223

Biometric Identities and E-Government Services

Murray Scott
Dept. of Accountancy & Finance
National University of Ireland, Galway
murray.scott@nuigalway.ie
+ 353 - 91 - 512426
Fax: + 353 - 91 - 750565

Séamus Hill
Dept. of Accountancy & Finance
National University of Ireland, Galway
seamus.hill@nuigalway.ie
+ 353 - 91 - 495232
Fax: + 353 - 91 – 750565

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

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

Biometric Identities and E-Government Services

Keywords: e-government, biometrics, e-commerce, Internet, services, authentication, security, privacy, trust.

INTRODUCTION

Governments are using the Internet and E-Commerce technologies to provide public services to their citizens (Watson & Mundy, 2001). In so doing, governments aim to form better relationships with businesses and citizens by providing more efficient and effective services (Al-Kibisi, de Boer, Mourshed, & Rea, 2001). E-Government provides opportunities to streamline and improve internal governmental processes, enable efficiencies in service delivery, and improve customer service (Bannister & Walsh, 2002). As a result, achieving successful e-government delivered over the Internet has become a key concern for many governments (Eyob, 2004). 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.

BACKGROUND

E-Government Challenges

The Internet can be used to provide access to centrally stored data to support services and transactions and 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 (DeConti, 1998). 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 (Dearstyne, 2001).

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 (Layne & Lee, 2001). Furthermore, the design of e-systems may also deter some citizens from using the electronic medium, preferring the familiarity of traditional physical interactions (Jupp & Shine, 2001). These factors necessitate the building of trust between citizens and government to ensure successful levels of adoption of Internet-based e-government services (Bellamy & Taylor, 1998).

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 (Dearstyne, 2001; Dridi, 2001).

Biometrics

Biometrics is the application of computational methods to biological features, especially with regard to the study of unique biological characteristics of humans (Hopkins, 1999). 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 (Oppliger, 1997).

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. 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).

Biometrics and Authentication

Three general categories of authentication exist with respect to electronic systems: 1) PINs (Personal Identification Number) or passwords, 2) Keys, smart cards, or tokens, and 3) Biometrics (Liu & Silverman, 2002). Passwords are the most commonly used means

of authentication in information systems (Furnell, Dowland, Illingworthand, & Reynolds, 2000). However this authentication technique is often insecure, as users tend to choose passwords that are easily guessed or breakable by hackers (Bradner, 1997). Jain et al. (2000) 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 worldwide. However, Ratha et al. (2001) argues that the process of biometric authentication can be automated, and unlike token- or password-based methods, physiological characteristics cannot be lost or stolen.

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.

As a result of the "Enhanced Border Security and Visa Entry Reform Act " and new US border control policy, countries currently eligible for the visa exemption programme, including all current EU countries, must set up a programme to issue their nationals with biometric passports (IDA, 2003). European countries which have started to update their

border control policies incorporating the use of biometric authentication include; the UK (UKPS, 2004), Bulgaria(EBF, 2004a), France, Germany and Italy. In Australian the Customs Service (ACS) has revealed a biometric passport recognition pilot (ENN, 2004). Elsewhere, the Japanese government plans to introduce biometric features in passports (EBF, 2004b).

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 (Nanavati, Theime, & Nanavati, 2002). 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 (Nanavati et al., 2002; Ryman-Tubb, 1998). 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.

Privacy Concerns and Trust

Biometric technologies have the potential to provide governments and other organizations with increased power over individuals, thus threatening personal

entitlements and civil liberties (Clarke, 2001). As such, privacy concerns are an important consideration in successful biometric implementation and uptake amongst citizens. These privacy issues relate to data collection, unauthorized use of recorded information, and improper access and errors in data collection (Smith, Milberg, & Burke, 1996). 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 (Crompton, 2002).

Trust is a central defining aspect of many social and economic interactions; it is the belief that others will behave in a predictable manner. 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 (Bellamy & Taylor, 1998). 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 authorization from the individual, and to ensure the non-repudiation of services (Tolchinsky et al., 1981). Governments also have an interest in developing trust in electronic transactions, since electronic mechanisms require the capability to uniquely identify the individual to prevent fraud.

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 become available 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.

BIOMETRICS FOR E-GOVERNMENT SERVICES IN IRELAND

Background

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. In order to assess Governmental attitudes towards biometric services and the underlying biometric technologies available to enable these services, four in-depth structured interviews were conducted with management personnel working in the area of biometrics in the DCMNR and management personnel within the Irish Government's Biometric Task Force. 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.

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. 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, 2002).

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 (Government of Ireland, 2002). 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 and a complete installation of the PSB is for 2005.

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.

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.

Key Issues in Biometric Implementation

With respect to electronic, biometric-involved citizen-to-Government interactions, the key issues influencing successful biometric implementation encompass Governmental views on 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 number of key principles for successful implementation of biometrics and a description of the challenge each presents.

Principle	Description
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	Biometric technologies are fundamental to the effective interaction between citizen and state inherent in the secure handling and execution of e-

services, in addition to other applications	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 Principles for Biometric Implementation

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, 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.

FUTURE TRENDS

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.

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. 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.

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 cognisant 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.

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:

Al-Kibisi, G., de Boer, K., Mourshed, M., & Rea, N. (2001). Putting citizens on-line, not inline. *The McKinsey Quarterly, Special Edition*(2), 64.

Bannister, F., & Walsh, N. (2002). The virtual public servant: Ireland's public services broker. *Information Polity: The International Journal of Government & Democracy in the Information Age, 7*(2/3), 115.

Bellamy, C., & Taylor, J. A. (1998). *Governing in the Information Age*. Buckingham: Open University Press.

Bradner, S. (1997). But will they pay attention this time? *Network World, 14*(4), 32-34.

Clarke, R. (2001). *Biometrics and Privacy*. Retrieved April, 2003, from http://www.anu.edu.au/people/Roger.Clarke/Cnotice.html

Crompton, M. (2002). *Biometrics and Privacy: The End of the World as we Know it or The White Knight of Privacy*. Retrieved April, 2003, from http://www.biometricsinstitute.org/bi/cromptonspeech1.htm

Dearstyne, B. W. (2001). E-Business, e-Government & Information Proficiency. *Information Management Journal, 34*(4), 16.

DeConti, L. (1998). *'Planning and Creating a Government Web Site: Learning from the Experience of the USA' Information Systems for Public Sector Management.* University of Manchester.

Dridi, F. (2001). Security for the electronic governent. *In the Proceedings of the First European Conference on E-Goverment*, 99-111.

EBF. (2004a). *Bulgarian government announces introduction of biometric identifiers at border controls*

EBF. (2004b). *Japanese government set to introduce biometrics*

ENN. (2004). *The Australian Customs Service (ACS)*

Eyob, E. (2004). E-government: breaking the frontiers of inefficiencies in the public sector. *Electronic Government, 1*(1), 107-114.

Furnell, S. M., Dowland, P. S., Illingworthand, H. M., & Reynolds, P. L. (2000). Authentication and Supervision: A Survey of User Attitudes. *Computers & Security, 19*(6), 529-539.

Hopkins, R. (1999). An Introduction to Biometrics And Large Scale Civilian Identification. *Computers & Technology, 13*(3).

IDA. (2003). *E-Government News*

Ireland, G. o. (2002). *New Connections: Action Plan for the Information Society*: Government of Ireland.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric Identification. *Communications of the ACM, 43*(2).

Jupp, V., & Shine, S. (2001). Government portals - the next generation of government online. *In the Proceedings of the First European Conference on E-Government*, 217-223.

Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly, 18*(2), 122.

Liu, S., & Silverman, M. (2002). *A Practical Guide to Biometric Security Technology*. Retrieved February, 2004, from http://www.findbiometrics.com/Pages/lead.html

Nanavati, S., Theime, M., & Nanavati, R. (2002). *Biometrics: Identity Verification in a Networked World*: Wiley Computer Publishing.
Oppliger, R. (1997). Internet Security: Firewalls and Beyond. *Communications of the ACM, 40*(5).
Ratha, N., Connell, J., & Bolle, R. M. (2001). Enhancing security and privacy in biometric based authentication systems. *IBM Systems Journal, 40*(3), 614-635.
Ryman-Tubb, N. (1998). Combating Application Fraud. *Credit Control, 19*(11/12).
Smith, S., Milberg, J., & Burke, S. (1996). Information Privacy: Measuring Individuals' Concerns about Corporate Practices. *MIS Quarterly, 20*(2), 167-196.
Tolchinsky, P., McCuddy, M., Adams, J., Ganster, D. C., Woodman, R. W., & Fromkin, H. L. (1981). Employee perceptions of invasion of privacy: A field simulation experiment. *Journal of Applied Psychology, 66*(3), 308-313.
UKPS. (2004). *Biometrics British Passports*
Watson, R. T., & Mundy, B. (2001). A strategic perspective of electronic democracy. *Communications of the ACM, 44*(1), 27.

Key terms:

Portal: the provision of integrated services, combining personalisation features, via the Internet.

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

Biometric Identifiers: the use of biometric data to enable the reliable identification of an individual from the measurement of a physiological property which provides the ability to control and protect the integrity of sensitive data stored in information systems

Authentication/Identification: biometric identifiers 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 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.

Trust: the provision of adequate measures to ensure the security of private or sensitive data thus providing confidence in the reliability of electronic services.

Privacy: measures or regulations created to protect the individual in relation to data collection, unauthorised use of recorded information, and improper access and errors in data collection.

Fingerprint scanning: enables the identification of an individual based on the analysis of unique patterns and ridges found in a fingerprint.

Iris scanning: enables the identification of an individual based on the analysis of the coloured tissue surrounding the pupil.

Speech recognition: enables the identification of an individual based on the analysis of a

‘voiceprint’ derived from the digital acquisition of unique patterns found in individual speech patterns.