Available online at www.sciencedirect.com

ScienceDirect

Materials Today: Proceedings XX (2016) XXX–XXX

materialstoday: PROCEEDINGS

www.materialstoday.com/proceedings

PMME 2016

Conceptual model for identity management to mitigate the database security of the registry civil of Ecuador ⋆

Moisés Toapanta[a], Enrique Mafla[b], José Orizaga[c]*

[a]*Systems Engineering Career, Universidad Politécnica Salesiana Ecuador, Robles 107 y Chambers, Guayaquil, P.O. Box 09014, Ecuador*
[b]*Faculty of Engineering Systems, Escuela Politécnica Nacional, Ladrón de Guevara E11-253, Quito, Pichincha, P.O. Box17012759, Ecuador*
[c]*Information Systems Departament CUCEA, Universidad de Guadalajara, Periferico Norte # 79, Zapópan, Jalisco, P.O. Box 45100, México*

Abstract

Were Analyzed different conceptual models that apply identity management for authentication, authorization, auditing (AAA) with confidentiality, integrity and availability (CIA) to mitigate information security. Is considered Organic Law of Identity Management and Public Data issued by the National Assembly of Ecuador. The aim is to develop a conceptual model to determine the organizational structure and define security levels in the next phase to develop or adopt algorithms and security protocols. Used deductive method was in exploratory research to verify trends in security models. It was the conceptual model for identity management for civil registration of Ecuador in a distributed environment. It was determined the flow of information, identifying the user roles and permission, the prototype of the conceptual model to identify vulnerabilities in the security of information.

Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

Keywords: Identity management models; Conceptual models; Security; Authentication; Authorization; Confidentiality; Integrity.

* Corresponding author. Tel.: +593-04-2590630; fax: +593-04-2590630 Ext. 4618.
E-mail address: stoapanta@ups.edu.ec (M. Toapanta), enrique.mafla@epn.edu.ec (E. Mafla), jorizaga@cucea.udg.mx (J. Orizaga)

Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

1. Introduction

The Directorate General of Civil Registry and Identification of Ecuador is part of the National System of Public Data that is authorized to provide information to the people to different public and private organizations as an agency: Internal Revenue Service, National Electoral Council, National Secretary Education Science Technology and Innovation, Ministries, International Organizations, agencies authorized by the competent authorities. The information available is inconsistent has serious problems of confidentiality, integrity and availability for this reason requires a management system identification authentication, authorization and auditing[1].

For the above and considering that the information is strategic; The National Assembly of the Republic of Ecuador in the Official Gazette Supplement 684 of February 4, 2016 creates the Organic Law of Identity Management and Civil Data in Art. 6 Lit.2 says: Promote, in coordination with the governing body science, technology and innovation and other public and private institutions, scientific and technological research to strengthen the management of identity and civil registry data[2]. For this reason as a doctoral student in Information Technology at the University of Guadalajara; at this stage a prototype of a conceptual model of identity management for civil registration of Ecuador in a distributed environment develops. In the next phase is to develop or adopt algorithms and security protocols to apply this model will be the basis to mitigate information security.

Because it is necessary to create a model of identity management to mitigate information security of civil registration?

To mitigate security information database of civil registration of Ecuador in accordance with the provisions of the Organic Law of Identity Management and Data Civil.

Objective is to create a prototype of a conceptual model of identity management for civil registration of Ecuador in a distributed environment; applying authenticity, authorization, auditing with confidentiality, integrity and availability.

The articles analyzed regarding the issue at this phase are:

Chapter 1 - General Security Concepts: Access Control, Authentication, and Auditing BT - Security+ (Second Edition)[3], New Authorization Tracks: Role-Based Access Control and Digital Rights Management[4], Identity Management and Access Control From A Perspective Organizational[5], Usage and Impact of Model-Based User Authorization[6], Differentiating user authentication graphs[7], Digital Identity Management [8], ZEBRA: Zero-effort bilateral recurring authentication[9], Evaluation of the Conceptual Model for Corporate Identity Management in Health Care[10], Security Controls and Services[11], Security solution frames and security patterns for authorization in distributed, collaborative systems[12], Chapter 5 – Risk Management[13], Grid authentication from identity-based cryptography without random oracles[14], Adding Enterprise Access Management to Identity Management[15].

The deductive method to review and analyze the information referenced to identify the application of identification, authentication, authorization, auditing (IAAA) and confidentiality, integrity and availability (CIA) to mitigate information security in an organization applies.

The results obtained in this phase is the flow of information in general, object permissions / operations *Prototype of a conceptual model of identity management for civil registration of Ecuador in a distributed environment*; which determines the levels of technical, physical and administrative security using authentication, authorization, auditing, confidentiality, integrity and availability of information.

It is concluded that the information flow is based on the types of users who access the information to create, update and query information. The identification of users, roles and permissions to mitigate information security. The prototype of a conceptual model of identity management for civil registration of Ecuador in a distributed environment helps identify the different levels of technical, physical, administrative security with their respective levels of identification, authentication, authorization (AAA), confidentiality, integrity and availability (CIA).

1.1. Relate Works

These objectives include having a working knowledge of the concepts of access control, authentication, and auditing (AAA). These concepts are widely used to support the concept of confidentiality, integrity, and availability (CIA). It is discovered that there are three distinct methods of providing access control. Mandatory access control (MAC) is rules that are defined and hard-coded into operating systems and applications to allow or deny access to services or applications. In the case of discretionary access control (DAC), the user or service that owns an object, such as a file, has control of who or what else has the ability to access the file or object, and at what level. The chapter explores the capabilities of role-based access control (RBAC)[3], One of them is support for role-based access control management, using a technology called the authorization manager and a brand-new API—the authorization API. Authorization manager is a fundamental shift in Microsoft's way of dealing with access control enforcement and management[4], The model identity management using authentication, authorization and auditing (AAA) confidentiality, integrity and availability (CIA) mitigates the vulnerability of information in organizations that have large databases, applications, systems and have a high demand for local users, network, web, corporate to achieve unified management of the lifecycle of identities, allocation and appropriate designation of controls access to resources and efficient allocation of roles, for reducing operational burdens, collection timely information, diminution technical and financial costs[5], Projects identity management is a major challenge for organizations. Not because of the technical complexity of the projects, but due to the fact that the management of access to resources and services involves a deep understanding of the responsibilities of the organization, workflow and processes. The integration of the organic layer is achieved through the seamless integration of project data model for process optimization. Conceptual models carry the knowledge of the structure of an organization and its processes. The presented approach is not limited to the technical level and therefore allows a high degree of automation. The aim of this work is to give a first positive answer to this question and provide a way to automatically generate a useful option to configure identity management systems based on semi-formal models[6], Authentication using centralized methods is a primary trust mechanism within most large-scale, enterprise computer networks. This paper proposes using graphs to represent user authentication activity within the network[7], Privacy rights with authentication and authorization can be done with technology. Contribute and obtain information, and emerging technologies, which use communicating objects (radio frequency identification (RFID), sensors, smartdust, etc.) to provide future solutions for facilitating everyday life. This development creates issues concerning the application of legal provisions, particularly concerning the collection, use and transmission of personal data[8], Common authentication methods based on passwords, tokens, or fingerprints perform one-time authentication and rely on users to log out from the computer terminal when they leave. Users often do not log out, however, which is a security risk. The most common solution, inactivity timeouts, inevitably fail security (too long a timeout) or usability (too short a timeout) goals. To address this problem we propose Zero-Effort Bilateral Recurring Authentication (ZEBRA). In ZEBRA, a user wears a bracelet (with a built-in accelerometer, gyroscope, and radio) on her dominant wrist. When the user interacts with a computer terminal, the bracelet records the wrist movement, processes it, and sends it to the terminal. In our experiments ZEBRA performed continuous authentication with 85% accuracy in verifying the correct user and identified all adversaries within 11s. For a different threshold that trades security for usability, ZEBRA correctly verified 90% of users and identified all adversaries within 50s[9], This paper reflects findings from the evaluation of the conceptual model for corporate identity management in health care developed by Rutitis and Batraga (2013).[10], Controls and security services. The principles of safety control describes the general requirements and objectives for technical controls, which are recommended as part of risk mitigation. These principles include: fault condition, modularity, standardization, compartmentalization, balanced operational constraints, and default settings. Considering as principles authentication, authorization and auditing to protect information confidentiality, integrity and availability[11], The design of an authorization infrastructure is one of the most important aspects of engineering a secure software system. Unlike other system types, distributed systems - and especially distributed collaborative systems - can require custom, fine-grained authorization models and enforcement approaches that are able to take into account a range of semantic subtleties. We illustrate and evaluate the proposal in the context of greenfield system development by applying our solution frames to design the authorization infrastructure of a (new) distributed system for secure file sharing and collaborative editing; and also use our solution frames to briefly analyze and capture the design decisions underlying two existing distributed

authorization infrastructures: one based on UCON for collaborative Grid systems and another based on ZBAC for SOA-based systems[12], Risk management and looks at the critical success factors and risk components of information security. Addresses the issue of risk assessment and risk management. It also covers the need for a management system of information security and a series of functions is analyzed, responsibilities[13], This article mentions the importance of authentication, authorization through to primary key that in one or another way mitigates security information. As a critical component of grid security, secure and efficient grid authentication needs to be well addressed. However, the most widely accepted and applied grid authentication is based on public key infrastructure (PKI) and X.509 certificates, which make the system have low processing efficiency and poor anti-attack capability[14], This IDM systems, which usually work with user directories to authenticate users, represent only the authentication process of the AAA triad (Authentication, Authorization and Accounting) defined in Tech Target's Search Security site. All three elements of the AAA framework are required to intelligently control access to computer resources, enforce policies across multiple systems, audit usage, and provide the information necessary to bill for services. This type of model is not sustainable in most enterprises with diverse operating systems, applications, databases and other systems[15].

1.2. AAA servers to mitigate security

To generate a conceptual model of identity management (IAAA) applying the following servers, authentication, authorization, Directory Server, civil registry database server were considered; in order that users who enter have appropriate levels to mitigate the security of information confidentiality, integrity and availability. Also in this table the number of servers for each activity and order of user access is defined to servers.

Table 1. AAA servers to mitigate security

Servers	Quantity	Access order
Authentication	1	1
Authorization	1	2
Directory Server	1	3
Audit	1	4
Civil registry database server	1	5

1.3. Flow of information in the database

The civil registration information is stored in a master database and two secondary databases for backup replicated in real time; this database users enter such compliance authentication, authorization, auditing (IAAA). These users are defined as: Identification Administrators, organizations identity, identity in the Wan, identity on the Web, identity of citizens, and local identity to mitigate the vulnerability of information.

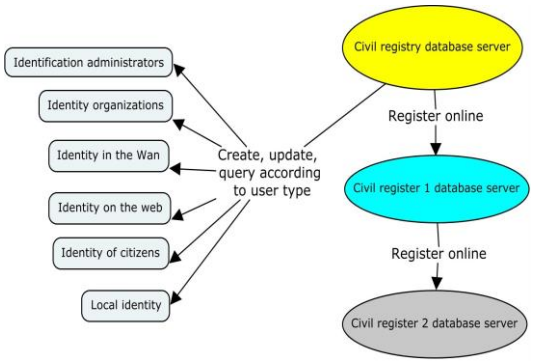

Fig. 1. Flow of information in the database

1.4. Permissions to objects and operations

Permissions to objects are given to through competition from the direction of the civil registry for operations that can be created, updated consult according to the type of user identified (Wan, Web, Local, Citizens, Organizations) with different roles (Dweller, support, Operator Administrators). To control access to information from the primary database and backups.

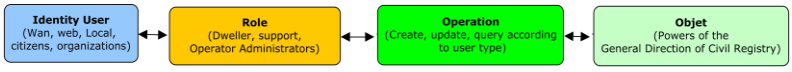

Fig. 2. Permissions to objects and operations

1.5. Result

Prototype of a model identity management for civil registration of Ecuador in a distribute environment was performed as conceptual model applying the authentication, authorization, audit considered confidentiality, integrity, availability to mitigate the vulnerability of information; based on the Organic Law of Identity Management and public data issued by the National Assembly of Ecuador and revised in this exploratory research work.

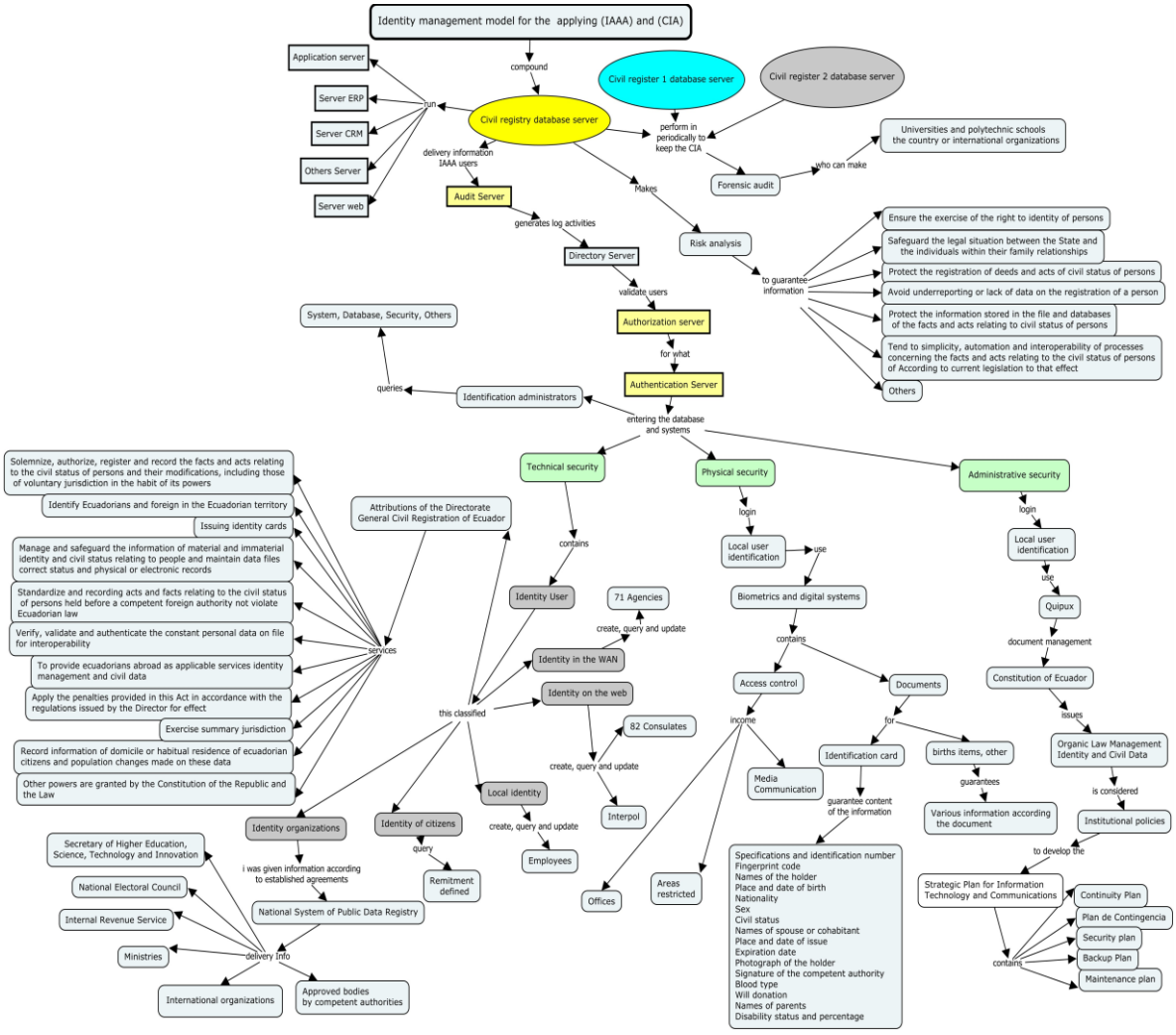

Fig. 3. Conceptual prototype model for identity management of civil registration of Ecuador

1.6. Future work and conclusions

Validate the conceptual model of identity management in the civil registry of Ecuador. Develop or adopt appropriate algorithms and security protocols to mitigate the vulnerability and risks of information. Consider authentication, authorization, auditing (IAAA) with confidentiality, integrity and availability (CIA) to ensure the security of the database of civil registration.

It is concluded that the information flow is based on the types of users who access the information to create, update and query information. The identification of users, roles and permissions to mitigate information security. The prototype of a conceptual model of identity management for civil registration of Ecuador in a distributed environment helps identify the different levels of technical, physical, administrative security with their respective levels of identification, authentication, authorization (AAA), confidentiality, integrity and availability (CIA).

Acknowledgements

The authors thank the CUCEA of Universidad de Guadalajara, Jalisco, México, Program IT PhD Information Technologies, Universidad Politécnica Salesiana del Ecuador and Secretaria de Educación Superior Ciencia, Tecnología e Innovación (Senescyt).

References

[1] P. D. Student, S. Moisés, T. Toapanta, P. D. Luis, and E. Mafla, "Security analysis of civil registry database of Ecuador," *Int. Conf. Electr. Electron. Optim. Tech. - 2016*, pp. 1024–1029, 2016.

[2] R. O. S. De, H. Del, P. Barrezueta, D. E. L. E. Y. Organica, D. E. G. D. E. La, and I. Y. Datos, "Ley Orgánica de Gestión de la Identidad y Datos Civiles," Quito, 2016.

[3] I. Dubrawsky, "Chapter 1 - General Security Concepts: Access Control, Authentication, and Auditing BT - Security+ (Second Edition)," in *Security+*, 2007, pp. 3–54.

[4] J. De Clercq and J. De Clercq, "12 – New Authorization Tracks: Role-Based Access Control and Digital Rights Management," in *Windows Server 2003 Security Infrastructures*, 2004, pp. 417–440.

[5] J. a M. S and Z. R. R, "Management and Access Control From Organizational Perspective Gestion D ' Identites Et Contrôle D ' Acces D ' Apres Une Perspective Organisationnelle," vol. 3, no. 1, pp. 23–34, 2012.

[6] M. Juhrisch and G. Dietz, "Usage and Impact of Model-Based User Authorization," *Inf. Resour. Manag. J.*, vol. 25, no. 3, pp. 98–116, Jan. 2012.

[7] A. D. Kent and L. M. Liebrock, "Differentiating user authentication graphs," *Proc. - IEEE CS Secur. Priv. Work. SPW 2013*, pp. 72–75, 2013.

[8] C. Levallois-Barth, *Digital Identity Management*. 2015.

[9] S. Mare, A. Molina-markham, C. Cornelius, R. Peterson, and D. Kotz, "ZEBRA : Zero-Effort Bilateral Recurring Authentication," 2014.

[10] D. Rutitis, A. Batraga, D. Skiltere, and K. Ritovs, "Evaluation of the Conceptual Model for Corporate Identity Management in Health Care," *Procedia - Soc. Behav. Sci.*, vol. 156, pp. 439–446, 2014.

[11] F. S. Services, "Security Controls and Services," in *Security Controls and Services*, 2011, pp. 127–146.

[12] A. V. Uzunov, E. B. Fernandez, and K. Falkner, "Security solution frames and security patterns for authorization in distributed, collaborative systems," *Comput. Secur.*, vol. 55, pp. 193–234, 2015.

[13] D. Watson, A. Jones, D. Watson, and A. Jones, "Chapter 5 – Risk Management," in *Digital Forensics Processing and Procedures*, 2013, pp. 109–176.

[14] Y. ZHENG, H. yan WANG, and R. chuan WANG, "Grid authentication from identity-based cryptography without random oracles," *J. China Univ. Posts Telecommun.*, vol. 15, no. 4, pp. 55–59, 2008.

[15] V. S. J Michae Butler (Advisor: Dave Shackleford, "Adding Enterprise Access Management to Identity Management," *SANS Read. Room*, pp. 1–14, 2011.