Chapter 4.42
Certificate Management Interoperability for E–Government Applications

Andreas Mitrakas
European Network and Information Security Agency (ENISA), Greece

ABSTRACT

Secure e-government aims at supporting public administration in delivering enhanced public services. In e-government, electronic signatures and certification services are used to invoke trust and security in services and applications. Certification services, however, are often on offer in an apparent geographical or contextual isolation threatening to create new fault lines across e-government services that rely on them. As public administration often operates at multiple levels and in a compartmental manner, the risk is that limitations in the interoperability of certification services might hamper trust and security in the whole value chain of e-government. Drawing from the case of small public administrations, this chapter proposes a certification service architecture and approach to support interoperability in secure e-government services.

INTRODUCTION

The promise of e-government for a simplified and efficient Public Administration (PA) has been regarded by governments worldwide as a means to carry out public policy and enhance services to citizens and organisations. E-government aims at introducing to public administration, information, and communication technologies (ICT) at a mass scale in a way previously unknown and for tasks often impossible to carry out without ICT. Online citizens and organizations gain access to 24/7 services over an array of transactions with the PA and often in combination with private sector or other third party services. Cross-border interoperability is a critical aspect in delivering such services. Electronic signatures are an infrastructure technology upon which e-government applications rely to ensure authentication and non-repudiation of transactions. While electronic

authentication is often associated with identity management, non-repudiation is essential for critical e-government applications that require the undisputed commitment of the signatory. Using electronic signatures in cross-border transactions across multiple application environments may become an awkward experience due to interoperability limitations that may lead to setbacks in trust. It is therefore becoming critical to allow for the seamless validation of electronic signatures in multiple application environments. This chapter addresses certain issues related to certification authority (CA) services across e-government infrastructures and it reviews prevailing models to assess their suitability for interoperability in e-government. Emphasis is placed on the suitability of these models for applications made available by e-government organizations, particularly small ones that typically rely on limited resources that cannot necessarily sustain demanding deployments in terms of technology used and organisational cost. In building trusted e-government services, grasping the trust requirements of each application is an essential prerequisite. Since trust is likely to be based on certificate-based services, ensuring interoperability across the board is a priority for administrations in the Member States but also for the European Union (EU) in an effort to enhance interoperability and encourage cross-border deployments. After providing a short overview of the state of art, the remainder of this chapter presents existing interoperability models. Furthermore, this chapter presents a proposed interoperability model that leverages on an overarching interoperability capability.

BACKGROUND: TRUST AND E-GOVERNMENT

While the EU E-Europe initiative has focused on government services online, seamless access to government information services and decision-making procedures have also been seen as a priority (Prins, Eifert, Girot, Groothuis, & Voermans, 2001). The envisaged application environment for e-government seeks to meet the expectations of citizens and businesses alike especially with regard to providing efficient and cost effective e-government services (UNCTAD, 2001). Applications of e-government aim at citizens and business with varying levels of involvement and service functionality. These applications may often rely on electronic signatures to safeguard the transmission of user and transaction data. Online e-government services that leverage upon electronic signatures for citizens include for example: taxation, social security, registration services, etc. Typical e-government applications that require the identification of organisations include social security contributions, corporate tax, VAT submissions, company registries, and electronic public procurement. More recently, the set up of official registries such as those required for accountants and companies, also rely on the use of electronic signatures. In certain areas a drive toward greater cooperation among PAs can be observed, that is often motivated by the need to service a larger population in the EU internal market or leverage upon a greater range of services. In some cases, cooperation may also be instantiated by interactions at a political level that have led to successful deployments, like for example, the European Digital Tachograph (see, Council regulation (EC) No 2135/98 of 24 September 1998 amending Regulation (EEC) No 3821/85 on recording equipment in road transport and Directive 88/599/EEC concerning the application of Regulations (EEC) No 3820/84 and (EEC) No 3821/85). As it can be expected in complex transaction areas such as electronic procurement, a combination of technologies and a multitude of interoperability options have to be taken into consideration to allow for the seamless cooperation among PAs and provide appropriate interactions with private sector services. In such environments, PA processes may require re-designing to ensure interoperability and accessibility.

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/certificate-management-interoperability-government-applications/9862

Related Content

Policy Factors Influencing Reduction of HIV/AIDS Stigma in Tanzanian Local Government Authorities
R. W. Kisusu, H. N. Menda, S. P. Magembeand E. M. Nyaonge (2014). *Governometrics and Technological Innovation for Public Policy Design and Precision (pp. 218-231).*
www.irma-international.org/chapter/policy-factors-influencing-reduction-of-hivaids-stigma-in-tanzanian-local-government-authorities/101274

A Secure and Efficient Scheme for Remote Poll Station Voting
Vinodu Georgeand M. P. Sebastian (2013). *International Journal of Electronic Government Research (pp. 75-91).*
www.irma-international.org/article/a-secure-and-efficient-scheme-for-remote-poll-station-voting/103894

Electronic Democracy at the American Grassroots
Donald F. Norris (2005). *International Journal of Electronic Government Research (pp. 1-14).*
www.irma-international.org/article/electronic-democracy-american-grassroots/2002

G2C Adoption of E-Government in Malaysia: Trust, Perceived Risk and Political Self-Efficacy
Ramlah Hussein, Norshidah Mohamed, Abdul Rahman Ahlan, Murni Mahmudand Umar Aditiawarman (2010). *International Journal of Electronic Government Research (pp. 57-72).*
www.irma-international.org/article/g2c-adoption-government-malaysia/45741

Implementation of Information and Communications Technologies for Financial Inclusion in Programs to Alleviate Poverty in Brazil, Colombia and Mexico
Judith Mariscaland César Rentería (2013). *E-Government Success around the World: Cases, Empirical Studies, and Practical Recommendations (pp. 105-130).*
www.irma-international.org/chapter/implementation-information-communications-technologies-financial/76636