Title	An assessment of biometric identities as a standard for e-government services.
Author(s)	Scott, Murray; Acton, Thomas; Hughes, Martin
Publication Date	2005-03
Publication Information	Scott, M., Acton, T., & Hughes, M. (2005). An assessment of biometric identities as a standard for e-government services International Journal of Services and Standards, 1(3), 271-286.
Publisher	Inderscience
Link to publisher's version	http://inderscience.metapress.com/openurl.asp?genre=article&eissn=1740-8857&volume=1&issue=3&spage=271
Item record	http://hdl.handle.net/10379/1693

An Assessment of Biometric Identities as a Standard for E-Government Services

Scott, Murray
Centre for Innovation & Structural Change
National University of Ireland, Galway
Direct Dial: + 353 - 91 - 512426
Fax: + 353 - 91 - 750565
email: ***murray.scott@nuigalway.ie***

Acton, Thomas
Dept of Accountancy & Finance
National University of Ireland, Galway
Direct Dial: + 353 - 91 - 512164
Fax: + 353 - 91 - 750565
email: ***thomas.acton@nuigalway.ie***

Hughes, Martin
Dept of Accountancy & Finance
National University of Ireland, Galway
Direct Dial: + 353 - 91 - 512167
Fax: + 353 - 91 – 750565
email: ***martin.hughes@nuigalway.ie***

Abstract

This paper investigates the applicability and potential use of biometrics for E-Government services. An in-depth case study is presented outlining the development of E-Government services in Ireland, highlighting potential areas for growth in biometrics and also areas for caution in the implementation of the underlying technologies. Biometrics is becoming an important international standard as an authentication technology providing cross-border immigration and security controls; however, the case for biometrics in e-government services is more complex. As an enabler of e-services, the implementation of this technology is challenged by a wider set of more profound societal issues including, citizen privacy, security and trust. However, the rapid development and adoption of this technology has the potential to inform and hasten its diffusion into wider e-government usage. Specifically, this paper examines the current attitudes to the feasibility of biometrics as a component in the delivery of E-Government services.

1. Introduction

Governments are using the Internet and E-Commerce technologies to provide public services to their citizens [1, 2]. In so doing, governments aim to form better relationships with businesses and citizens by providing more efficient and effective services [3-6]. E-Government provides unparalleled opportunities to streamline and improve internal governmental processes, enable efficiencies in service delivery, and

improve customer service [7, 8]. As a result, achieving successful e-government delivered over the Internet has become a key concern for many governments [9, 10]. Additionally, there are privacy, security, and trust issues for citizens interacting with Government services compounded by the electronic nature of the interaction. Biometric identifiers may present a solution to some of these concerns, leading to increased levels of secure, private, and trusted E-Government interactions [11].

However, there are trade-offs between the usage of such identifiers, not only with their technological effectiveness, but also with the range of biometric solutions and anticipated investment benefits. Indeed, the successful implementation of biometrics is also challenged by a number of factors: end-user perceptions of potential transgressions into personal privacy; lack of choice in accepting such technologies for particular services; perceived trust in the technology and the usage of collected data; and sensitivity to existing data protection laws. Not withstanding these challenges, biometric identities may be a necessary standard for personal identification as a gateway through which to access internet-delivered e-government services.

2. E-Government Challenges

The Internet can be used to provide access to centrally stored data to support services and transactions. Such centralised data storage can help the efficient running of government and provide convenient services to citizens. However, the permanent storage of confidential and personal data present significant security challenges [12, 13]. International data protection reforms recommend security measures to protect sensitive information, and in doing so present potential restrictions for government agencies on the usage of data in transactions and the storage of citizen information [11]. Strategic choices are therefore required regarding how information is made available for transactions, how long it can be stored for, and how that information can be used.

With E-Government, citizens are exposed to threats to data privacy and the security of information, similar to those encountered in an E-Commerce environment. Privacy, security and confidentiality are thus natural concerns for businesses and citizens in this context [3, 14]. Many citizens may feel that their privacy is threatened if personal data is stored centrally. Furthermore, the design of e-systems may also deter some citizens from using the electronic medium, preferring the familiarity of traditional physical interactions [15]. These factors necessitate the building of trust between citizens and government to ensure successful levels of adoption of Internet-based e-government services [5, 16].

Trust needs to be established in the ability of systems acting as interfaces to E-Government services to provide security to resist external attacks, maintain the confidentiality of the information stored and prevent the threat of fraud [17]. With E-Government services often requiring citizens to provide highly personal information, there has been an increase in the potential of technology to provide reliable means of user identification and provide security for government information systems [11, 18, 19]. In particular the development of biometrics has ignited widespread interest by citizens, businesses and Governments, on how these technologies operate and the implications of their usage. In addition the development of new technologies has the potential to develop citizen trust by offering advanced levels of security [11, 17].

3. Biometrics

Biometrics is the application of computational methods to biological features, especially with regard to the study of unique biological characteristics of humans

[20]. As an emerging technology, biometrics offers two related and important capabilities: first, the reliable identification of an individual from the measurement of a physiological property, which provides second the ability to control and protect the integrity of sensitive data stored in information systems [21]. All biometric technologies share the same underlying processes: all operate either in verification (authentication) mode or in a recognition (identification) mode. A verification system authenticates a person's identity by comparing the captured biometric characteristic with the person's own biometric 'original'. In this system a person who desires to be identified submits a claim to an identity usually via a magnetic-stripe card or smart card, and the system either accepts or rejects the submitted claim of identity. In a recognition system, the system establishes a subject's identity by searching the entire template for a match, without the subject initially claiming an identity.

As the levels of worldwide information system security breaches and transaction fraud increase, the imperative for highly secure authentication and personal verification technologies becomes increasingly pronounced. Oppliger [21] highlights the significance of this issue, arguing that concerns about security problems have already begun to chill the overheated expectations about the Internet's readiness for full commercial activity. Governments are concerned about user verification and system security in developing E-Government services particularly with moves towards combined, seamless services, which are delivered electronically. As a result the potential benefits of biotechnologies, in particular identification issues and security, are gaining importance on political agendas for E-Government development (UK Government Strategy Unit, 2002).

3.1 Biometrics and Authentication

Primarily there exist three general categories of authentication with respect to electronic systems: 1) PINs (Personal Identification Number) or passwords, 2) Keys, smart cards, or tokens, and 3) Biometrics [22]. Passwords are by far the most commonly used means of authentication in information systems [23]. However this authentication technique is often insecure, as users tend to choose passwords that are easily guessed or breakable by hackers [24]. Jain et al. [25] describe token-based security and verification approaches as physical entities an individual possesses to make a personal identification, such as a passport, a driver's license, ID card, and so on. Such identification entities are currently widely used as methods of authentication for numerous applications world-wide. However, Ratha et al. [26] argues that advances in computer technology now mean that the process of biometric authentication can be automated, and unlike token- or password-based methods, physiological characteristics cannot be lost or stolen.

As the dependency on global and organisational information systems continues to grow, Bradner [24] argues that the level of sophistication in authentication should ideally be in proportion to this reliance. Biometrics has the capability to respond to this demand, with the most common developments occurring in automatic facial recognition, iris recognition, retinal biometrics, hand geometry, voice recognition and fingerprint imaging. As a result a range of biometric technologies are becoming the foundation of an extensive array of highly secure identification and verification solutions, suitable for both commercial and governmental use, as evidenced by the range of biometric trials currently underway by various nations.

3.2 Current Biometric Trials

Driven both rapidly and almost exclusively by US reforms to immigration control, biometrics has been forced onto political agendas internationally, hastening the implementation of this technology. Several European countries have started to update their border control policies incorporating the use of biometrics: as an example, in early 2002 the British government began issuing asylum seekers with identifying smart cards storing two fingerprints. General plans to extend the use of biometric technology throughout the UK visa system have also been announced [27], and similar plans have been unveiled in France, Germany and Italy. Indeed the Australian Customs Service (ACS) has revealed a biometric passport recognition pilot scheme at Sydney Airport as a precursor to a nationwide implementation of the system, where it is testing the SmartGate facial recognition system for passport verification on Qantas staff at that airport in the first phase of a project expected to lead to nationwide usage across all international air travellers [28]. Elsewhere, the Japanese government plans to introduce biometric features in passports in an effort to tackle illegal immigration and to enable tighter controls on terrorists: passports will be introduced with an embedded computer chip storing a biometric feature such as a fingerprint or a facial scan [29]. Finally, Bulgaria has announced the introduction of a collection of fingerprint- and iris-scan biometric identifiers at its border controls, to be completed by the end of 2004 [30]. As such, planned and in some instances piloted implementations of biometric technologies are well underway across various nations, pioneering these relatively new technologies in the provision of services.

4. Emerging Issues in Biometric Adoption

Biometrics is an emerging technology: there are a number of implementation issues pertinent to its widespread development and diffusion. Furthermore the lack of international biometric standards together with privacy and security concerns are relevant as potential inhibitors affecting the growth, deployment, and effective delivery of E-Government services. However, recent international developments, for example the US visa waiver scheme, have put biometrics on numerous political agendas in the context of enabling E-Government, and have consequently fuelled rapid growth in interest in biometric technologies over recent years.

4.1 International Standards

Due to the relative youth of biometric technologies, as well as the fragmented nature of the biometric industry, a lack of international standards has impeded many types of biometric implementation and has slowed the growth of the biometric industry [31]. In order to gain acceptance in both commercial and Government environments, biometric devices must meet widely accepted industry standards, which in turn would stimulate increased funding and developments in the industry [31, 32]. The development of standards would reduce the implementation and development risks of biometric solutions, making their deployment more attractive to risk-averse Government-run public sector environments.

4.2 Privacy Concerns and Trust

Biometric technologies have the potential to provide governments and other organisations with increased power over individuals, thus threatening personal entitlements and civil liberties [33]. As such, privacy concerns are an important consideration in successful biometric implementation and uptake amongst citizens.

These privacy issues relate to data collection, unauthorised use of recorded information, and improper access and errors in data collection [34]. Biometric technologies have the potential to be more privacy invasive in cases where it involves the storage of personal information without the knowledge or consent of the individual [35]. In relation to online access to data however, Clarke [13] paradoxically highlights the need for technological development, as there is currently no inherently correct and absolutely accurate method of ensuring an individual's identity, or indeed protecting the integrity of collected and recorded data.

Trust is a central defining aspect of many social and economic interactions; it is the belief that others will behave in a predictable manner [5]. In E-Government, threats to data privacy and the security of information necessitates the building of trust between citizens and government to ensure successful adoption levels of E-Government services [5, 16]. Specifically, trust should be developed in e-services to allay fears that information collected for one purpose is not used for secondary purposes without prior authorisation from the individual, and to ensure the non-repudiation of services [36]. Governments also have an interest in developing trust in electronic transactions as enabling mechanisms require the capability to uniquely identify the individual to prevent fraud. One potential mechanism to create trust is to provide the citizen with the ability to have some control over the information stored during E-Government transactions with the individual, and who or which Government department can access it [3]. An important development in this regard is the progression of international data protection laws and guidelines that govern the use, collection and storage of citizen data.

4.3 International Data Protection

The development of data protection legislation has been progressed by the European Union through directives in 1998 and 2002 and has subsequently been incorporated into legislation in member countries through the use of legislative bills. The purpose of EU directives in this context is to protect data privacy by ensuring that the individual is aware of the type and detail of data stored about them, and explicitly gives consent to the usage of their personal data. The challenge for European member states is to incorporate these directives relating to improvements in service quality, social inclusion and data protection principles into an overall strategic framework for implementing E-Government that combines legislative requirements with the need for high quality customer service.

4.4 Range of Biometric Technologies

An 'ideal' biometric should be universal, where each individual possesses the characteristic; unique, where no two persons should share the characteristic; permanent, where the characteristic should neither be changed nor alterable; and collectable, the characteristic is readily presentable to a sensor and is easily quantifiable (Jain et al., 2000). In attempts to satisfy these requirements, a diverse and varied range of different biometric technologies have available, such as those mentioned earlier: from recognition-based scanning systems measuring iris and retinal patterns, fingerprint layout and hand geometry constitution, to methods that gauge the accuracy of human sense-based output, such as voice patterns and olfactory sensing. Whilst consistent and rapid technological development has centred on only a subset of the available methods of biometric verification and personal identification, some methods may, in the context of E-Government service provision, be more suitable for the implementation of particular applications which in themselves may be

performance-specific, and be more acceptable to citizen perceptions in offering the best overall 'fit' in the inclusion of concerns regarding privacy and security.

4.5 External Influences on Biometric Growth

In 2002, the United States Congress passed the "Enhanced Border Security and Visa Entry Reform Act ", which mandates that, as of October 26, 2004, US authorities must issue machine-readable visas and other travel and entry documents using biometric identifiers, and that only countries having a programme to issue their nationals with machine-readable passports incorporating biometric identifiers will remain eligible for the visa exemption programme. After October 26, 2004, a foreigner seeking to enter in the US under the visa waiver program will thus have to present a biometrically inclusive machine-readable passport, otherwise a digital picture and fingerprints will need to be recorded upon entry. The US Department of Homeland Security launched in May 2003 a programme designed to implement this legislation, called "U.S.Visitor and Immigrant Status Indication Technology " (US-VISIT). As a result of the new US border control policy, the countries currently eligible for the visa exemption programme, including all current EU countries, must therefore set up a programme to issue their nationals with biometric passports [37].

Countries such as Australia and Japan have already begun biometric implementations for passport recognition: in particular Australia's Sydney airport is pioneered facial recognition scanning at passport control checkpoints, a measure which if successful will initiate a resultant roll-out to other airports. Japan has indicated intentions to embed biometric features on computer chips incorporated into physical passports, whereas Bulgaria intends to introduce fingerprint and iris scan biometric identification at border controls in a measure to address crime and identity fraud, and as a strengthening measure to tighten existing immigration controls. Biometric identifiers, through necessity based on various countries' concerns over immigration, terrorism, and other factors, are becoming more prolific in personal identification and verification.

5. Research Methodology

Exploratory research methods were used to investigate the applicability and potential use of biometrics for E-Government services and to examine the current attitudes to the feasibility of biometrics as a component in the delivery of E-Government services in Ireland. In particular, a qualitative in-depth case study approach was adopted, as this has been identified as most appropriate for understanding contemporary social phenomena in its natural context and in particular for the study of new phenomena [38-42]. Furthermore, the case study method is particularly appropriate for description and theory development, supported by an interpretive approach [43-47].

In 2001, the Irish Government set up a Biometric Task Force, under the auspices of the Department of Communications, Marine, and Natural Resources (DCMNR), to consider the use of biometrics technology in the delivery of Government services. The terms of reference of the Biometrics Task Force were as follows:

> *"To identify government, civil service and other public sector platforms, where biometric and associated technologies can be utilised effectively to produce outcomes including but not confined to the more efficient delivery of services to clients, increased attractiveness of service delivery to clients, improved security of government and public*

sector installations and buildings, and e-delivery of Government services."

To assess Governmental attitudes towards biometric services and the underlying biometric technologies available to enable these services, we conducted four in-depth structured interviews, each of 30-45 minute duration, with management personnel working in the area of biometrics in the DCMNR and management personnel within the Irish Government's Biometric Task Force. These interviews occurred in April 2002. The questions in the interviews were largely open, and posed with sufficient time and approach that facilitated discussion. These interview questions, together with the purposes of each question, are provided in Appendix 1. Given the complexity of the research domain a variety of data sources have also been collected and used in the course of the research process, allowing for a richer insight into the research context [48]. Complementing the interviews mentioned above, supplementary data sources included two report documents produced by the Irish Government's Biometric Task Force (one from 2002, the other from 2003), and informal discussions outside of interview contexts with management working in the area of biometrics in the DCMNR and within the Biometric Task Force.

6. Case Study

6.1 Developing a Framework for E-Government Services

In June 2003, the European Council stated that a coherent approach is needed in the EU for the standardisation of biometric identifiers. In response to requirements of the European Commission, the development of a European Biometrics Forum has been implemented in Ireland. This forum is composed of leading privacy, technology and usability experts. Through the contribution of its research, this forum has the potential to overcome the current fragmentation of biometrics providers with respect to standards, foster inter-operability amongst such providers, and develop agreement on international standardisation. In 1999, the Irish Government released its first action plan on the Information Society; this plan made specific reference to the need to develop e-government initiatives and outlined an initial commitment to e-enable the delivery of public services. In March 2002, the Irish government further committed itself to placing all appropriate services accessible via the Internet by 2005 [Government of Ireland, 49]. The central strategic thrust of the government was to make better use of the Internet for service access and provision in order to gain radical improvements in the quality of service to customers; major improvements in administrative efficiencies and enhanced control of fraud and abuse of publicly funded services.

The concept of a portal based Public Service Broker (PSB) was subsequently adopted as the central mechanism for delivering the e-government agenda, as this was identified as the most efficient model to provide mediated, citizen-centred services. The model of the entry point was designed to provide a mechanism to coordinate government service providers and to manage the various interactions with resource providers in delivering a service. In turn the entry point provided the ability to combine and restructure those services around the needs of citizens. The PSB supports multiple delivery channels in order to ensure that all citizens have access to E-Government services; the government is further committed to the rapid development and diffusion of Internet access to citizens through education and the

investment in appropriate infrastructure to enable all citizens the benefit of online services and resources [Government of Ireland, 49].

An online prototype of the PSB known as 'reachservices', was officially launched and implemented in 2002. A tendering process has also been completed for the construction of the full version of the PSB. A complete installation of the PSB is planned to be implemented by 2005.

6.2 Potential Role for Biometrics

At present, user authentication on reachservices is limited to a user name and password provided by the Government. As part of the procurement process for the construction of the PSB however, the use of biometrics has been included as a mandatory feature for development. In order to provide more sophisticated security for user identification and verification, biometric identifiers are highlighted as an essential component of the services intended for the PSB. To ensure the inclusion of this feature in the design of the PSB, prospective tenders have been required to provide evidence of the following capabilities: the development of authentication protocols and methods to support biometrics and the necessary in-house expertise to develop the usage of technologies such as biometrics.

6.3 A Regulatory Framework for Biometrics

The Irish government has progressed data protection legislation in line with EU recommendations, to govern how citizens can be identified and to define and govern how citizen data can be used by service agencies. The Irish government's commitment to data protection is evidenced by the legislative acts that have recently been implemented: Data Protection Act (1998), EC (Data Protection and Privacy in Telecommunications) Regulations (2002) and the Data Protection (Amendment Bill) (2002). The concept of a single unique identifier (termed a 'PPS number', that is, a Personal Public Service number), which is compulsorily allocated to all citizens at the registration of a birth, was motivated by the need to uniquely identify citizens and in response to EU directives, to provide the citizen with the ability to decide *what* information is stored about them and to determine the conditions of that information's usage.

Various legislative procedures have also been progressed to support the introduction of biometrics in facilitating and enabling E-Government services. For example, The Social Welfare Act 2002 provides for the creation of a Public Service Identity (PSI), which consists of the PPS number and associated identity data. This act allows for the inclusion and legal recognition of biometric data as part of the PSI identity data set. In turn the PSI is intended to act as the key component of registration and authentication used by the PSB.

7. Findings

With respect to electronic, biometric-involved citizen-to-Government interactions, findings encompass Governmental views on issues related to privacy, security, and trust, both from planning and implementation standpoints. Although the development of Governmental policy governing the use of biometrics in Ireland is at an early stage, there have been a number of distinct areas of growth. Specifically these areas recognize the potential role for a range of biometric technologies as enablers of public service delivery. Table 1 presents a summary of the major findings of this study

together with our interpretations: these findings are expanded upon in the sections that follow.

Finding	**Interpretation**
Implemented biometrics must be accurate	Biometric technologies should significantly increase the accuracy of personal identification measures already in use or adaptable from other applications to e-Government services.
Strong forms of authentication methods are necessary for e-Government provision. As such, Biometric technologies are a necessary authentication measure	Inherent in the effective provision of usable e-Government services is a dependable and effective authentication process.
Biometrics are an important component in the provision and delivery of e-Government services, in addition to other applications	Biometric technologies are fundamental to the effective interaction between citizen and state inherent in the secure handling and execution of e-Government services. Biometric identifiers are also appropriate for other applications, such as driving licenses and health-related matters.
Biometric implementations for e-Government must address privacy and citizen trust	Biometric systems should not become a de-facto standard for personal identification without consideration of citizen perceptions and attitudes towards potential infringements into privacy. Potential biometric implementations for e-Government services should use a framework that encompasses both privacy and trust as components central to effective deployment and acceptance.
The Irish Government needs to be aware of internationally external factors influencing advances in biometric deployments	The adoption and usage of various biometric technologies are heavily influenced by international politics, such as concerns over immigration, terrorism, requiring accurate means of user identification. The Irish Government must be cognizant of biometric developments in other countries, so that Irish systems equivalent to international measures of personal identification are not 'lagging'. Also, the Irish Government needs to be aware of technological advances in some forms of biometric technologies over others, spurred by external factors, which could impact upon the methods and tools used in Ireland to provide electronic Government

Table 1 Findings and Interpretations of Findings

7.1 Privacy, Security, and Trust

Results of interviews with members of the DCMNR and the Biometric Task Force indicate that to effectively provide citizens with secure electronic access to public services and indeed for E-Government to be successful, it is imperative that the underlying systems can instantly and accurately validate the claimed identity of any

individual. Furthermore, there was consensus that a strong form of authentication, such as those facilitated via biometric methods, is a key enabler in the delivery of online public services.

In terms of privacy and trust, the interviews suggest that the Irish Government should not try to impose biometric technology on citizens, but that a challenge exists to develop reliable high-trust biometric mechanisms for citizens to interact securely and privately with e-services in through well-planned, well-designed, usable and non-threatening implementations that are tuned with existing legislation on data privacy and access. Findings here indicate that the deployment of biometric technologies facilitating E-Government provision should not result in citizens feeling that their Government are overreaching themselves in terms of invasion of their personal privacy.

Interviewees also stressed the influence of external factors, such as the measures initiated by U.S., U.K. and other Governments regarding security and immigration controls post September 2001, as key to recent increases in interest in biometric technologies, their uses and their potential. These interviews suggest that the Irish Government must not only be aware of developments in relation to international biometric standards, but additionally that the Irish Government should monitor the current situation in relation to the use of biometric technologies to ensure that Irish citizens will not be excluded from international or EU-based e-services because their Government has not kept pace with international policy and developments.

7.2 Areas of Biometric Usage in Ireland

In recognition of the significant international developments in security and immigration control, the Department of Foreign Affairs is in the process of reviewing the design of Irish passports with a view to incorporating biometric data. This Department is closely monitoring the international debate on biometric use in passports to ensure that prompt action can be taken when international agreement is reached.

The Road Haulage Division (RHD) of the Department of Transport is in discussions with EU counterparts as to the feasibility of using biometric technology to ensure the integrity of a tachograph system. The RHD is concerned that companies comply with regulations governing the maximum hours drivers can work. Biometric driver validation would enable inspectors to establish the link between the driver in the cab and the driver logged in to the tachograph during inspections, thereby improving compliance and road safety.

The Department of Social and Family Affairs has currently progressed sophisticated modes of authentication to identify applicants for welfare benefit. Through the progression of the Social Welfare Act 2002 and the legal enactment of the PSI data set, the Department is further in a position to enhance the level of security authentication through the use of biometric identifiers. The Department also has a critical interest in tracking decisions relating to the award of benefits and to ensure that awards are not repudiated by officials working on particular cases. In this instance the application of biometrics has a potential role to promote citizen trust by recording the input of a deciding officer in any given case thus ensuring the non-repudiation of services.

This research has identified biometrics as an important component in the provision and delivery of a comprehensive set of public services. For example, special provision has been made in the design of the PSB to accommodate biometric

identifiers for certain services requiring advanced levels of security, such as passport applications. In the delivery of services, citizen access will include call centres and walk in offices where an official will assist the citizen in availing of a service. In these cases, the use of biometrics could generate a non-reputable audit trail by creating a record of the assent of the citizen to a transaction and the participation of the official. Such mechanisms could help promote the acceptability of these alternative service delivery channels.

Other areas that have been identified as appropriate for the application of biometrics are driving licenses and the health sector. The driving license is considered to be particularly susceptible to forgery, as it contains only an identity photograph and signature. Biometric data could significantly enhance its value for identification purposes, especially given the recent introduction of a penalty points system, which further motivates the need to link a driving license with its rightful owner. Some hospitals in Ireland are assessing the feasibility of using a biometric application to record clinical events in the development of clinical audit procedures. Recording the presence of healthcare workers or their participation along a clinical decision trail or treatment history are possible applications that could significantly enhance review systems in hospitals, which in turn could assist in maintaining the confidence of patients and other stakeholders.

7.3 Range of Biometric Technologies

The range of potential biometric technologies being considered for differing situations to support the provision of services has an important impact on the likely success of the implementation effort. The task force identified that each technology has particular strengths and weaknesses and as such no single technology is likely to suit all applications. The two variables that influence the implementation of biometrics in the public domain were identified as a) public perception of the technology, and b) performance of the technology. Fingerprint scanning was identified as being the most accurate technology, however it has the lowest public acceptance rate given the associations with criminality. The technology with the highest level of public acceptance is facial scanning, however this is the weakest performing technology, as there are difficulties in distinguishing between similar facial images. The technology that satisfies both public perception and performance criteria is iris scanning. This application does not require physical contact and is accurate; currently trials are underway at U.K.'s Heathrow and the Netherlands' Schipol airport under the auspices of these countries' Governments.

8. Discussion and Conclusions

Increased security concerns associated with global terrorism are currently driving the need for biometric enhanced passports as the standard, minimum documentation required for international travel. As a result, citizens will have little choice but to participate in biometric identification schemes, as determined by their passport issuing authority. This situation will provide governments, many for the first time, with the ability to uniquely identify an individual citizen solely on the basis of some physiological property. Given the fact that in most developed countries a very high percentage of citizens hold passports, it will be tempting for governments to extend the use of biometric technology beyond passport identification. While the implementation of biometrics to e-government services offers many advantages for both citizen and government alike, the extended use of biometric identifiers needs to be carefully evaluated.

Although there are significant security risks in implementing e-government services, the potential to improve internal government processes and provide better quality public service is an opportunity many governments are willing to pursue. In this study, some critical factors have been highlighted relevant to the implementation of biometric identities as a necessary enabler of e-services. Public acceptance of the technology is imperative for although strong forms of authentication have been shown to be a prerequisite for effective e-service provision, the deployment of biometric technologies must be cognizant of a number of issues. Biometric mechanisms must not only be reliable and user friendly but also appropriate to the service. An indiscriminate application of biometrics to government services may exacerbate public fears that personal privacy is being unnecessarily compromised. Hence, a central question in the context of utilising biometrics in E-Government service provision is the extent of verification deemed necessary and appropriate to access a particular service. The issue of implementing biometrics is further complicated by the need to adhere to strict EU laws on data protection, which protect data integrity but also challenge the design and operation of authentication mechanisms.

As a rapidly developing technology there is also an imperative for Governments to keep pace with innovations in biometric development to ensure that national interests are not compromised. In particular there have been a number of potential areas that biometrics can be of use in the Irish context and further a number of different options in the range of available technologies. Since the range of technologies also confer differing advantages in implementation, an informed choice is essential not only to ensure that the benefits of this technology are realised but that the type of technology is appropriate to the service.

The use of biometric technologies by governments is being accelerated by technological developments and the need for increased security. However, while it will become beneficial for governments to use biometric identification procedures outside the realm of international travel and associated security issues, such an extension needs careful consideration. Further research into citizen acceptability, and citizen trust of biometric identifiers would add significantly to the current debate on biometric usage.

References

1. Gouscos, D., et al., *Re-orientating Information Systems for Customer Centric Service.* In the Proceedings of the First European Conference on E-Government, 2001.
2. Watson, R.T. and B. Mundy, *A strategic perspective of electronic democracy.* Communications of the ACM, 2001. **44**(1): p. 27.
3. Layne, K. and J. Lee, *Developing fully functional E-government: A four stage model.* Government Information Quarterly, 2001. **18**(2): p. 122.
4. Al-Kibisi, G., et al., *Putting citizens on-line, not inline.* The McKinsey Quarterly, 2001. **Special Edition**(2): p. 64.
5. Warkentin, M., et al., *Encouraging Citizen Adoption of e-Government by Building Trust.* Electronic Markets, 2002. **12**(3): p. 157.
6. Davidrajuh, R., *Planning e-government start-up: a case study on e-Sri Lanka.* Electronic Government, 2004. **1**(1): p. 92-106.
7. Bannister, F. and N. Walsh, *The virtual public servant: Ireland's public services broker.* Information Polity: The International Journal of Government & Democracy in the Information Age, 2002. **7**(2/3): p. 115.

8. Heeks, R., ed. *Reinventing Government in the Information Age: International Practice in IT enabled public sector reform*. 1999, Routledge: London.
9. Li, F., *Implementing E-Government strategy in Scotland: current situation and emerging issues.* Journal of Electronic Commerce in Organizations, 2003. **1**(2): p. 44-65.
10. Eyob, E., *E-government: breaking the frontiers of inefficiencies in the public sector.* Electronic Government, 2004. **1**(1): p. 107-114.
11. Dearstyne, B.W., *E-Business, e-Government & Information Proficiency.* Information Management Journal, 2001. **34**(4): p. 16.
12. DeConti, L., *'Planning and Creating a Government Web Site: Learning from the Experience of the USA' Information Systems for Public Sector Management*, in *Working Paper Series No. 2, Institute for Development Policy and Management*,. 1998, University of Manchester.
13. Clarke, R. *Electronic Services Delivery: From Brochure-Ware to Entry Points*. in *12th International Electronic Commerce Conference*. 1999. Bled, Slovenia.
14. Tambouris, *European cities platform for online transaction services: The euro city project.* In the Proceedings of the First European Conference on E-Government, 2001.
15. Jupp, V. and S. Shine, *Government portals - the next generation of government online.* In the Proceedings of the First European Conference on E-Government, 2001: p. 217-223.
16. Bellamy, C. and J.A. Taylor, *Governing in the Information Age*. 1998, Buckingham: Open University Press.
17. Dridi, F., *Security for the electronic governent.* In the Proceedings of the First European Conference on E-Goverment, 2001: p. 99-111.
18. Carrick, K., *E-Government - Lessons to be learned from e-Business experience.* European Conference on E-Government, 2001: p. 91-99.
19. Horton, F.W., *The message of the medium; The risks and opportunities of migrating pre-electronic government information products to the Internet.* Journal of Government Information, 2001. **28**(1): p. 1-20.
20. Hopkins, R., *An Introduction to Biometrics And Large Scale Civilian Identification.* Computers & Technology, 1999. **13**(3).
21. Oppliger, R., *Internet Security: Firewalls and Beyond.* Communications of the ACM, 1997. **40**(5).
22. Liu, S. and M. Silverman, *A Practical Guide to Biometric Security Technology*. 2002, http://www.findbiometrics.com/Pages/lead.html.
23. Furnell, S.M., et al., *Authentication and Supervision: A Survey of User Attitudes.* Computers & Security, 2000. **19**(6): p. 529-539.
24. Bradner, S., *But will they pay attention this time?* Network World, 1997. **14**(4): p. 32-34.
25. Jain, A., L. Hong, and S. Pankanti, *Biometric Identification.* Communications of the ACM, 2000. **43**(2).
26. Ratha, N., J. Connell, and R.M. Bolle, *Enhancing security and privacy in biometric based authentication systems.* IBM Systems Journal, 2001. **40**(3): p. 614-635.
27. UKPS, *Biometrics British Passports*. 2004, http://www.ukpa.gov.uk/identity.asp.
28. ENN, *The Australian Customs Service (ACS)*. 2004, http://www.enn.ie/.

29. EBF, *Japanese government set to introduce biometrics*. 2004, http://www.eubiometricforum.com/index.php?option=content&task=view&id=122&Itemid=2.
30. EBF, *Bulgarian government announces introduction of biometric identifiers at border controls*. 2004, http://www.eubiometricforum.com/index.php?option=content&task=view&id=124&Itemid=2.
31. Nanavati, S., M. Theime, and R. Nanavati, *Biometrics: Identity Verification in a Networked World*, ed. J.W. Sons. 2002: Wiley Computer Publishing.
32. Ryman-Tubb, N., *Combating Application Fraud.* Credit Control, 1998. **19**(11/12).
33. Clarke, R., *Biometrics and Privacy*. 2001, http://www.anu.edu.au/people/Roger.Clarke/Cnotice.html.
34. Smith, S., J. Milberg, and S. Burke, *Information Privacy: Measuring Individuals' Concerns about Corporate Practices.* MIS Quarterly, 1996. **20**(2): p. 167-196.
35. Crompton, M., *Biometrics and Privacy: The End of the World as we Know it or The White Knight of Privacy*. 2002, http://www.biometricsinstitute.org/bi/cromptonspeech1.htm.
36. Tolchinsky, P., et al., *Employee perceptions of invasion of privacy: A field simulation experiment.* Journal of Applied Psychology, 1981. **66**(3): p. 308-313.
37. IDA, *E-Government News*. 2003, http://europa.eu.int/ISPO/ida/egovo: European Commission.
38. Galliers, R.D., *Choosing Information Systems Research Approaches.*, in *Information Systems Research: Issues, Methods and Practical Guidelines*, R.D. Galliers, Editor. 1992, Blackwell Scientific Publications, Oxford.: Oxford. p. 144-162.
39. Stake, R.E., *The Art of Case Study Research*. 1995, Thousand Oaks, CA: Sage Publications.
40. Stake, R.E., *Case Studies*, in *Handbook of Qualitative Research*, N.K. Denzin and Y.S. Lincoln, Editors. 2000, Sage: Thousand Oaks. p. 435-455.
41. Yin, R.K., *Research Design Issues in Using the Case Study Method to study Management Information Systems*, in *The Information Systems Research Challenge: Qualitative Research Methods*, J.I. Cash and P.R. Lawrence, Editors. 1989, Harvard Business School Press: Boston. p. 1-7.
42. Yin, R.K., *Case Study Research: Design and Methods*. 2nd ed. 1994, Newbury Park: Sage Publications.
43. Myers, M.D., *Dialectical hermeneutics: a theoretical framework for the implementation of information systems.* Information Systems Journal, 1994. **5**(1): p. 51-70.
44. Klein, H. and M. Myers, *A Set of Principles for Conducting and Evaluating Interpretative Field Studies in Information Systems.* MIS Quarterly, 1999. **23**(1): p. 67-94.
45. Orlikowski, W.J. and J.J. Baroudi, *Studying Information Technology in Organizations: Research Approaches and Assumptions.* Information Systems Research, 1991. **2**(1): p. 1-28.
46. Cavaye, A.L.M., *Case study research: a multi-faceted research approach for IS.* Information Systems Journal, 1996. **6**(3): p. 227-242.

47. Benbasat, I., D.K. Goldstein, and M. Mead, *The Case Research Strategy in Studies of Information Systems.* MIS Quarterly, 1987. **5**(4): p. 369-386.
48. Darke, P., G. Shanks, and M. Broadbent, *Successfully completing case study research: combining rigour, relevance and pragmatism.* Information Systems Journal, 1998. **8**(4): p. 273-289.
49. Ireland, G.o., *New Connections: Action Plan for the Information Society*. 2002, Government of Ireland.

Appendix 1

Case Study Interview Questions and Question Purposes

Question	Text of Question	Purpose(s) of Question
1	Why might the Irish Government support biometric technologies?	• To identify the central applications which biometric technologies can enable and benefit, in particular to identify public service and other Government-related applications • To identify any economic or other factors influencing Government support for biometric technologies and implementations
2	What regulations will the Irish Government need to put in place to govern the use biometric technologies?	• To explore the legislative effect of the usage of biometric technologies on existing country-specific laws • To explore the necessity of regulatory frameworks dealing with biometric usage
3	How will the use of biometric technologies affect the relationship between citizen and government?	• To explore and identify the barriers related to successful biometric implementations
4a, 4b, 4c	a) Are there citizen concerns regarding the use of biometrics? b) If so, what are these concerns? c) How can these concerns be addressed?	• To identify the central concerns for citizens with respect to biometric implementations, in particular concerns related to privacy, security, and trust
5	How can the use of biometric technologies improve the delivery of public services for citizens?	• To explore how biometric technologies can enable the electronic provision of services to citizens
6	What other biometric-related issues are	• To provide interviewees with an opportunity to discuss other factors

	important, which we haven’t discussed?	associated with biometrics in e-Government