cc:eGov
Organisational change for citizen-centric eGovernment
http://www.ccegov.eu/

Think Paper 11: Trust and Identity in Interactive Services: Technical and Societal Challenges

Frank Wilson

Version No. 1.2

http://www.ccegov.eu/

i2010
Information Space
Innovation & Investment in R&D
Inclusion

ECOTEC
RESEARCH & CONSULTING

cc:eGov
Organisational change for citizen-centric eGovernment
http://www.ccegov.eu/

Think Paper 11: Trust and Identity in Interactive Services: Technical and Societal Challenges

Frank Wilson

Version No. 1.2

Prepared for the eGovernment unit, DG Information Society and Media, European Commission
http://europa.eu.int/egovernment_research

"Think Papers" aim to present strategic issues that will be explored with stakeholders and researchers. They are intended to be high-level summaries both of the issues and challenges, and of the ongoing work undertaken by the project team. They will be updated on the project web site http://www.ccegov.eu/ where registered participants can contribute to interactive explorations of definitions and issues.

Think paper series editors: Trond Arne Undheim and Michael Blakemore

i2010
Information Space
Innovation & Investment in R&D
Inclusion

ECOTEC
RESEARCH & CONSULTING

TABLE OF CONTENTS

1 Key Messages

- Trust requires verifiable identity – we need to be sure who we are dealing with. Therefore 'Trust enables Security' – 'Security enables Trust' – the requirements of each must be met.
- Trust levels are tied to 'acceptable risk' levels – for some services it is not necessary to implement highest security – cost and risk must be balanced.
- Trust hierarchies such as Public Key Infrastructures require investment and constant policing, while direct methods such as biometrics are more invasive – invasiveness, investment and risk must be balanced.
- Even eID cards can be misused and so verification in critical applications should combine card 'possession' with declaration of hard-to-copy information held by the person (e.g. knowledge not encoded on the card), or with data intrinsically tied to the person (e.g. biometrics).
- Partnerships with existing 'trust relationship manager' (e.g. banks) can provide additional verification channels for public authorities.
- A clear 'pact' is required between citizens and governments concerning the usage of citizen data so that there is a clear basis for citizen trust and a willingness to adopt electronic trust mechanisms.

2 Introduction

2.1 Trust - The eGovernment Context

The Ministerial declaration on eGovernment in 2007 [1] shows that the European Member States unanimously reconfirm the Member States' commitment to continue improving public services offered to citizens and businesses through the use of Information and Communications Technologies (ICT). While there are now numerous 'good practice' cases [2] emerging in Europe, recent studies [3] show the need to increase efforts to make services more 'citizen centred' and to continue efforts to spread the best approaches Europe-wide [4].

The European Commission, as part of its ongoing development of programme support for eGovernment issues, has identified specific priorities (see [5]) : Inclusive eGovernment, Efficiency and Effectiveness of eGovernment, High Impact Services, Key Enablers such as Electronic Identity (EID), and broader eParticipation. In all the priorities, trust is a critical issue, and so trust is reflected in the specific programmes supporting the above priorities, including various actions within the 7th Framework Programme [6], eTEN[7], and CIP[8] , including its EID pilot.

[1] European eGovernment Ministerial Declaration 2007 at: http://www.epractice.eu/document/3928
[2] ePractice.eu (good practice case) http://www.epractice.eu/cases/epractice
[3] Benchmarking Report on Electronic Public Services - http://www.epractice.eu/document/3929
[4] Taking stock of eGovernment 2005-2007 : http://www.epractice.eu/document/3927
[5] eGovernment priorities : http://ec.europa.eu/information_society/activities/egovernment/
[6] 7th Framework programme http://cordis.europa.eu/fp7
[7] eTEN http://ec.europa.eu/eten
[8] CIP-ICT-PSP http://ec.europa.eu/ict_psp

2.2 Trust in eGovernment

In common parlance, trust is a 'reliance' relationship between different parties or 'identities'. A trusted party is assumed to be both willing and able to fulfil agreements, policies, laws, promises, or simply received codes of ethics. Trust is reliance between two or more identities that one or more will act in specific ways. In the information society, some of the 'interacting' identities may be software systems acting as agents for authorities, organisations or customers.

This paper explores and explains some examples of technical and social challenges for eGovernment in the area of Trust and Identity in relation to Electronic Services.

The domain of discourse on the 'Information Society' (IS) concerning trust has, until recently, mainly emphasised the technical issues concerning 'trust and security', and has focused on the integrity of communication channels to ensure only lawful access to communications and their contents, and to minimise unlawful tampering or usage. However, as the scope of IS applications and services expands to include semantic web, remote agents, and a complex web of interoperable services and information sources, there is a significant increase in emphasis on 'trust' at the human level. This trust demands the inclusion of methods for ensuring, proving, and verifying the identity, not only of software agents and remote systems seeking interaction, but also of people seeking to access interaction opportunities concerning information, communication channels, and active electronic services (eServices).

The concepts of trust and identity have become intimately bound, and have been broadened beyond a purely technical focus. This paper seeks to explore some of the consequences of these changes for public authorities and other interested parties, as we move towards the i2010 goals of greater inclusion and easier access to services for all citizens.

This topic presents particular challenges to eGovernment, and since the cases used in this paper rely on some understanding of the underlying technologies, or coverage necessarily moves from technologies through to cases and examples. Readers with some understanding of the technology should note that empirical examples are included in "Trust and Identity – Enabling Interactive Services" (Section 6) and in "Monitoring Behaviours – trust In Knowledge Owners" (Section 7). where we provide reference to the different types of technical infrastructures which are necessary to create trust. Section 3 (Trust : People Interacting Through technology) provides some perspectives on how trust is formed and how it relates to technology, while Section 4 (Trust and Security – Technology for Access Control) deals with specific technologies being widely deployed, and Section 5 (Electronic Identity – Trends and Challenges) illustrates some critical issues being addressed by eGovernment service providers at the present time.

These themes will be further elaborated by the work of the SecureEgov [9]study recently launched by the European Commission and a panel of experts in all aspects of security and eGovernment. Interested readers can register there to join online discussions, workshops and information events.

[9] http://www.securegov.eu/

3 Trust: People Interacting Through Technology

3.1 Trust, Risk and Reassurance

The basis for trust may lie in the use of an encryption code, the 'perception' of a secure system, or in the reputation of an authority. Either may engender 'trust', yet neither is proof since either can fail in extreme circumstances. Society cannot work without trust, since placement of trust allows actions that otherwise are not possible (Coleman., 1990), but there is an element of risk until 'proof' by experience provides the parties a more solid basis. Initial establishment of trust sometimes therefore utilises 'icons of conviction' or symbols that induce risk taking (e.g. solidity of bank image, icons indicating security technologies in use, etc.). Trust is an action that involves the placement of resources (financial, intellectual, informational, etc.) under control of a trusted party while there is no 'provable' commitment. Since there can be an lapse of time between the giving of trust and the result from trusting behaviour, assurances and support for entry into trust relationships are necessary.

"Trust is to rely upon actions or reactions at a different point in space or time."
"Trust is that which is essential to a communication channel but cannot be transferred from a source to a destination using that channel." – Ed Gerck (1997)

3.2 Trust as Experience and Context

A mother, when selecting a nursery school for her child, will place more trust in another mother with children in nursery school than in her bank manager. However, when seeking financial advice she may prefer the views of her bank manager. Trust is about experience and context. Nissenbaum notes that *". . evidence that others merit trust is their past behaviour. If they have behaved well in the past, protected our interests, have not cheated or betrayed us, and in general have acted in a trustworthy manner, they are likely to elicit trust in the future*"[10]. This experience applies equally well to citizens and organisations and demonstrates a need for both to have access to evidence of previous behaviour as a basis for trust, and such evidence may be direct or indirect (e.g. credit reference and other referred information). In using

3.3 Privacy Leads to Trust Networks (History)

In 1991 a US developer with interest in human rights (Philip Zimmerman [11]) developed a 'privacy protection' package which he labelled 'Pretty Good Privacy' (PGP). Its use was intended to secure email inclusions / attachments from snoopers, and it came at a time when discussion of government access to emails for 'security' was a newly debated topic. So hot was this issue that the release of PGP worldwide initiated a 3-year investigation of Zimmermann when the government declared that US export restrictions for cryptographic software were violated. This exposed the delicate balance between National Security needs (access to data), and the needs of business and citizens (privacy of data - the technology issues are described in section 4). PGP is still in widespread use and relies on business and public users to share keys with persons they trust. Keys for 'unlocking' documents can be handed on by 'trustees' to others whom they trust, and so a 'trust network' or web of trust is developed. As will be seen when considering the operation technology issues. This 'informal' or social network model has some limitations.

[10] H. Nissenbaum, Will Security Enhance Trust Online, or Supplant It?. In P. Kramer and K. Cook (eds.) Trust and Distrust Within Organizations: Emerging Perspectives, Enduring Questions., Russell Sage Publications, 2004.

[11] Phil Zimmermann web site and home of PGP : http://www.philzimmermann.com

3.4 Models of Trust – Keys to Knowledge

Explicit models of trust can be developed from ratings supplied by users of commercial eServices[12], or from surveys of citizens answering questions about their government and its functions[13]. In contrast, informal models of trust rely on social network information (referred trust). For example, in using PGP (Pretty Good Privacy) people publish unique public key identifiers (a component of public key infrastructure – PKI – see later). Such 'keys' have 'claimed' associations with persons or organisations, and so trust is limited at that level until proven through experience. Each participant is responsible for supplying and receiving identity information, and so verification relies on social network information[14]. In contrast to PGP, where there is no 'agency of trust', more recent developments have begun to develop 'trust hierarchies'[15] where networks of agencies and authorities oversee registration and usage of virtual keys for assurance of 'trust and security' (e.g. Public Key Infrastructure – PKI, see later). These basic issues still shape trust networks, and the critical choice is between a centralised 'regulator' (highest level of control) versus an acceptance of personal choice for sharing of trust (lowest level of control).

3.5 Trust Beyond Technology

Since people learn to trust others through experience, and through judgement based on both direct and referred experience, the move towards electronic communications and services removes some opportunities and mechanisms for both acquiring (trusting) and engendering (reassuring).

Technology can in itself go some way to reassuring us that a data channel is difficult to invade, that the contents of a digital file have not been altered, and that parties in communications appear to be who they say they are.

Going a stage further, we may use technology to recognise fingerprints or the iris of the human eye as a method of verification of identity. These methods are known as "biometric recognition" and they refer to the use of "distinctive physiological (e.g., fingerprints, face, retina, iris) and behavioural (e.g., gait, signature) characteristics, called biometric identifiers (or simply biometrics) for automatically recognizing individuals". [16]. While iris and fingerprint show some initial usage (e.g. in-house credit systems for company canteens use fingerprint, and some airports allow iris recognition to replace passport at exit), they are not yet widespread and are limited to 'monitoring' physically present individuals in 'free' situations (see later for further issues in biometrics).

In the domain of eGovernment, trust is not wholly defined by the security of the communication technology or by the individual conception of trust engendered through education and socialisation, since government is a 'given' and carries very strong social expectations. However, in the 'information society', development of trust can combine these two factors to assist in the making of educated decisions in situations typically characterised by uncertainty, and can add verification techniques for greater rigour when required.

[12] P. Massa and B. Bhattacharjee. Using trust in recommender systems: an experimental analysis, 2004. Published in iTrust2004 International Conference

[13] M. Blakemore and P. Lloyd. Trust and Transparency: pre-requisites for effective eGovernment. Think paper No. 10. CC:Egovernment initiative. http://www.ccegov.eu 2007

[14] S. Garfinkel. PGP: Pretty Good Privacy. O'Reilly & Associates, 1994

[15] R. Housley and T. Polk. Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure. Wiley. 2001

[16] Maltoni D., Maio D., Jain A K., and Prabhakar S. 2003 Handbook of Fingerprint Recognition, Springer 2003, Corr edition 2005

The following subsections examine some of the human-technology integration issues under selected trust and identity topics. In each we try to expose both the technical and operational (human and organisational) issues to be addressed.

4 Trust and Security – Technology for Access Control

The term 'trust and security' has historically been associated with making communication channels secure, ensuring communication contents would be tamper proof, and guaranteeing that identities could be known (trusted) at least at the level of 'ownership' of keys, PINs, passwords, etc. (PIN = personal identification number): "Security makes trust work. Trust makes security work"[17].

4.1 Virtual Keys in a Virtual World

The simplest security 'key' is the 'personal identification number' or PIN. The PIN is no more than a secret password and is 'NUMERIC' because it was designed for use in simple bank 'automated teller machines' (ATMs) in the early 1960's. It has since become a standard way of managing security in other devices having a numeric keypad, for example 'point of sale' machines with 'chip and PIN' card readers. Here, the user provides a non-confidential token such as a bank card, and insertion of this card, plus the entry of a PIN, allows the bank to determine if the card used, and the PIN entered, match the data stored by the bank. If they match, it is assumed the user is a valid user of that card and has legitimate access to the associated 'rights'.

Taking this approach a step further, 'public key cryptography' uses a pair of cryptographic keys which are not the same, and so has a public key (to be disclosed) and a private key (to be kept secret). Software can be used to encode (encrypt) and decode (decrypt) information to enable secure transmission (e.g. sending my credit card details, or an order form), or can simply be used to 'authenticate' the person offering the key. Encryption software uses algorithms (encoding methods) that determine encryption based on a pair of keys, such that the private key can be used to encode (lock) while the public key can be used to unlock (open). In this way, people can give their public key to those they trust to access data.

While cryptography had much of its early development for military and national security purposes, initiatives such as PGP brought this technology within the reach of citizens so as to protect their human rights (see section 3), and making keys (and hence encryption) easy to use is still a major challenge for developers aiming at 'citizen friendly' online services.

4.2 Trust Webs, Hierarchies, and Networks

PGP (Pretty Good Privacy) appeared in the early 90's as a solution for citizens seeking improved privacy online. The use of encryption keys in PGP relied on a 'web of trust' or trust network. It was up to users to share keys with 'trusted parties', and to understand they may, based on their own trust, pass these keys on so that others may access selective information. In time this became formalised by explicitly including, along with a key, the signatures of 'trusted introducers' (PGP version 2.0 [18]). In such a scheme we each accumulate keys from other people that we may want to use as trusted introducers. Other people will choose their own trusted introducers, and so

[17] Graham Klyne, ninebynine.net

[18] Web Of Trust : http://en.wikipedia.org/wiki/Web_of_trust

people gradually acquire and then distribute with their own key an added collection of certifying signatures from 'trusted' people. The expectation is that anyone receiving it might find a signatory they will trust among the 'introducers'. This is intended to allow growth of a decentralized 'web of confidence' for public keys that is 'fault-tolerant'. However, 'self signed' or self assured schemes do have limits, and a person may wish to access information where they do not recognise a 'trustee' – so have no real basis for trust.

Whenever 'self signed certificates' are seen as a source of weakness, the most common alternative approach to developing 'webs of trust' is to develop a 'trust hierarchy' based on secure technology and 'certification agencies'. The use of common and well known public agencies is what distinguishes a 'public key infrastructure' (PKI [19]). This is a system of digital certificates, digital signatures, certification authorities, and registration agencies which together verify and authenticate the validity of the parties in an Internet transaction. While they can guarantee a high level of confidence in the initial creation of keys and binding to known identities, in operation they can only examine keys, check validity, and approve transactions on the 'assumption' that the key is used by its legitimate owner. They add a level of confidence based on the rigorous certification process – and so any misuse is liable to be a localised event (e.g. stolen card or key) and not systematic (e.g. large scale fraud). This is a similar approach as, for example, credit cards. If I lose my credit card (material object) I will report it lost and it will be stopped. However, a lost (virtual) key may be harder to notice, and can be used until misuse is detected, either through automatic detection (e.g. scanning for fraud patterns) or by being reported as mis-appropriated.

PKIs are still evolving and there is no overall PKI, nor even an agreed standard for setting up a PKI. Nonetheless, it has become widely accepted that reliable PKIs are necessary to enable widespread deployment of secure electronic services for Commerce and Government. A major issue for PKIs is to ensure that *"disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship"*[20]. Policing and enforcement of trust networks will be a major undertaking in future.

Federating PKI – Multi PKI Validation - As PKIs evolve, a challenge will be the emergence of multiple PKIs operating within a given domain. One solution may be 'federation' whereby multiple PKIs can be co-operated (interoperability) via a single superstructure. Section 6 deals with example applications, but for the purpose of illustration here, we can say that Ministry of Public Administrations of Spain, in promoting eGovernment and new citizen's Electronic Identity Card (eID), has established a Multi-PKI Validation Platform (MPVP) to provide free Electronic Identity and Signature Services (eID Services) to any eGovernment Applications with qualified electronic certificates issued by different Certification Service Providers (CSP's) accredited in Spain[21]. The service includes the two qualified certificates of the citizen's eID card, and so allows all eServices to extend their reach to eID card usage immediately.

A contrast with trust hierarchies based on registration authorities involves those offering trust references based on personal experience. For example 'Linked In' (www.linkedin.com, www.linkedin.net) claims that it "*strengthens and extends your existing network of trusted contacts . . . a networking tool that helps you discover inside connections to recommended job candidates, industry experts and business partners*". Here, the failure rate is determined by knowledge and caution (cross checking). Like credit card security, performance is not 100% but appears to be an 'acceptable risk' based on growth and usage, underpinned by human networks of trust based on experience.

---

[19] Public Key Infrastructure article online at : http://en.wikipedia.org/wiki/Public_key_infrastructure

[20] K. Cameron. The Laws Of Identity (2005 – updated 2007) : available online at http://www.identityblog.com

[21] Rodriguez M A., 2006, "MultiPKI Validation Platform for eID and eSignature Services " Case Study online at http://www.epractice.eu/cases/afirma.

4.3 Symbols of Security – Trust in Brands

Some authorities suggest that security has replaced real human trust (e.g. Nissenbaum 2004 [22]), insofar as security offers a "suite of technical security mechanisms aimed at inducing users in various roles to trust networked information systems and one another". Indeed the use of public key infrastructure (PKI), encryption techniques, and other clever tools do induce us to feel systems and organisations behind them are 'trustworthy' even if they may be a bank or finance house taking unnecessary risks on our behalf. The level of risk appears to be the main issue and so 'badges' of security, such as the 'padlock' on the browser window showing use of Secure Sockets Layer (SSL - a technology providing encryption of sensitive information such as name, address and credit card number), reduce the 'perceived' risk.

Many eServices 'badge' themselves with appropriate icons such as SSL, PKI, etc. and while the technology is necessary at the data level, the icon may be of as much value at the interface level in supporting user acceptance that they are in a safe place. Just as we trust the obvious security of banks based in strong buildings with cameras, guards and other paraphernalia, so we appear to be developing a kind of 'brand awareness' of digital trust and security. There are also moves to provide added assurances such as the "privacy seal"[23] in use in parts of Germany since 2000, and now being developed as a European service offering confirmation that a product conforms to specific privacy expectations (e.g. Data Protection Directive).

4.4 Trust and Identity – Co-dependencies

Although trust and security technologies can and do ensure control of access to sensitive data, our ability to determine 'who' has access is mainly limited to the 'possessor' of a card, a key, a password, or some similar 'unlocking' device. These devices do not in and of themselves prove identity.

Identity and trust mechanisms are co-dependent – knowing 'who' we are dealing with is often critical. This can mean authorities accessing 'other' information as part of a service to consider who they are dealing with (e.g. profile data), or resorting to accessing images or biometric data.

In the area of eDemocracy we are especially open to abuse of electronic identity. Ways of confirming not only the presence of access keys, but also the actual identity of the holder, are required to really open up the potential of eService in this area.

4.5 Multiple Identities – Managing Complexity

Web users often have multiple 'identities' since the must manage login / access details for numerous web sites. Similar to approaches seen in PKI etc., identities can be managed to allow a user to have a single identity whereby an agent manages access to multiple service providers. One such scheme is OpenID [24] which is a decentralized single sign-on system. When using OpenID-enabled sites, the web users need not remember authentication tokens like username and password. They only need to be registered on a site with an OpenID "identity provider". Any website can employ OpenID software as a way for their users to log in.

---

[22] H. Nissenbaum H., Will Security Enhance Trust Online, or Supplant It?. In P. Kramer and K. Cook (eds.) Trust and Distrust Within Organizations: Emerging Perspectives, Enduring Questions., Russell Sage Publications, 2004.

[23] Privacy Seal : http://www.epractice.eu/document/3682

[24] Open ID online at http://openid.net/

This basic issue is present not only in the commercial arena, but also in the domain of government services where citizens commonly have 'multiple identities' – one per service. On way to overcome that is to have a single identity per citizen, this being an "electronic identity".

5 Electronic Identity – Trends and Challenges

Electronic identity refers to any number of means of providing a 'digital' presence to enable participation in transactions where a person's specific identify must be known. Key issues include, but are not confined to, digital signature, authentication, biometric data and electronic identity cards which may integrate several of these. Recent developments in the area of trust have concentrated upon the 'identity' issue as the main problem for trust, since low level security using 'tokens' is open to abuse by anyone who can get hold of such tokens (e.g. electronic keys).

Electronic identity is not without some of the weaknesses of physical identity tokens. Credit cards could be stolen, as could any other identity token, and so 'possession' of the token (e.g. eID Card) is not necessarily proof of rights, but its inclusion of several tokens, including the owner's image (and possibly biometric data), can greatly increase certainty. Some experts also believe we need a single reliable means of ascertaining identify to reduce the complexity of citizens having 'multiple identity relationships with different government agencies' [25].

5.1 Digital Signature

A digital signature serves the same purpose as a written signature, and so is "an electronic sound, symbol, or process, attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record" (United States – Uniform Electronic Transactions Act). The same act holds that an electronic record is "a record created, generated, sent, communicated, received, or stored by electronic means", and in this act is acknowledged the necessity that an electronic signature is linked or logically associated with the record, while in the paper world the signature is placed 'upon' the document being signed.
The above definitions are useful for our purposes, and do not differ greatly from the various definitions to be found in emerging EU documents as the legislative process proceeds on this topic (e.g. [26]).

5.2 Authentication

Electronic authentication (e-Authentication) is the means and process of determining the level of confidence in claimed identities that have been presented electronically (to an e-Service). The technical challenge concerns the remote authentication of individuals engaged with e-Government online services. eServices use an authenticated identity to determine the authorisation status of a person (e.g. access a service, view data, etc.).

Token-based Authentication; Authentication and transactions normally occur over Internet, and users must first 'register' via a 'registration authority' and a 'credential service provider' to obtain a

[25] Fishenden J.. "Identity Management In An Online World". 5th European e-Government Conference, Antwerp, Belgium, June 2005.
[26] CEC 2003 - Commission Decision of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council (Text with EEA relevance) (notified under document number C(2003) 2439 - 2003/511/EC)

token (digital signature) as well as a record (registration) that links the token to a name. Authentication involves checking the token against the registration and any data entered by the citizen, and so is not unlike management of credit card payments, etc.

Knowledge-based Authentication; Here the claimant "does not need an established relationship with the relying party"[27], since identity verification is based on information associated with the claimant and previously provided by him or her. The result depends on consistency between what is 'known' by the identifier and what is provided by the claimant.

Biometric Authentication; Here, authentication is based on 'actual measures' of verifiable and highly reliable data obtained from the person (see later for fuller discussion).

These three types of authentication are in order of increasing reliability and security. Tokens are easiest to steal, and while knowledge can be obtained illegitimately it may be hard to predict what knowledge may be held, and hence asked for, in a verification system. Finally, it is almost impossible to replicate biometric data.

5.3 Electronic Identity Card (eID)

eID cards are one way to provide a citizen with a portable repository of essential information. Citizens interact with numerous organisations, departments and service systems resulting in numerous 'identities' – different logins, passwords, case numbers and so on. Identity management is a key issue for eGovernment since having a unique ID for each citizen allows cross referencing, security, avoidance of fraud, and more effective service delivery (to known profiles). For example, the Crossroads Bank in Belgium, in providing data between departments, allows a citizen with an eID card automatic access to free bus travel or free dental care when they reach the appropriate age[28].

All the many forms associated with registering, checking and declaring 'qualification' have disappeared because a person is 'known' to their authority. Countries like Estonia now have almost 100% penetration of eID cards[29], and electronic identity methods are now being tried in so many countries that the concept of 'federated identity management'[30] now requires exploration – how to reliably encode identity and exchange identity information between authorities at national and inter-national level. A number of potential solutions are looking at biometrics as the only really reliable way to ensure that our 'identity' is safe from improper use by those who can acquire or clone cards or other tokens.

Fishenden[31] looks at several example National schemes to see how they conform to the 'laws of identity'[32] and notes that different approaches are in place and require some degree of harmonisation to support a federated (European) approach supporting free movement of EU citizens.

---

[27] J. Fishenden. "Identity Management In An Online World". 5th European e-Government Conference, Antwerp, Belgium, June 2005

[28] F. Robben. CBSS: The eGov Programme of The Belgian Social Sector. Case study of the 'CrossRoads Bank'. (2007) – online at http://www.epractice.eu/cases/CBSS http://www.socialsecurity.be/ http://www.bcss.fgov.be/En/CBSS.htm

[29] ESTONIA 2007 - http://www.pass.ee/64.html

[30] A. Davoux, J-M. Crom, P Smadja, and J-P Tual. European Federated Identity Management : Key Concepts through the Fidelity Approach. In proc. eChallenges Conference, Barcelona, 2006

[31] J. Fishenden. "Identity Management In An Online World". 5th European e-Government Conference, Antwerp, Belgium, June 2005

[32] K. Cameron. The Laws Of Identity (2005 – updated 2007) : available online at http://www.identityblog.com

5.4 European Pilot on Electronic ID (EID)

As part of EU's preparation for increased citizen mobility, research pilots are envisaged to test cross border use and application of eID via the STORK project. According to the ePractice initiative "The ultimate goal of the STORK project is to implement an EU-wide interoperable system for the recognition and authentication of eIDs that will enable businesses, citizens and government employees to use their national eIDs in any Member State".[33]

5.5 Biometric Data

Biometrics involves methods for recognizing people based on physical or behavioural characteristics – actually knowing who we are dealing with as opposed to 'estimating risk'. The most common measures involve facial recognition, fingerprint recognition, iris (eye) recognition, and signature. Biometric data can be stored on an eID card and so used in transactions, service requests and occasions requiring proof of identity. Lozhnikov suggests "*Financial losses due to unauthorized access and theft of proprietary information make companies pay more attention to users' identification . . . the most promising and reliable method of identification is biometrics*"[34]. At present, handwriting recognition is quite limited in applicability, and so iris and fingerprint are gaining wider use. They are almost impossible to forge, and so provide the highest level of confidence. Cave points out that while privacy and identity are inextricably linked, "*biometrics can greatly enhance privacy, especially in comparison to the alternatives . . . we can exploit its strength to minimise false linkages or to secure access to personal data*"[35]. In routine usage of biometrics, fingerprint is probably the easiest to apply, and is least intrusive or disturbing for users.

6 Trust and Identity – Enabling Interactive Services

Trust, based on verifiable identity is becoming more widespread and, needless to say, the 'easier' technologies lead the way even if they are less secure in the long run. However, there seems to be increasing demand to move quickly towards ensuring we know exactly 'who' we are dealing with in electronic interactions.

6.1 Digital Signatures for Rapid Health Care

The Treviso Healthcare Unit in Italy[36], reports a completely digital system where digital signatures are used to support signing, transmitting, and storing clinical documents while preserving the privacy and security of healthcare data. As a result, patient clinical data are handled rapidly but only by the validating personnel and by the final users. Service delivery is greatly enhanced and yet data are more secure than in paper format since no 'casual' access is possible.

---

[33] ePractice profile of STORK : http://www.epractice.eu/document/3983

[34] P. Lozhnikov. "TEOFRAST" – A Biometric System Based on Users' Identification Through Handwriting Dynamics. In proc. eChallenges Conference, Barcelona, 2006

[35] J. Cave. Biometrics and the Bioethics of Privacy, presentation at workshop for the Nuffield Council on Bioethics, 21 February 2006

[36] R. Rigoli. Telemedicine - Electronic Signature in Care Activities for Paper Elimination. Case study of TELEMED-ESCAPE (2007) – online at http://www.epractice.eu/cases/1854

6.2 Trust Hierarchies Supported By Trusted Organisations

While the illustrative example (Spanish Government) given in section 4.2 described the problem of using multiple PKIs, the Finnish Centre For Pensions shows how an online pensions management system can be supported by PKI (trust hierarchy) and also address interoperability of security data systems by involving banks. Here the insured can use a card with PKI technology, or can opt to use the authentication technology of their own Internet bank to confirm identity[37]. This shows blending of PKI (trust hierarchy) with other forms of trust (referred trust from a trusted third party) by accepting the bank's confirmation of identity.

6.3 Domain Keys for Email Authentication

An extension of the PKI general principles is being exploited to begin addressing the problems of fraudulent email, email forgery, phishing, and other scams. It is known as Domain Keys Identified Mail (DKIM [38]), whereby the email 'trustworthiness' is judged through validation of a domain name identity by associating it with a message via cryptographic authentication. This approach involves collaboration of Alt-N Technologies, AOL, Brandenburg InternetWorking, Cisco, EarthLink, IBM, Microsoft, PGP Corporation, Sendmail, StrongMail Systems, Tumbleweed, VeriSign and Yahoo.

6.4 Trusted Parties and Inclusion of Citizens

The Belgian Social Security system is built upon a collaboration of different agencies, and is now supported by an inter-agency data exchange scheme[39]. By using common data formats and by only collecting information once – then sharing between information owners – a high level of trust has been developed within a shared data system, involving numerous Government organisation and private sector supply companies. They clearly show how they can make social service provision more effective and less wasteful, but only if monitoring of trusted parties can be effectively used to ensure conformance to regulations on 'appropriate' data usage. This activity is now being extended with the introduction of the electronic citizen identity card (eID) to further speed up transactions and Government-Citizen interactions by facilitating more citizen-centred service delivery (more active citizens).

6.5 Citizen Mobility – Information Rich Passports and ID Cards

Since the 1980's, countries around the world have been issuing machine readable passports (MRPs), which are passports with essential data presented in 'optical character recognition' format. This format allows scanning for rapid service execution, and also for automated retrieval of associated data (e.g. photograph, criminal data, etc.). Added to this, countries are also adding biometric data, and Germany was the first in Europe in 2005 to add fingerprint and facial recognition data[40]. A biometric passport stores biometric data and digital signature data in a tiny contact-less chip (e.g. RFID - radio frequency identification, as in some smart cards). While it has

[37] T. Ojala. Tyoelake – Finnish centre For Pensions. Case study of PKI usage in pension service access. (2006) online at http://www.epractice.eu/cases/218

[38] http://www.dkim.org/

[39] F. Robben. CBSS: The eGov Programme of The Belgian Social Sector. Case study of the 'CrossRoads Bank'. (2007) – online at http://www.epractice.eu/cases/CBSS http://www.socialsecurity.be/ http://www.bcss.fgov.be/En/CBSS.htm

[40] BBC (2005) News article on German adoption of Biometric passport. http://news.bbc.co.uk/1/hi/world/europe/4395726.stm

been shown that these chips can be cloned, just as mobile phone chips, the scope for copying is reduced. A future step might be to place the recognition data not on the passport, but in the terminal at the airport.

6.6 Enhanced Citizen Identification – Biometric Data

Given the limitations of data carried by the citizen, an avenue for very high level security is to place the biometric data at the disposal of authorities via networked technology. For example, people can now pass through passport control in many European airports using 'iris recognition'. Travellers registered for such a scheme (e.g. Schiphol [41], Gatwick [42], Frankfurt [43]) go to an automated barrier and look into a camera where the iris of the eye is scanned. If the system recognises them then they simply pass through. This technology stores an image of the passenger's iris patterns and their passport details together, and only people whose details have been authenticated by an immigration officer are able to use such technology[44].

6.7 Knowing the Voters – Identity in eDemocracy

In many countries it has been the tradition to send a card or paper to each registered citizen, and this card or paper then acts as a 'token' of identity in voting activities. The assumption is that the majority of law-abiding citizens will ensure that their identity is not misused, yet stories abound to show how fraudsters systematically attempt to subvert the democratic process (e.g. Birmingham, UK, 2004). In the move to e-Voting, a key challenge is to identify "*ways of solving the voting paradox of unequivocal identification of the voter yet full anonymity of the vote*"[45].

7 Monitoring Behaviours – Trust in Knowledge Owners

General concerns among citizens often centre around questions such as who needs access to personal information, why do they need it, what is done with it, when and how often. Unbeknown to most citizens, data is gathered on citizen activities on a continuous basis by both public authorities and commerce. Embedded contact-less chips (e.g. RFID), passports, car number plates, loyalty cards, and even credit-card based shopping, all add to the available mountain of data that could be, and in many cases is being, used to survey individuals, groups, and social sectors. Citizens are concerned to know when such monitoring is appropriate.

Keeping Order in Data Rich Societies

Crossroads Bank[46] shows that in order to improve efficiency they had to allow social agencies (and private partners in social service delivery) to cross-access data held by other agencies. The main driver was efficiency and cost reduction in services, but the mechanism (data interchange

[41] Privium Iris Scanning at Schiphol Airport, NL – `http://www.schiphol.nl/privium/privium.jsp`

[42] Iris Scanning at Gatwick, UK - `http://news.bbc.co.uk/1/hi/england/sussex/6664747.stm`

[43] Biometrics at Frankfurt airport - `http://news.zdnet.co.uk/emergingtech/0,1000000183,39146224,00.htm`

[44] Silicon.com (2006) Public Sector : Airport Iris Scanners http://www.silicon.com/publicsector/0,3800010403,39157104,00.htm

[45] EVOTE08 – challenges expressed in call for papers for the e-Voting 2008 conference. http://www.e-voting.cc/stories/4176263/

[46] F. Robben. CBSS: The eGov Programme of The Belgian Social Sector. Case study of the 'CrossRoads Bank'. (2007) – online at http://www.epractice.eu/cases/CBSS http://www.socialsecurity.be/ http://www.bcss.fgov.be/En/CBSS.htm

and interoperability) opens social data to new usage opportunities. External partners are monitored to ensure only 'proper' usage, but of course effective policing is, as always, limited by opportunity for audit (the problem of knowing what is done with data).

Being Known by the Unknown

In most countries financial security relies on agencies such as credit bureaus gathering information on loans, debts and transactions relative to actual persons for the purpose of analysis and prediction. In different countries there are different rules, but overall they look at payment records, control of debt, signs of responsibility and stability, etc. These are used to advise financiers who make credit enquiries. We are all 'known' at some level by agencies unknown to us.

What do Badges Say about Us?

Passive information exchange such as RFID uses transponders that can be built into badges, product labels, and other thin surfaces. They are used as badges to determine access control for workers (where they may or may not go), but can also create concerns about 'factory prisons' by tracking worker movements[47].

In a similar way, the products we buy can be automatically scanned, and other sensors can then track our movements around the marketplace or high street. The opportunity for abuse is not inherent in the technology, but is inherent in the ability of knowledge harvesters to exchange information about citizens. A company can make 'offers' to us on the basis of what is (unseen) in our shopping bag.

Shaping Citizens through Knowledge

Following on from the previous example, one class of information system (e.g. Autonomy[48]) is specifically designed to support tracking and analysis, using 'known' customer identities (via Credit card or Loyalty card) to profile citizens and so allow 'targeted' marketing. A store may offer special deals when we are shopping online because it 'knows' about us from previous purchase behaviour. This kind of 'profiling' (Meaning-Based Computing or MBC), uses deep semantics to develop usable profiles and, in concert with credit checks, can be used to develop sophisticated 'marketing pitches' for a wide range of seemingly unrelated products and services. This same approach can be used to develop semantic relationships of a socially useful kind – for example profiling citizen activities and service usage to 'predict' likely service requirements in future (e.g. medical developments, etc.).

Sharing of information between agencies within government, and between government and business partners, is not unlike what already happens in the finance area for credit checking. All of our behaviours as citizens are open to recording, especially our interactions with online services, and so our status as 'qualifiers' for services (rights), and as 'participants' (usage), are open for examination by appropriate authorities. They could use information about us not only to develop and improve services, but also to predict and plan future service provision at a personal level, and also at municipal, regional, and national levels. However, citizens might only support such developments within a reliable pact of trust and transparency.

[47] K. Robbins, and F. Webster. Times of the Technoculture: from the Information Society to the Virtual Life, London, Routledge (1999)

[48] AUTONOMY - http://www.autonomy.com/content/Autonomy/index.en.html

8 Trust in eGovernment – A Pact ?

According to the research of Simoens[49] "*Information technologies are becoming pervasive and powerful to the point that privacy of citizens is now at risk. In the Information Society, individuals want to keep their autonomy and retain control over personal information, irrespective of their activities. The widening gap on this issue between laws and practices on the networks undermines trust and threatens critical domains like mobility, health care and the exercise of democracy*". This and other similar publications offer a suggestion that unless we can find a way to show how personal and private information is being protected, through policies, legislation, and practice, citizens will continue to resist adoption of the latest information society applications in critical areas.

Concerning 'trust' in Information Theory, Ed Gerck[50] defines and contrasts trust with social functions such as power, surveillance, and accountability. This perspective, when applied to Information Society services, indicates a potential exercise of power in acquiring, storing and using personal information, while monitoring developments and activities in the lives of citizens as they unfold. Such a scenario brings with it a much greater demand for openness, honesty, conformance with citizen requirements for privacy, and real accountability for data use.

A significant initiative addressing the above issues is led by Mat Poelmans[51] whose efforts inspired and developed the so-called 'e-Citizen Charter' in the Netherlands. The Dutch e-Government policy aimed to improve interactive participation in eServices and information exchange, and they elected to use a 'partnership' between government and citizen as a key driver. A central support for that partnership is the charter - a code of conduct built around ten 'quality requirements' that in turn provide guiding principles, along with rules for creation and operation of effective e-Services. The principles and rules define the rights to choose preferred service channel, to have immediate access to easy-to-use information about citizen rights to services, and so forth. While these principles are mainly expressed as 'intention' statements in the current draft, they provide a solid basis for discussion and argumentation whenever citizens think something is amiss.

Taking openness and clear principles a step further, at least in some services, the Estonian government have arranged it that citizens can, through the use of their eID card, immediately see who has been accessing information about them and for what purpose[52].

[49] K. Simoens. Privacy and Identity Management for Europe. Case Study Report from the PRIME Project. (2006) – online at http://www.epractice.eu/cases/208

[50] E. Gerck, (1997 et seq.) Toward Real-World Models of Trust: Reliance on Received Information - http://mcwg.org/mcg-mirror/trustdef.htm

[51] M. Poelmans. The e-Citizen Charter as an Instrument to boost e-Government. In Exploiting the Knowledge Economy: Issues, Applications, Case Studies Paul Cunningham and Miriam Cunningham (Eds) IOS Press, 2006 Amsterdam

[52] EPRACTICE. (2006). Estonian eID card passes 1 million threshold. (October 23) European Commission, [cited October 25 2006]. http://www.epractice.eu/document/295

9 Summary

In order to achieve the many ambitious goals of the European Information Society, we require enhanced technologies to manage trust relationships at a distance, and at the same time accelerate our development and usage of methods for electronic identity management. Trust-based service systems are required in all areas of European society, and so our governments and citizens must together develop an agreement on the acceptable ways of gathering, storing and using data about citizens within a secure electronic service environment.

The future of electronic service provision in all European societies relies on development of a citizen-centred European trust network to underpin and facilitate the many secure electronic service networks under development at present.