Chapter 89
Trends in Government e-Authentication:
Policy and Practice

Mike Just
Glasgow Caledonian University, UK

Karen Renaud
University of Glasgow, UK

ABSTRACT

Government engagement of its citizens through digital channels offers the potential for efficiencies and savings, while at the same time allowing the government to reach out to constituents in novel ways. Yet such endeavours must be undertaken with care, especially with personalised service delivery, which requires effective management of security and privacy. Proper authentication and management of identity are key related factors. In this chapter, the authors examine government use and adoption of e-authentication and identity management technologies in order to securely interact with citizens. They first provide some background in which the state-of-the-art for protecting and managing identities is reviewed in terms of the various methods studied in academia and marketed by industry. The chapter then describes the degree to which these methods have been, and continue to be, used in the e-government initiatives of several developed countries. Finally, the authors consider the lessons learned, and how they might be applied to similar initiatives in developing countries.

INTRODUCTION

As governments look to reduce costs and improve efficiency, many turn to interacting and engaging their citizenry online. In the simplest incarnation, offering such online services might involve the provision of documents and information in digital form, reducing the need for physical government sites that would otherwise provide such information in person, as well as reducing costs related to travel to government offices, printing paper documents, etc. Personalized government services are more advanced, allowing users to add, view, or change information about themselves and their

DOI: 10.4018/978-1-4666-1740-7.ch089

relationship with their government. In addition to the aforementioned efficiencies, such services additionally strive for building a fuller, interactive relationship between government and the citizens they represent.

With a vision of a more efficient and engaged government with personalized information and services for citizens comes the increasing need to protect any gathered information and to be seen to do so. In offering such services, *identity* becomes a key factor whereby the *management of identity* of individuals accessing these services becomes a critical requirement. Such factors are key to ensuring participation from citizenry by ensuring the delivery of *trustworthy* services (Carter and Bélanger, 2005).

The main objective of this chapter is to highlight the challenges that a government of a developing country might face in performing identity management as part of their e-government services to citizens. E-authentication is an integral component of identity management, and is the focus of this chapter. We build toward this objective by first reviewing the various means of e-authentication and identity management in use today, based upon their academic study, or as solutions marketed today by industry. We then examine some examples of e-authentication used in several countries in the developed world for their e-government initiatives. Finally, we present the lessons learned and provide some guidance for e-government initiatives to support the unique circumstances of delivering secure e-government services in developing countries.

BACKGROUND

An identity is a collection of characteristics by which a person is defined, recognized, or known. It includes information such as their name, their date-of-birth, as well as other information about themselves, their preferences and behaviours, etc. Since names are not unique a particular character string is often used as a unique identifier, which allows us to refer to the identity without enumerating all of the personal data. In some countries a national identity number serves this purpose, in others a combination of name, birthdate and address suffices.

Traditionally, in the physical world, identities are validated by means of trusted tokens such as a driver's license or birth certificate. These are issued by a trusted entity and support verification of someone's claim to a particular identity. Some of the tokens now being used to verify identity, such as a driver's license, were originally intended to represent a privilege, establishing the permission to operate a motor vehicle (Pato, 2005) but their use has been extended to verification, or authentication, of identity too.

A *digital identity* is the corresponding concept in the digital world. In cases of (digital or physical) identity changes, such as a change of address, the changes need to be managed to ensure accuracy and consistent distribution. *Identity management* refers to the set of processes, tools, and social contracts surrounding the creation, maintenance, and termination of a digital identity for people or, more generally, for systems and services, to enable secure access to an expanding set of systems and applications (Pato, 2005).

Traditionally, identity management has been a core component of system security environments where it has been used for the maintenance of account information for login access to a system or a limited set of applications. An administrator issues accounts so that resource access can be restricted and monitored. Control has been the primary focus for identity management. More recently, however, identity management has exploded out of the sole purview of information security professionals and has become a key enabler for electronic interactions of all kinds, including e-government.

Mirroring the physical world, the digital identity requires a unique identifier. A person will tender this identifier in order to make use of personalized services online. The identity will then