Category: Concepts, Trends, and Challenges

Biometric Identities and E-Government Services

Murray Scott
National University of Ireland, Galway, Ireland

Séamus Hill
National University of Ireland, Galway, Ireland

Thomas Acton
National University of Ireland, Galway, Ireland

Martin Hughes
National University of Ireland, Galway, Ireland

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, Hong, and Pankanti (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, Connell, and Bolle (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 U.S. 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 U.S. border control policy, countries currently eligible for the visa exemption program, 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 Australia, 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.