EXECUTIVE SUMMARY

This is an eGISE network article. It is motivated by a concern about the extent to which trust issues inhibit a citizen’s take-up of online public sector services or engagement with public decision and policy making. A citizen’s decision to use online systems is influenced by their willingness to trust the environment and agency involved. This project addresses one aspect of individual “trust” decisions by providing support for citizens trying to evaluate the implications of the security infrastructure provided by the agency. Based on studies of the way both groups (citizens and agencies) express their concerns and concepts in the security area, the project will develop a software tool—a trust verification agent (TVA)—that can take an agency’s security statements (or security audit) and infer how effectively this meets the security concerns of a particular citizen. This will enable citizens to state their concerns and obtain an evaluation of the agency’s provision in appropriate “citizen friendly” language. Furthermore, by employing rule-based expert systems techniques, the TVA will also be able to explain its evaluation.

Keywords: citizens; e-government; trust

ORGANISATION BACKGROUND

With over 90% of United Nations member countries now operating government Web sites (Swartz, 2004), it is imperative that citizens engage in the process to maximise public investment in e-government systems and services. Although e-government is still a relatively new phenomenon, it shares similar characteristics with the fields of e-commerce and e-business in terms of the use and implementation of Internet technology; re-engineering inter, and intra-organisational processes and structures; and generating new services, products, and channels for the end users or consumers (Shackleton, Fisher, & Dawson, 2004). Expectations of e-government by both government and citizens emanate
from the example of the private sector’s implementation and use of e-commerce and e-business and are drivers for its adoption and use. Customers (or citizens) now expect the same level and type of service from government that they receive from the private sector, while government itself anticipates increased efficiency, productivity improvements, and cost savings similar to those experienced by the private sector (Clark, 2003; Stamoulis, Gouscos, Georgiadis, & Martakos, 2001). But despite these similarities, e-government is unique because of its role in the interaction between government and its citizens and the governance of nations (Finger & Pecoud, 2003). It is a complex mix of a variety of issues such as social inclusion and political engagement, management of change and innovation, integration and standardisation of information technology, and information systems, legal, ethical and political responsibilities. While individuals still have concerns about security and privacy issues using commercial Web sites, there is even more of a concern over security and privacy for citizens engaging electronically with public services (McDowell, 2002).

In order for e-government to achieve its ambitious objectives of being able “(1) to develop and deliver high quality, seamless, and integrated public services; (2) to enable effective constituent relationship management; and (3) to support the economic and social development goals of citizens, businesses, and civil society at local, state, national, and international levels” (Grant & Chau, 2005, p. 9), citizens need to engage with the e-government process. The aim of this research is to explore citizen engagement in e-government in a security context, dealing with the different stakeholder perspectives on issues of security, trust, and authentication.

**SETTING THE STAGE**

The major aim of this article is to present the case for building a trust verification agent (TVA) to bridge the gap in interpretation of security information between e-government service providers and citizens. This article defines e-government and the context in which the TVA will operate, which involves both citizen facing front-end and back-end e-government services. A review of the literature and empirical studies on e-government identifies the criteria for adoption of e-government from a citizen and government perspective, which highlights trust and security as major factors. An examination and classification of trust models for e-commerce and government are consolidated to define trust and security in the context of this project. Having established that security and its dissemination to citizen users of e-government service is an important factor in building trust, the concept of the trust verification agent is presented. The TVA will provide citizens with the ability to judge the level of security provided by an e-government application. This will enable them to take critical decisions about their ability to trust the service and increase citizen take-up of services. Technical descriptions of the security infrastructures are complex and difficult for the citizen to understand and this project will bridge the gap by developing an independent TVA that can translate these descriptions into appropriate language for the citizen.

The majority of e-government empirical studies published by practitioners such as Accenture, and international organisations such as the UN and OECD, focus on descrip-