models.* Paper presented at the OECD Workshop on Digital Identity Management, Trondheim.

Hansen, M., Berlich, P., Camenisch, J., Clauß, S., Pfitzmann, A., & Waidner, M. (2004). Privacy-enhancing identity management. *Information Security Technical Report, 9*(1), 35-44.

Harper. (2006). *Identity Crisis - How Identification Is Overused and Misunderstood*: Cato Institute.

Hayat, A., Posch, R., & Rössler, T. (2005). Giving an Interoperable Solution for Incorporating Foreign e-IDs in Austrian E-Government. *IDABC Conference*.

Jøsang, A., Fabre, J., Hay, B., Dalziel, J., & Pope, S. (2005). Trust requirements in identity management. *Proceedings of the 2005 Australasian workshop on Grid computing and e-research, 44*, 99-108.

Leitold, H., Hollosi, A., & Posch, R. (2002). Security Architecture of the Austrian Citizen Card Concept. *Proceedings of the 18th Annual Computer Security Applications Conference*.

Liberty Alliance Project (2004). Whitepaper: Benefits of Federated Identity to Government. In T. Candia (Eds.), Available from http://www.projectliberty.org/liberty/content/download/388/2723/file/Liberty_Government_Business_Benefits.pdf

Lips, A.M.B., J.A, Taylor & J. Organ (2006). Identity Management as Public Innovation: Looking Beyond ID Cards and Authentication systems' V.J.J.M. Bekkers, H.P.M. van Duivenboden & M. Thaens (eds.), *ICT and Public Innovation: assessing the modernisation of public administration*, IOS Press, Amsterdam

Lips, A.M.B., J.A, Taylor & J. Organ (2006). *Identity Management, Administrative Sorting and Citizenship in New Modes of Government*, Paper presented at the Journal of Information, Communication & Society 10th Anniversary International Symposium, University of York, 20th - 22nd September 2006

Lips, A.M.B. (2007), Separating the Informational from the Electronic: Challenges and Opportunities for New Zealand Government in an Information Age, Inaugural Lecture Victoria University of Wellington, 20 November 2007, in: *Policy Quarterly, forthcoming*

Lyon, D. (2003). *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, Routledge.

Lyon, D (2004) *Identity Cards: Social Sorting by Database*, Oxford Internet Institute Internet Issue Brief No. 3, available at: http://www.oii.ox.ac.uk/research/publications.cfm

Marx, G. T. (1999a). Ethics for the New Surveillance. *Visions of Privacy: Policy Choices for the Digital Age*.

Marx, G. T. (1999b). What's in a Name? Some Reflections on the Sociology of Anonymity. *The Information Society, 15*(2), 99-112.

Marx, G. T. (2003). *Varieties of Personal Information as Influences on Attitudes Toward Surveillance*. Paper presented at the The New Politics of Surveillance and Visibility. from http://web.mit.edu/gtmarx/www/vancouver.html

Marx, G. T. (2004). What's New About the" New Surveillance"?: Classifying for Change and Continuity. *Knowledge, Technology, and Policy, 17*(1), 18-37.

McKenzie, R., M. Crompton & C. Wallis (2008), Use Cases for Identity Management in E-Government, in: IEEE Security & Privacy, pp.51-57.

Meredith, P. (2008), *Maor-e*, paper presented at the Managing Identity in New Zealand Conference, Wellington, 29-30 April 2008

Murakami-Wood, D, Ball, K, Lyon, D, Norris, C and Raab, C (2006) *A Report on the Surveillance Society*, available at

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

The National Electronic Commerce Coordinating Council. (2002). *Identity Management, A White Paper*. Paper presented at the NECCC Annual Conference.

Nissenbaum, H. (2003). Securing Trust Online: Wisdom or Oxymoron? *Virtual Publics: Policy and Community in an Electronic Age*.

Noiriel, G. (2001). The Identification of the Citizen: The Birth of Republican Civil Status in France, in: J. Caplan & J. Torpey (eds) *Documenting Individual Identity. The Development of State Practices in the Modern World*, Princeton: Princeton University Press, pp.28-48.

Norlin, E., & Durand, A. (2002). Federated Identity Management. from http://www.durand.com/ping/FIM_Whitepaper.pdf

Organisation for Economic Co-operation and Development. (2007). *At A Crossroads: "Personhood" and Digital Identity in the Information Society*, STI Working Paper 2007/7, 29 February 2008, Paris

Oxford Internet Institute (2007). *e-Infrastructures for Identity Management and Data Sharing: Perspectives across the Public Sector*: Oxford Internet Institute.

Pfitzmann, A. (2007). *An Introduction to Digital Identity.* Paper presented at the OECD Workshop on Digital Identity Management, Trondheim, Norway.

Pfitzmann, A., & Hansen, M. (2006). Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management-A Consolidated Proposal for Terminology (v0.3 ed.).

Privacy & Identity Management for Europe (2004), Social-economic requirements deliverable D1.1a.part 2, 11 October 2004, available at https://www.prime-project.eu/prime_products/reports/reqs/pub_del_D01.1.a.part2_ec_wp02.1_V7_final.pdf

Schneier, B. (2007). "Will REAL ID Actually Make Us Safer? An Examination of Privacy and Civil Liberties Concerns", *Testimony of Bruce Schneier*. Senate Judiciary Committee

Scorer, A. (2007), 'Identity Directories and Databases', in: D.G.W. Birch (ed) *Digital Identity Management. Technological, Business and Social Implications*, 2007, Gower, pp 41-49

Snellen, I.Th.M. (1998), 'Street Level Bureaucracy in an Information Age', in: I.Th.M. Snellen & W.B.H.J. van de Donk (eds.), *Public Administration in an Information Age. A Handbook*, IOS Press, Amsterdam

State Services Commission (2006), *E-Government Strategy*, November 2006, available at http://www.e.govt.nz/about-egovt/strategy/

Taylor, J.A., A.M.B. Lips & J. Organ (2007), 'Information-intensive Government and the Layering and Sorting of Citizenship', in: *Public Money & Management*, Vol.27, No. 2, Blackwell Publishing, pp.161-164.

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

Van der Ploeg, I. (1999). Written on the body: biometrics and identity. *ACM SIGCAS Computers and Society, 29*(1), 37-44.

Varney, C., & Hogan & Hartson. (2003). Privacy and Security Best Practices (2 ed.): Liberty Alliance Project.

Windley, P. J. (2005). *Digital Identity*, O'Reilly.

ANNEX I E-AUTHENTICATION SOLUTIONS IN OTHER JURISDICTIONS

1 Singapore

1.1 Singapore's E-Government Action Plan

Aiming to deliver accessible, integrated and value-adding public services to customers and help bringing citizens closer together, Singapore's second e-Government Action Plan (eGAPII, 2003-2006) was focused on the following three policy initiatives: Delighted Customers, Connected Citizens and a Networked Government. More specifically, eGAPII aimed to achieve the following goals by 2006:

- implement 12 more cross-agency integrated e-services;
- have 90% of the Government's customers use e-services at least once a year; and
- have 90% of these users satisfied with the overall quality of e-services.

In October 2004, under eGAPII's 'Delighted Customers' initiative, the Singapore government launched its Government Online Portal. The Government Online Portal integrated the previously released eCitizen portal and brought all government information and services under one site. The Public Services Infrastructure (PSi) is the infrastructure behind the Government Online Portal and aims to provide a platform for government agencies to rapidly develop e-services and deliver them to the public (Infocomm Development Authority of Singapore, 2006). The PSi offers development resources, such as an e-service generator, payment gateways, authentication services, electronic data exchanges, and e-service management tools.

'Singapore Personal Access' (SingPass) is one of the authentication methods supported by the PSi; other authentication methods include smartcards and username/password combinations. SingPass is a joint project between the Singapore Central Provident Fund Board, the Ministry of Finance, and the Infocomm Development Authority. The Government Online Portal utilises SingPass as the default authentication scheme for online public service provision to citizens. However, individual agencies are not obliged or restricted to use SingPass but they can tailor the selection of authentication methods to their perceived needs.

More than 40 government agencies are using SingPass to provide user authentication in about 370 different online service transactions. Online transaction services to SingPass holders include:

- Checking online statements (e.g. Central Provident Fund)
- E-filing of income tax
- Personal alerts for passport renewal, road tax renewal, overdue library books, etc
- Electronic payments for:
    - Vehicle fines
    - Property and income taxes

- Licences (e.g. TV, radio, vehicle, radio, dog ownership)
- Parking tickets
- Road tax

In 2007, 3 million SingPass users were registered, out of a total population of 4.59 million. Most registrants used SingPass to access information on their Central Provident Fund accounts (Infocomm Development Authority of Singapore, 2007). In 2006, the total volume of SingPass authentication transactions was 18.9 million.

1.2 SingPass

Singapore Personal Access (SingPass) provides single-factor authentication in online service transactions with government. The authentication scheme utilises a combination of an individual's National Registration Identity Card (NRIC) number and a privately selected alphanumeric password. The NRIC is the compulsory identification document for all Singaporean citizens and permanent residents over fifteen years of age. SingPass is automatically issued by the Singapore Central Provident Fund Office to Singapore citizens and permanent residents who register for their new NRIC or for other permits and passes that qualify for a SingPass account, such as an Employment Pass, an Entrepreneur Pass and a Work Permit. However, the use of SingPass is not compulsory for NRIC holders.

A dedicated SingPass website (www.singpass.gov.sg) provides opportunities for individuals to apply for a new SingPass account, update a SingPass account profile, retrieve a SingPass password, and change a SingPass password.

In order to apply for a new SingPass account, an individual needs to provide name, NRIC number, NRIC issue date, and current mailing address details. Once an individual's request has been successfully processed, the new SingPass will be mailed out to the address provided.

If a user would like to update her SingPass account profile, she needs to login using her SingPass ID and password. Moreover, she needs to provide mobile phone number which is registered in Singapore. The individual is offered the selection of two security questions out of five "shared secrets" stored in the individual's SingPass account. After verification of the user's details, a one-time code will be sent to the mobile phone number stored against the Singpass account. The user will need to enter the one-time code on the website as well as verify a dynamically generated security code displayed on the page. If the one-time code and security code are correct, the user will be prompted to enter a new 8 to 24 characters, case-sensitive password for the SingPass account, and re-enter the password to confirm it.

2 Hong Kong

2.1 Digital 21 Strategy

Presented as the blueprint for the development of ICT in Hong Kong, the Digital 21 Strategy includes E-government and IDM programmes. In 2007, the Digital 21 Strategy announced five key action areas to be accomplished between 2008 and 2010:

1. Facilitating a digital economy;
2. Promoting advanced technology and innovation;
3. Developing Hong Kong as a hub for technological cooperation and trade;
4. Enabling the next generation of public services; and
5. Building an inclusive, knowledge-based society.

In late 2007, as part of the 4th key action area, the Hong Kong government portal (GovHK) was launched to provide one-stop access to around 1,200 online government services (The Government of the Hong Kong Special Administrative Region, 2008). E-government programmes focused on IDM include Hong Kong's Smart Identity Card System (SMARTICS) and its Public Key Infrastructure initiative.

2.2 Smart Identity Card System (SMARTICS)

The Smart Identity Card System (SMARTICS) was introduced as part of the 2001 edition of Hong Kong's Digital 21 Strategy. Since 2003, the Hong Kong Immigration Department has been issuing the new chip-enabled multifunctional ID cards, also in replacement of the existing ID card system in Hong Kong (The Government of the Hong Kong Special Administrative Region, 2007). The ID card is obligatory for all Hong Kong citizens from 11 years of age on. Registration of an ID card is free of charge; a replacement however will cost a Hong Kong citizen c$335 Hong Kong dollar. The smart ID card is widely used for a variety of services, including public safety; online government services; library services; banking services; as a drivers licence; cross border management; and for getting employment.

Similar to the previous ID card system, the smart ID card displays the holder's photograph and several personal details, such as name, date of birth, and the Hong Kong Identity Card number (ICNO). However, the new smart ID card also holds digitised data in its embedded chip, including biometric templates for facial recognition and two thumbprint images and several personal details, such as the individual's name in English; the individual's name in Chinese; the individual's name in Chinese Commercial Code; a name change indicator; gender; date of birth; a gender change indicator; the Hong Kong Identity Card number (ICNO); date of issue; date of first registration; place of birth code; and resident status (Immigration Department, 2002). Moreover, digital certificates have been stored on the SMARTICS chip to enable PKI two-way authentication, fingerprint and card PIN verifications, and encryption of the biometric templates stored on the chip (Hong Kong Trade Development Council, 2005).

Individuals can apply for a smart card ID at a Hong Kong Registration of Persons office.

SMARTICS holders are able to utilise a number of features offered by self-service card-reader kiosks, installed at various Registration of Persons Offices, Immigration Headquarters and Immigration Control Points around Hong Kong. Using these smartcard readers, card holders are able to:

- View the personal data stored in the SMARTICS' chip.
- View e-Cert content and change associated PIN number, if there are e-Certs stored on the card's chip.
- Update the condition of stay or limited stay, if the holder is a Hong Kong resident with condition of stay (Immigration Department, 2008).

2.3 Public Key Infrastructure (PKI)

In 1998, a public key infrastructure (PKI) was introduced under Hong Kong's Digital 21 Strategy. The objective of adopting PKI was to enable safe and secure electronic transactions by providing a framework to ensure the integrity of information exchanged and the authenticity of participants' identity. The root Certification Authority of Hong Kong's PKI was established on a partnership between the Hong Kong government, and two private corporations – Hongkong Post Certification Authority, and Digi-Sign Certification Services Limited. These corporations became the only two accredited certification agencies responsible for issuing digital certificates in Hong Kong. Under Hong Kong's Electronic Transactions Ordinance (Cap. 553), PKI based digital signatures have the same legal status as paper-based signatures. All digital certificates supplied by either of the two certification authorities can be stored on the smart ID card, with card reader hardware and software available separately to support management and backup of these digital certificates.

The Hong Kong Post Certification Authority is the publicly acknowledged certificate authority in Hong Kong, issuing approved digital certificates named 'e-Cert' for personal and organisational use. These e-Certs are used in a wide range of E-Government services, online banking services, and electronic exchanges of encrypted documents with third parties. In April 2007, the provision of e-Certs was outsourced to a private contractor, E-Mice Solutions (HK) Limited.
Currently, a wide range of online services utilises e-Cert for authentication purposes, including:

- Secure e-mail – the PKI technology enables the digital signing of electronic mail, to indicate the sender's approval of content, and the content's authenticity and integrity.
- Online government services – Several services provided via the Hong Kong Government portal (GovHK) require e-Cert for authentication. Examples are voter registration, business registration, vehicle certification, road tests, and drivers licence renewal;
- Online banking services – Several banks in Hong Kong use e-Cert to provide authentication for Internet banking;

- Online stock trading and custodian services – Since 2001, authenticated investors can directly transact with their brokers in the Hong Kong Exchange and Clearing Limited (HKEx)'s system, allowing investors to place, modify, cancel, or enquire stock orders;
- Online entertainment service – e-Cert provides authentication for Online Betting Service offered by the Hong Kong Jockey Club. This free online service enables users to place bets, receive odds update via email, and transfer funds between their betting account and designated bank account;
- Electronic services provided by other organisations – The Securities and Futures Commission of Hong Kong utilises e-Cert to facilitate the electronic submission of Financial Resources Rule (FRR) returns from SFC registrants.

3 Australia

3.1 E-Government Strategy

In 2006, the Australian Government published its E-Government strategy "Responsive Government: A New Service Agenda", in which it announced its vision to achieve a connected and responsive government by 2010. The Australian Government identified four main areas of activity:

- meeting users' needs
- establishing connected service delivery
- achieving value for money
- enhancing public sector capability

The overseeing, coordination of implementation, and tracking the strategy's progress towards the 2010 target is carried out by the Australian Government Information Management Office (AGIMO), in consultation with the Secretaries' Committee on ICT, the Business Process Transformation Committee and the Chief Information Officer Committee.

3.2 The Australian Government e-Authentication Framework (AGAF)

In facilitating access for government agencies to cost effective ICT infrastructure, AGIMO has developed the Australian Government e-Authentication Frameworks (AGAFs) for government-to-individual transactions and government-to-business transactions respectively. While the two frameworks are structurally and principally similar, they address the different nature and requirements for government in transacting with individuals and businesses, respectively. In this report we will focus on the Australian Government Authentication Framework for Individuals: AGAF(I).

AGAF(I) is a non-obligatory guideline for government agencies. However, AGIMO has been successful in promoting AGAF(I), as the guideline is often used by government agencies when assessing e-authentication needs for their electronic services.[8]

AGIMO defines e-authentication as "*the process of establishing a level of confidence in whether a statement is genuine or valid when conducting a transaction online or by phone*." The AGAF(I) framework provides Australian government agencies with a set of guidelines, which encourages using a risk-assessment based approach in designing e-authentication processes. Aim of the risk assessment is to allow agencies to evaluate the suitability (e.g. the strength) of an authentication mechanism for their particular E-Government services.

[8] Personal interview Malcolm Crompton, 1 May 2008.

AGAF(I) is based on the following principles (Australian Government Information Management Office, 2005):

1. Transparency – agencies will make e-authentication decisions in an open and understandable manner involving consultation with relevant stakeholders;
2. Risk management – selection of e-authentication mechanisms by an agency will be guided by the likelihood and consequences of identified risks. These risks will be articulated as part of the development and justification of e-authentication mechanisms. Agency risk assessment and management will be conducted in accordance with the Australian and New Zealand Standard, AS/NZS: 4360;

3. Consistency and interoperability – agencies will apply a consistent approach to selecting e-authentication mechanisms, so individuals can expect similar e-authentication processes for transactions with similar assurance levels offered by different government agencies. Agencies will deploy e-authentication mechanisms that are consistent with the Australian Government Technical Interoperability Framework;

4. Responsiveness and accountability – agencies will be responsive to individuals' needs. They will be accountable for the delivery of e-services, provide guidance on use of those e-services and will facilitate dispute-handling processes;

5. Trust and security – agencies will implement security measures that will create an environment in which transacting parties can have a trusted relationship. The e-authentication mechanisms used will be useful and safe for government and individuals;

6. Privacy – agencies will collect personal information only where necessary for the processes being undertaken. Agencies will conduct Privacy Impact Assessments (PIAs) for all new e-authentication initiatives and the extension of existing e-services that go beyond their original scope;

7. Choice – agencies will ensure that individuals will have the capacity to determine whether or not they wish to access government services electronically. While it may be compulsory for individuals to engage in particular transactions with government, it may not be necessary for them to engage via electronic channels. As agencies choose the appropriate e-authentication mechanisms for their e-services on the basis of risk and business requirements, as far as possible, agencies will accommodate choice in designing and implementing authentication solutions. Choice will be limited only where required by overriding considerations, such as national security, or where unavoidable operational requirements make choice impossible or prohibitively expensive. Individuals will be able to choose, on a case-by-case basis, which government services they wish to access electronically or through non-electronic channels;

8. Diversity – agencies will support diverse e-authentication approaches that are aligned to assurance requirements. Agencies can choose the most appropriate e-authentication approaches on the basis of risk, public policy and PIAs;

9. Cost-effectiveness and convenience – agency e-authentication processes will be as seamless and as simple as possible. Individuals will not have to undergo cumbersome and expensive e-authentication processes for simple or low-risk transactions. There is potential for government to implement systems that will give individuals the option of using e-authentication processes for multiple government services, where there are benefits to citizens and the use complies with government security and risk management practices.

The AGAF(I) framework encourages government agencies to evaluate the following risk factors either quantitatively (in terms of monetary cost of risk compared to the cost of risk reduction techniques), or qualitatively (in terms of low, medium, high) if reliable data is unavailable (Australian Government Information Management Office, 2005):

- the likelihood that a damaging event will occur
- the costs of potential losses
- the costs of mitigating actions that could be taken

Other issues that agencies need to consider when assessing each risk factor include the relationship between the parties; the value of the transaction; and the risk of intrusion.

The AGAF(I) framework is based on four levels of risks (Australian Government Information Management Office, 2005):

	Level 1	Level 2	Level 3	Level 4
AGAF for Individuals	Minimal assurance	Low assurance	Moderate assurance	High assurance
	Minimal risk posed by transaction; therefore, little requirement for confidence in the assertion of the individual	Low risk posed by the transaction; therefore, some confidence in the assertion of the individual is required	Moderate risk posed by the transaction; therefore, moderate confidence in the assertion of the individual is required	High risk posed by the transaction; therefore, high confidence in the assertion of the individual is required

For government agencies, in order to assess their level of e-authentication requirements, these four risk levels have been matched with a four-staged approach to E-Government service provision, i.e. 1) information; 2) interaction; 3) transaction; 4) integration/transformation.

Under this approach, stage 1 of online service delivery does not require authentication, as it involves information provision only; 'light touch' authentication, such as passwords, cookies, or SSL authentication, may be considered for stage 2 of online service delivery, as interaction may involve accessing an agency's database for

example. Authentication requirements for stages 3 and 4 of E-Government service provision are similar: as exchanges of identity information take place between the agency and users (stage 3) as well as between agencies (stage 4), agencies will need to be able to verify the user's identity and enforce their access entitlements (Australian National Audit Office, 2001).

In terms of authentication options, AGAF provides an overview of common authentication mechanisms, including (Australian Government Information Management Office, 2005):

- passwords, personal identification numbers (PINs) and user identification (User IDs);
- cookies;
- biometrics;
- Pretty Good Privacy (PGP);
- Tokens such as smartcards, magnetic strip cards or physical keys;
- Secure Sockets Layer (SSL), Transport Layer Security (TLS)

In the case of high-risk situations where stronger authentication mechanisms are needed, AGAF(I) suggests using mechanisms like one-time passwords; challenge and response devices; conventional encryption; or PKI encryption. Agencies wishing to utilise PKI as their e-authentication mechanism will be required to adopt Gatekeeper, the Australian Commonwealth's strategy for PKI use in government.

4 United Kingdom

4.1 The policy context of the UK Central Government's Gateway initiative

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[9] 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 citizens 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, 2002a):

- 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

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

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

(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 the number of departmental participants. Logistically, the Gateway is now being taken forward by the e-Delivery Team within the Cabinet Office. This team was created in June 2001 when the Government Gateway and UK Online teams merged into a single unit (eDT, 2005b, p.23).

At present, the Gateway has more than 100 enabled services from over 50 government offices. There are three main groups of online service that you can register for: online services for individuals, online services for organisations, and online services for agents (third parties on behalf of individuals or organisations). For individuals there are c80 online services offered through the Gateway, including self-assessment taxation service online, child benefit service, State Pension Forecast online service, and applying for a provisional drivers licence. In 2005, most of the enrolments came 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, 2005a).

4.2 Functioning of the Government Gateway

The following key features of the Gateway can be recognised (eDT, 2005c, 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 UK Central Government Portal Directgov or individual 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 via the internet, but may not be aware that they are using the Government Gateway programmatically through Directgov or 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, 2005c, p.2).

To use any Gateway service, a citizen would need to register first; for many Gateway services this entails providing a full name and email address and choosing an alphanumeric password (eDT, 2005c, 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 HM Revenue & Customs Department's Self Assessment Service, the known facts are the Unique Tax Number, National Insurance Number or postcode, data already held on citizens within the department. Thus, when a citizen enrols for 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 is 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.*, p.2).

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, 2005d, pp.2-3). 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*., p.3). 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 (OeE, 2002a; 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 use of the Gateway. Digital Certificates are small pieces of encrypted software embedded in a smart card or hard drive of a PC (eDT, 2005d, p.8). 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 including 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, third party organisations are involved in identity management processes as providers of digital certificates and authentication solution providers in online service transactions with individuals.

As an example of third party organisations as digital certificate providers, 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 c£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.

Moreover, third party organisations are involved in providing authentication solutions, such as in the recently developed on-line application for a provisional driving licence. The full authentication process can be described as follows (Taylor et al, 2007):

An applicant for a licence enters the Government Gateway, almost certainly through first of all accessing the citizen-facing website Directgov (direct.gov.uk). The applicant for a licence inputs standard identity information - surname, initials, date of birth and three year address history (using postcode locator software as needed). These details are then electronically matched against existing driver databases in the back-office of the UK central government department concerned. If this data matching does not produce a match (which is very likely in the case of an applicant for a provisional licence), the applicant continues the transaction and a new record is created. Equally, the applicant can proceed if a match is found (i.e. the applicant has been positively identified in the departmental database) so long as these records do not preclude progression (e.g. he/she is not a disqualified driver). Having gone through this in-house matching system the applicant's details are automatically and in real time transferred to the data management company Experian. Using name and address history in particular, Experian seeks to match the applicant's details against a host of public and private sector databases.

The purpose of this ‘third party’ involvement of Experian is to validate, verify and authenticate the identity of the citizen making a licence application. Experian systems run personal information from the applicant against the Credit Application Previous Searches (154 million records) and Address Links (252 million records) databases, for example, seeking as they do so the agreed level of validation for the particular service that is being provided. In the case of an application for a provisional driving licence three or more corroborations are needed for name and address and two or more corroborations on the date of birth or an equivalent combination of these factors. This is the validation aspect of the check.

In addition, a verification score is assigned to an applicant, which is an outcome of a further data matching exercise that seeks to corroborate biographical details that only the applicant is likely to know and which again are to be found in other databases, such as Mother’s maiden name or some other ‘shared secret’.

Finally, all of these data are distilled into an authentication index with each applicant receiving a specific ‘trust score’. This final score, indicating the strength of the applicant’s ‘digital footprint’, is heavily influenced by the perceived quality of the databases within which the matching process occurs. Customer databases such as those of the main clearing banks are given higher salience in the authentication process than those of mail order companies, for example. Only when the trust score reaches the pre-ordained level can the applicant proceed to a successful conclusion of their on-line application. The trust score arrived at is not therefore a judgment of creditworthiness but a risk assessment attaching to the degree of certainty that the identity of the applicant is an accurate one. In the Experian methodology, the highest possible trust score is 99. A citizen coming on-line to transact with Government may appear in any of the deciles that this scale allows, therefore, and will only succeed in any particular transaction if the trust score is at or above the level set for that transaction.

5 Ireland

5.1 New Connections Action Plan

In 2002, in order to achieve an information society in Ireland, the Irish government launched a second action plan "New Connections" with four key strategic initiatives:

- All services capable of online delivery should be available electronically by 2005, through a single point of contact;
- The delivery of Government services should be reshaped around user needs, including continuous on-line availability and delivery of integrated services;
- Ireland's international competitiveness should be improved, through reduced business costs, higher efficiencies, better services and opportunities for businesses to develop new services and content;
- The business community and the general public should be stimulated to wider engagement with ICT, through contact with quality on-line public services (Department of the Taoiseach, 2002).

By 2005, the Irish government had not achieved the strategic goal of having all services available electronically. However, several E-Government transaction services were in operation, such as online payment for motor tax, filing tax returns and paying taxes, application for Area Aid, and property registration searches (Office of The Comptroller and Auditor General, 2007).

5.2 The Reach Services Portal and Public Service Broker (PSB)

Reach is an inter-departmental E-Government service delivery agency under the aegis of the Irish Department of Social & Family Affairs. Reach was established to develop and implement an infrastructure framework for the integration and delivery of public services in Ireland. The Public Service Broker (PSB) framework aims to provide users with a single point-of-access to numerous public services through the reachservices.ie website. The portal provides continuous access to public services through the internet and telephone, while maintaining existing face-to-face service provision. Its underlying PSB integration framework allows the portal to act as an intermediary between individuals and agencies, providing consolidated services that are normally delivered by different agencies, eliminating the need for individuals to submit information repeatedly or submit redundant information, and provide service progress updates to individuals. The PSB framework has been observed as one of the first examples of a federated identity service, operated by a central public service agency at the national level (Coughlan, 2008; Department of the Taoiseach, 2002).

The Reach services portal is a non-obligatory service and is available free of charge to users. Benefits of registering an account with the portal include (reachservices):

- Users do not have to provide the same personal details every time they complete an application form;
- Users can submit online payment for services;
- Users can view the history of their transactions with the Reach services portal;

- Users have the option to change or reset their password, change their personal details, or have their personal details permanently removed from the portal's database of registered users;
- Users may upgrade their registration by supplying their Public Service Identity (PSI) details. The PSI is exclusively used in dealings with public agencies, or agents authorised to act on their behalf. The PSI consists of the individual's Personal Public Services Number (PPSN), surname, forename, date of birth, gender, all previous surnames if applicable, all of their mother's previous surnames if applicable, address, nationality, and date of death in the case of a deceased person.

Users can create a standard Reach services portal account by registering a self-selected username, a password and a security question answer. At present, there is no restriction to the number of accounts an individual may register for. Users can store their personal details in a standard user account and use these details to pre-populate online forms. However, standard accounts are very limited in terms of access and subject to deletion after 60 days if they remain unverified.

The option to upgrade to a secure account is offered to all standard account holders. This involves verifying the stored PSI details in the user account against the details stored by the Department of Social and Family Affairs. To establish the account holder's identity, an unique account activation code will be sent to the account holder's home address (reachservices). Users with successfully verified PSI details will be able to apply for online government services that require the use of PSI details, including personal records retrieval, online payment for services, and automatic form completion.

The Reach agency is responsible for data collected on its site. User registration data is collected and stored in the portal's registration database, as well as copies of electronic forms that users have completed and submitted via the website.

The range of public services currently offered through the PSB has been described as quite limited (e.g. OECD, 2007). Currently, the only major user of PSB's shared authentication service is the Revenue On-Line Service (ROS). In this scenario, the account's username and password is used in conjunction with a personal identification number (PIN) issued separately by the Revenue Commissioner in order to access the individual's tax account online. The main online services available to the public through the PBS are the following (Office of The Comptroller and Auditor General, 2007):

- on-line submission to the Equality Tribunal of completed forms about discrimination complaints;
- on-line application for Arts Council grants;
- identity authentication for employees who wish to access the ROS in connection with their income tax affairs.

5.3 Personal Public Service Number (PPSN)

In 1999, to enable public service administration, the Personal Public Service Number (PPSN) was introduced. The PPSN replaced the Social Insurance Number. Since mid 2000, the Department of Social and Family Affairs is responsible for PPSN applications.

Each individual is allowed to only hold one PPSN. The PPSN is not a national identity however. At present, the PPSN is required for access to many public services, including:all social welfare services; revenue schemes including taxation and mortgage interest relief; free travel pass; Pupil ID; public health including Medical Card and drug payment schemes; child immunisation; housing grants; and driver theory testing and driver license (Department of Social and Family Affairs, 2007).

6 Austria

6.1 E-Government Strategy

Located in the Austrian Federal Chancellery, the ICT Strategy Unit is responsible for the Austrian E-Government Act. The e-Cooperation Board coordinates E-Government implementation project at both the federal, province and local levels of Austrian public administration.

The Austrian E-Government strategy is based on the following principles:

- Proximity to citizens – The administration must be at the service of citizens and not vice versa. Online services must be easy to locate;
- Convenience through efficiency – Citizens expect greater convenience from online procedures, public administrations must optimize processes by automating them and making use of modeling;
- Confidence and security – Electronic contact with the public administrations must be just as secure as the traditional visit to an office. In the electronic world, the secure exchange of information and transfer of data is guaranteed by defined security standards;
- Transparency – The success of technical solutions and their acceptance is dependent on the involvement of all relevant groups in their development;
- Accessibility – Services provided by the public authorities must be available to all without discrimination;
- Usability – The range of electronic services offered must be structured in an easily comprehensible, clear and straightforward manner;
- Data protection – Electronic signatures and encryption mechanisms shall contribute to the provision of high security standards;
- Cooperation – Close co-operation between all public administration actors is needed to promote e-government in Austria. Thus, E-Government services and infrastructures must be jointly used in order to achieve organizational, financial and administrative benefits;
- Sustainability – The Austrian E-Government strategy follows a staged plan involving several strategies and policies allowing the continuous development of advanced online services. Strategic ICT co-ordination within public administration shall help to foster Austria's competitiveness;
- Interoperability – In order to guarantee trouble-free online exchange among the systems, the Austrian E-Government systems are based on internationally standardized and open interfaces;
- Technological neutrality – E-Government services have to be open towards new developments in the ICT sector in order to offer the best solutions.

In March 2004, the Austrian E-Government Act entered into force. The Act provides the legal basis for the various elements of the Austrian e-government system, and for closer collaboration between E-Government service providing agencies. The Act’s principles are:

- Freedom of choice between service channels for applications to government services;
- Security for the purpose of improving legal protection by creating appropriate technical means, such as the Austrian citizen card;
- Unhindered access to government information and services for people with special needs by the end of 2007, in compliance with international web accessibility standards

The E-Government Act has defined principal e-government system elements for Austria, including the citizen card initiative, coupled with an identity management scheme based on sector-specific personal identifiers and authoritative registers.

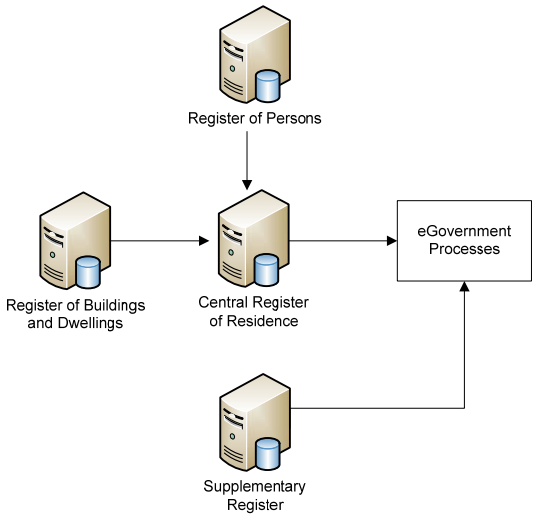
6.2 Identity Management in Austrian E-Government

6.2.1 Central Register of Residence

In 2002, the Central Register of Residence (CRR) was launched. The CRR repository holds authoritative personal and residence data, which are used in a wide range of E-Government service provision processes at different administrative levels.

The following data repositories feed into the CRR (United Nations Online Network in Public Administration and Finance, 2005):

- Register of Persons: containing identity information of all identified natural persons staying or residing in Austria (i.e. Austrians and foreigners), including name, gender, nationality, place and date of birth, and travel documentation data (type, number, issue date and authority) for foreigners;
- Register of Buildings and Dwellings
- Supplementary Register to the Register of Persons: containing personal data of all Austrians living abroad and foreigners transacting electronically with Austrian authorities; and
- Register of Residence: containing the residence data that belong to an individual, including address, type of residence (main or secondary), date of registration or de-registration, and name of the house owner or leaseholder.



Implementation structure of the CRR repositories
(United Nations Online Network in Public Administration and Finance, 2005)

The source PIN Register Authority is responsible for the Supplementary Register (SR). This repository holds identity information of natural persons that are not required to be registered in the CRR, such as expatriates and foreigners with no residence in Austria. The unique identifier in the Supplementary Register shares the same format as the CRR number, enabling transfer of records between the two repositories while maintaining unique identification in case of returning expatriates or foreigners gaining Austrian residency.

All individuals and entities registered in the CRR have been assigned a CRR-number: a unique 12-digit decimal number. Individuals or entities registered within the SR have been provided with a SR number. However, for privacy reasons, these CRR and SR numbers are never used for any other purpose than being a primary key for records hold in the CRR and SR. Instead, a separate unique identification number called Source PIN (sourcePIN) is specially derived from these CRR and SR numbers. The main purpose of the sourcePIN is to provide a unique identifier for electronic transactions (Rössler, Posch, & Hayat, 2005).

The Source PIN Registration Authority (i.e. the Austrian Data Protection Commission) is the only central governmental department with the ability to create sourcePINs, at the request of a Certification Service Provider (CSP). The Source PIN Registration Authority does not maintain a copy of generated sourcePINs, as these soucePINs should be kept solely by the owner, i.e. individual or entity. However, even the sourcePIN cannot be used for identification purposes in order to protect its privacy. Derivatives of the sourcePIN named Sector Specific PINs (ssPINs) can be made through encryption to support an individual's online transactions with different governmental departments. A ssPIN is made from the combination of a government sector's own alphanumeric code with the individual's sourcePIN. This allows a set of different ssPINs to be generated for interactions with different government agencies. The application of one-way encryption also makes it neither possible to reverse-engineer the ssPIN to obtain the underlying sourcePIN, nor generate a ssPIN for another sector (Rössler et al., 2005).

In 2007, the CRR held c8.3 million main residence data, 1.4 million sub residence data and 65 million historical data. The platform handles c200 million transactions per year, with approximately 100,000 users, such as public authorities, the police and businesses (Mader, 2007).

6.2.2 The Austrian Citizen Card

In 2000, the Austrian Federal government decided to employ smart card technology to improve citizens' access to public services. The first Austrian Citizen Card was issued in February 2003. Since then, the Citizen Card concept was extended to other types of cards like ATM cards, public servant ID documents, Student service cards, and the Austrian health insurance e-card, as well as to other devices, such as mobile phones, PCs and USB tokens. The current Citizen Card concept defines the requirements that are necessary to carry out electronic administrative procedures securely, also depending on the individual's choice for a specific Citizen Card implementation, such as a passport, student ID card or membership card[10]. The two most important requirements for the Citizen Card are the provision of identification and a secure electronic signature in accordance with Austrian Signature Law requirements. Under Austrian law secure electronic signatures are legally equivalent to personal signatures. From this point of view, a Citizen Card can be compared with an "electronic identification document".[11]

Individuals can use their Citizen Card for a wide range of E-Government and E-Commerce services including:[12]

- Online tax declaration
- Child allowance application
- Student allowance application
- A digitally signed criminal record
- Electronic public service newsletters
- Verifying the authenticity of documents
- Simple logon to web services
- Signing a contract electronically

To be able to use the Citizen Card, the following components are required:

- A signature creation device (e.g. a smart card), containing the cryptographic keys and the electronic signature. Personal data stored on the Citizen Card are the individual's name, date of birth, and the SourcePIN;
- An electronic identity document containing a certificate and an identity link
- A smart card reader in case a smart card has been selected as the signature creation device;
- Software for communication with the smart card

[10] http://alt.buergerkarte.at/en/was_ist_die_buergerkarte/konzept_buergerkarte.html
[11] *Ibid*
[12] *Ibid*

The Federal ICT Staff Unit and the Secure Information Technology Center – Austria (A-SIT) jointly have developed the Citizen Card concept. The Federal ICT Staff Unit is also responsible for the integration of the Citizen Card concept in Austria's E-Government Strategy. A Certificate Service Provider (CSP) is responsible for verifying the citizen's identity as part of the registration procedure as well as requesting the identity link from the SourcePIN Registration Authority. At the moment, a.trust is the only CSP issuing qualified certificates in Austria (Bürgerkarte, 2005). While there is no indication of cost for obtaining a Citizen Card, there is an annual cost for certificate related CSP services and an one-off cost for purchasing a card-reader.[13]

[13] http://alt.buergerkarte.at/en/was_ist_die_buergerkarte/konzept_buergerkarte.html

References

Australian Government Information Management Office. (2005). The Australian Government e-Authentication Framework for Individuals, Overview and Principles. Retrieved 8 April 2008, from http://www.agimo.gov.au/infrastructure/authentication/agaf_i/overview_and_principles

Australian Government Information Management Office. (2008). Australian Government Online Service Point (AGOSP) Program. 14 April 2008, from http://www.agimo.gov.au/services/agosp_program

Australian Government Online Services. (2007). The Update [Electronic Version]. Retrieved 14 April 2008 from https://www.govdex.gov.au/confluence/download/attachments/28999808/The+Update+First+Edition+December.pdf.

Australian National Audit Office (2001). Audit Activity Report January to June 2001. Report no 7, August 2001

Bürgerkarte. (2005). Participating organisations. Retrieved 30 April 2008, from http://alt.buergerkarte.at/en/beteiligte_organisationen/index.html

Cabinet Office (1999) *Modernising Government* (cm. 4310) London:HMSO

Coughlan. (2008). Ireland's Framework for Transforming Delivery of Public Services. Retrieved 30 April 2008, from http://www.epractice.eu/cases/2162

Department of Social and Family Affairs. (2007). Your Personal Public Service Number - More Information on the PPS No. . Retrieved 1 May 2008, from http://www.welfare.ie/topics/ppsn/moreinfo.html

Department of the Taoiseach. (2002). New Connections, A strategy to realise the potential of the Information Society [Electronic Version]. Retrieved 30 April 2008 from http://www.taoiseach.gov.ie/attached_files/Pdf%20files/NewConnectionsMarch2002.pdf.

Department of the Taoiseach. (2004). New Connections 2nd Progress Report [Electronic Version] from http://www.taoiseach.gov.ie/attached_files/Pdf%20files/New%20Connections,%202nd%20Progress%20Report.pdf.

eDT (2005a) *Government Gateway and DotP – Service Delivery Executive Report April 2005* – London:e-Government Unit

eDT (2005b) *Interactive Guide to Connected Government* – London:e-Government Unit

eDT (2005c) *UK Government Gateway – EP03 Gateway Technical Briefing* – London:e-Government Unit

eDT (2005d) *UK Government Gateway – EP02 Gateway Business Briefing* – London:e-Government Unit

Equifax (2005) *Service Policy Disclosure Statement* - available at www.equifaxsecure.co.uk/policies/spds.html

The Government of the Hong Kong Special Administrative Region. (2007). Chapter 4 Programme For The 2001 Digital 21 Strategy. from http://www.info.gov.hk/digital21/eng/strategy/2001/strategy_part46.html

The Government of the Hong Kong Special Administrative Region. (2008). 2008 Digital 21 Strategy > Enabling the Next Generation of Public Services. from http://www.info.gov.hk/digital21/eng/strategy/2008/Chapter_6_6_1.htm

Hollosi. (2004). *Country Update Austria*. Paper presented at the Porvoo 5, Interoperable European Electronic Identities
Hongkong Post. (2007). Types of e-Cert. Retrieved 20 April 2008, from http://www.hongkongpost.gov.hk/product/ecert/type/index.html
IDABC European eGovernment Services. (2005). eID case study: Austria [Electronic Version]. *Synergy*. Retrieved 30 April 2008 from http://ec.europa.eu/idabc/en/document/4486/5584.
Immigration Department. (2001). Hong Kong identity cards in different phases [Electronic Version]. Retrieved 30 April 2008 from http://www.immd.gov.hk/40/eng/apd/apd_id.html.
Immigration Department. (2002). *FS On AVC for IMMD - Appendix C Relevant Areas of SMARTICS*. Retrieved 20 April 2008, from http://www.immd.gov.hk/pdf/apvc/avc/appendixc.pdf.
Immigration Department. (2008). Hong Kong Identity Card Frequently Asked Questions (FAQs). Retrieved 20 April 2008, from http://www.immd.gov.hk/ehtml/faq_hkid.htm
Infocomm Development Authority of Singapore. (2006). Key Programmes under eGAP I - Public Service Infrastructure. Retrieved 8 April 2008, from http://www.igov.gov.sg/Programmes/eGAP_I/KP_eGAPI_PublicServiceInfrastructure.htm
Infocomm Development Authority of Singapore. (2007). SingPass enhanced to improve user experience [Electronic Version]. *Infocomm News from Singapore, December 2007*. Retrieved 8 April 2008 from http://www.ida.gov.sg/InSG/Dec07/egov.html.
Mader. (2007). The central register of residence in Austria. Retrieved 30 April 2008, from http://www.epractice.eu/cases/2269
NAO (2002a) *Better Public Services Through e-government* (HC 704), London, HMSO
NAO (2002b) *Government on the Web II* (HC 764) - London, HMSO
Office of The Comptroller and Auditor General. (2007). Special Report Number 58: eGovernment [Electronic Version]. Retrieved 1 May 2008 from http://www.audgen.gov.ie/documents/vfmreports/58_eGovernment.pdf.
Office of the e-Envoy (2002a) *Registration and Authentication – e-Government Strategy Framework Policy and Guidelines – Version 3.0* - London: Office of the e-Envoy
Office of the e-Envoy (2002b) *UK Online Annual Report 2002* – London: Cabinet Office
OECD (2008) *Ireland: Towards an Integrated Public Service*, OECD Public Management Review Ireland, 25 April 2008.
Reachservices. Frequently Asked QUestions (FAQs). Retrieved 30 April 2008, from https://www.reachservices.ie/reachPortal/appmanager/portal/default?_nfpb=true&_pageLabel=faqsPage&lang=en
Rössler, Posch, & Hayat. (2005). *Giving an Interoperable Solution for Incorporating Foreign e-IDs in Austrian E-Government*. Paper presented at the IDABC Conference 2005.
Taylor, J.A., A.M.B. Lips & J. Organ (2007), 'Information-intensive Government and the Layering and Sorting of Citizenship', in: *Public Money & Management*, Vol.27, No. 2, Blackwell Publishing, pp.161-164.
tScheme (2004) *Online identity Security reaches a crossroads* – press release 26 May 2004.

United Nations Online Network in Public Administration and Finance. (2005). Good Practice Case - Civil Registration in Austria Case Study [Electronic Version]. Retrieved 30 May 2008 from http://unpan1.un.org/intradoc/groups/public/documents/Other/UNPAN022349.pdf.