Chapter 12
Attribute Hierarchies to Tally Fish

Andreas Mitrakas
European Network and Information Security Agency (ENISA)

ABSTRACT

This chapter presents a model that addresses some shortcomings associated with limitations in the way that electronic identities are used in an application environment. This model, Snowflake, allows the exchange of validation data in order to establish trust when identity attributes are used in applications. Snowflake leverages upon groups of validation authorities as electronic intermediaries to facilitate application interoperation. The application area of choice is the electronic reporting of fish catches by a vessel's master in line with the European Union legal framework. Grouping together the services of multiple validation authorities maximises the utilisation of resources available especially in environments that do not shy out in sharing resources and data such and the electronic fish logbook provides a good platform in this respect.

INTRODUCTION

Electronic identity management has emerged as the lynchpin of various eGovernment applications that depend on user authentication. Electronic identities based on electronic signatures allow the identifying, authenticating and ensuring the non-repudiation and integrity of a transaction. Electronic identity management also allows users to act under a role in environments where a multifunctional approach

is necessary. Attributes can be leveraged upon to come up with identity services in areas where there is a need to link a user with a role rather than with its real life identity. The growing use of electronic identity technologies in disparate groups of users has also highlighted the need for interoperability at the application level in order to allow for better diffusion of the benefits associated with these transactions. As applications grow in what is often perceived as isolated contexts, it is often necessary to ensure efficient application management by leveraging upon data sets generated in these isolated

contexts. Snowflake is an architecture that allows the exchange of information in order to establish trust in an electronic identity management based on a validation centric model. The remainder of this paper addresses the following areas: an overview of interoperability and identity, some considerations on an electronic identity model based on intermediaries and Snowflake, a model that enhances interoperability through a specific business process that relies on grouping together validation authorities.

The remainder of this Chapter describes the background of identity management upon which eGovernment services build. The use of attributes is described in the context of extending their functionality in a way that allows for carrying out performative transactions. To allow the interoperation of attribute hierarchies to interoperate, an interoperability architecture based on the validation of attribute certificates is discussed in a way that permits the interoperability of multiple validation authorities. This attribute validation model is set up against the transactions background of the electronic fish logbook, in line with the prevailing legal framework in the European Union. This Chapter claims that (a) attributes can replace fully fledged identities where it is not necessary or desirable to reveal fall or most identity elements in due consideration of privacy or the requirements of a transaction; (b) additionally a validation centric interoperability model can provide an alternative to interoperable certification authorities, the policy criteria of which might be a challenge to reconcile; (c) discreet policy environments and formal applications and transactions such as the electronic fish logbook can benefit from the functional interoperability allowed under the proposed certificate validation model in a way to facilitate European Union policies in terms of functional cooperation in discreet areas of public services.

INTEROPERABILITY IN MANAGING IDENTITIES

Interoperability is the ability of products, systems, or business processes to work together in order to accomplish a common task. While interoperability is a technical consideration it typically serves business needs by interlinking otherwise disparate systems that need to be leveraged together in order to deliver a common service. In eGovernment processes interoperability addresses such considerations as how information is used or exchanged in the various public administration applications, which parties have access to certain types of information and how information is presented to various types of end users that might belong to different contexts. Factors that contribute to determining the ability of a system to interoperate with others include the way a system is built, trade secrets and potential shortcomings in aligning with other peer systems. As a measure to contain such shortcomings user communities and government agencies have set up their shared interoperability structures like for example e-GIF in the UK, SAGA in Germany, IDABC at European Union level etc. Sometimes eGovernment services have been based on seemingly isolated and unrelated computerized applications that have overlapped in function and content within public organizations, thus resulting in relatively isolated islands of technology (Eymeri, 2001; Janssen & Wagenaar, 2004). This approach has clashed with the concept of information systems that had been viewed as an integral part of public services (Janssen & Wagenaar, 2004). In the specific case of electronic identification eGovernment, interoperability has emerged as a requirement for the provision of shared services in terms of authentication and non repudiation of public acts and systems use. Such shared services can eventually help organizations make available recurrent, pattern-based services to serve large populations of users. To facilitate large deployments service oriented architectures help the orchestration of eGovernment services

Related Content

Review for Region Localization in Large-Scale Optical Remote Sensing Images
Shoulin Yinand Lin Teng (2022). *The International Journal of Imaging and Sensing Technologies and Applications (pp. 1-12).*
www.irma-international.org/article/review-for-region-localization-in-large-scale-optical-remote-sensing-images/306654

Designing Mobile Learning Smart Education System Architecture for Big Data Management Using Fog Computing Technology
Muhammad Adnan Kaim Khani, Abdullah Ayub Khan, Allah Bachayo Brohiand Zaffar Ahmed Shaikh (2022). *The International Journal of Imaging and Sensing Technologies and Applications (pp. 1-23).*
www.irma-international.org/article/designing-mobile-learning-smart-education-system-architecture-for-big-data-management-using-fog-computing-technology/306653

Calibration and Measurement of Signal Strength for Sensor Localization
Neal Patwariand Piyush Agrawal (2009). *Localization Algorithms and Strategies for Wireless Sensor Networks: Monitoring and Surveillance Techniques for Target Tracking (pp. 122-145).*
www.irma-international.org/chapter/calibration-measurement-signal-strength-sensor/25582

Designing Mobile Learning Smart Education System Architecture for Big Data Management Using Fog Computing Technology
Muhammad Adnan Kaim Khani, Abdullah Ayub Khan, Allah Bachayo Brohiand Zaffar Ahmed Shaikh (2022). *The International Journal of Imaging and Sensing Technologies and Applications (pp. 1-23).*
www.irma-international.org/article/designing-mobile-learning-smart-education-system-architecture-for-big-data-management-using-fog-computing-technology/306653

LEAP Enhanced: A Lightweight Symmetric Cryptography Scheme for Identifying Compromised Node in WSN
Maleh Yassineand Abdellah Ezzati (2020). *Sensor Technology: Concepts, Methodologies, Tools, and Applications (pp. 753-779).*
www.irma-international.org/chapter/leap-enhanced/249590