International Journal of Advanced and Innovative Research (2278-7844)/

Volume 1 Issue 8

Analysis of Identity and Access Management alternatives for a multinational information-sharing environment

Ishaq Azhar Mohammed

Sr. IAM Engineer & Department of Information Technology

London, UK

ishaqazhar14@gmail.com

Abstract:

The main aim of this paper is to explore how Identity and Access Management (IAM) alternatives work in a multinational information-sharing environment work that for instance the Department of Defense. Every nation in the twenty-first century must make choices about how to best use contemporary technology to maximize advantages while minimizing consequences. The Department of Defence, for instance, must be able to quickly exchange information with its allies while at the same time limiting unauthorized exposure or cyberattacks [1]. However, although these cyberattacks represent a danger to the national security of the United States, the appropriate use of cyberspace may result in many advantages for all parties involved. The purpose of this paper is to get an understanding of how the Department of Défense maintains its IAM resources whilst reconciling the need to share information with the obligation to secure from unauthorized access. IAM is not a single process or technology, but rather a complex collection of systems and services operating according to many rules and organizations [1]. The DoD has many benefits in delivering IAM capabilities at the DoD level, particularly uniformity in the way in which services are delivered, better security, cost savings, and allocation by creating a specific, distinct digital identity. IAM is also essential to convert the Zero Trust (ZT) framework into a contemporary data-centered identity access management system. To achieve these benefits, DoD IAM solutions must serve both DoD's internal community and DoD's operational participants, offer gateways that are useful for Component Information Systems, as well as eliminate gaps in ICAM infrastructure support. The IAM supports the centralization of identity and credentials, encompassing management of attributes, credentials, and revocation. Additionally, the ICAM RD provides standardized authentication and authorization procedures and protocols. Considerations on the access of persons and non-personal entities (NPE), which demand access to information, should be primarily governed by local administrations, who understand the significance of protecting the sharing of information [2].

Keywords: Identity and Access Management (IAM), Identity, Credential, and Access Management (ICAM), DoD, Federal ICAM (FICAM)

I. INTRODUCTION

As defined by the Department of Defense (DoD), ICAM "provides a safe and trustworthy environment in which authorized user may acquire all permitted resources (particularly services, network security, or data) to have a successful operation."[2,3]. To do this, the DoD should make efforts to provide:

To achieve this, the DoD should make efforts to provide resources that:

• Enable companies to search for contact information for non-personnel organizations
• Enable companies to search for contact information for non-personnel organizations entities (NPE) [3].

ICAM capabilities are already widespread across DoD, since IT systems, platforms, software applications are used throughout the DoD. Most of these DoD IT has some kind of ICAM capacity in place to safeguard from least limited and accessible to most restricted and safeguarded, the entire spectrum of DoD information technology and DoD PACs assets [3]. Modern ICAM features also allow DOD employees to locate and contact each other and provide user behavior responsibility while using DoD resources. Although ICAM dod technologies currently exist, they need to develop and new ICAM infrastructure and applications to achieve the DoD ICAM goal and realign the DoD with the FICAM framework [4]. Furthermore, DoD ICAM has evolved to accommodate a new working environment including the cloud and to convert the future Zero Trust (ZT) architecture into a contemporary identities-based access control system. DoD ICAM is a complex collection of networks and applications under different rules and organizations, and not just a single process or utilize one platform [5]. The ICAM RD supports the consolidation of identity and credential administration, such as the management of attributes, credentials, and revocation. The ICAM RD also provides standardized authentication and authorization procedures and protocols. Recommendations on the accessibility of persons and non-personal entities (NPE), which demand access to resources, must be primarily governed by local administrations, who understand the context and make the mission-relevant [6,7]. ICAM capabilities address the safety controls of the Risk Management Framework (RMF) to mitigate and safeguard infrastructure. Access control (AC), authentication, and identity control (IA) are managed through ICAM, but other RMF control systems may also be managed fully or partly via the appropriate implementation of ICAM [7]. The study will examine IAM options, in particular, the Identity, Credentials and Access Management (ICAM), which the Defense Department often uses to share information with other departments and nations [7].

II. PROBLEM STATEMENT

The main problem that this paper will solve is to understand how the IAM is essential for a multinational information-sharing environment. DoD Services and Agencies have ICAM principles applied to safeguard access to protected systems. Nevertheless, decision-makers have implemented ICAM resources based on their vulnerability assessment rather than creating risk decision-making that supports the requirements of the DOD company [7]. The absence of uniform standards and corporate ICAM shared services complicates procedures and raises dangers to the Department. This basic authentication and authorization method depends on system owners to decide risk-based management of access to services, so that network administrators select implementation methods that suit the local requirements that cannot support corporate targets [8].

III. LITERATURE REVIEW

A. Applicability

The contents of this document apply to:

• Office of the Defense Secretary (OSD), Military Departments, Chair of the Joint Chief of Staff (CJCS) and Joint Staff, Combatant Command, OIG, Defense Agencies, DD Field Activities, and any other organizational entities of the DD (collectively referred to as the "DoD Components").
• Unclassified, secret, top-secret DoD networks and information systems owned by the US Department of Defence. Information systems include those which are owned and operated by or on behalf of Do-D, including do-d data center systems, information technology platform (PIT) systems including weapons and control systems, operating systems, cloud host systems, and systems that are hosted on closed operational networks that are not connected to the dod information networks (DoDIN).
• All DoD and non-DoD individual entity and NPE users (so-called "entity") that are

accessible to DoD through the Secretary of Défense's authority, including DoD mission partners and DoD recipients, unclassified, secret and top-secret networks and resources.

• All DoD ICAM capacities, functions, systems, and services, carried out from anywhere in the Continental Unit

B. DoD Community

The Department of Defense makes resources available to a large number of officers to fulfill its primary goals for a country, offer information services to its officers, and handle external data sharing with other countries. This is done with the help of ICAM. Features of ICAM technologies must be adaptable enough to satisfy the requirements of the information systems that support these communities, while also offering adequate precautions to avoid unauthorized access [8]. This group comprises all individuals that are qualified for fully supplied network accounts on NIPRNet or SIPRNet as a prerequisite of carrying out their professional function, as well as NPEs that are entirely controlled by the Department of Defense [8,9]. Individuals and organizations within the DoD's internal community are identified and authenticated using enterprise services like the Person Data Repository (PDR), and these individuals and organizations are authorized credentials for the NIPRNet on Common Access Cards (CAC) or Alternate Logon Tokens (ALT) by the Department of Defense Public Key Infrastructure (PKI) [10]. The DoD component of the NSS PKI issues these organizations' privileges on the SIPRNet. Depending on their main credential, these organizations may additionally be given secondary credentials to be used in specific contexts such as mobile computing and atypical technologies that do not accommodate the CAC form factor. NPEs within the Department of Defense may be handled via DoD integration services or by the relevant DoD Component, depending on their location within the organization [10]. The Department of Defense must engage with a large number of mission partners who are not authorized for DoD enterprise credentials. A small number of mission partner entities have authentication approved by third-party providers that have been accepted for use by DoD data systems, like Federal Agency Personal Identity Verification (PIV) smart cards, Defense Industrial Base (DIB) commercial PIV-Interoperable (PIV-I) smart cards, or credentials supported by a sovereign nation other than the United States [10,11]. Some mission partner organizations may communicate with the Department of Defense (DoD) in confined areas where they are given identities that are only recognized inside the restricted environment in which they operate. Authentication services must be able to consume mission partner credentials in terms of being able to communicate with all these mission partner entities [11]. This is accomplished by using a permanent, unique identity given by the mission partner entity. DoD services may map the identification included in the mission partner credential to a permanent, unique identifier issued by the DoD at any level, including the DoD enterprise, COI, or local level, to offer a comprehensive picture of authentication throughout the enterprise.

C. Capabilities of ICAM

For successful ICAM implementation to take place, data management must be carried out in line with data management standards, regardless of where the ICAM data is generated or stored. Identifiers and credentials to support authentication; authorization and environment attributes, as well as digital traditional data storage to support authorization; identity attributes to facilitate validation query; and access logs and provisioned entitlements to enable attribution are all examples of ICAM data. In addition to the importance of all data management principles, critical DoD Data Strategy objectives encompass making ICAM data accessible to data systems or even other entities that demand the data and making sure that ICAM data is of acceptable quality to be accepted by information systems when making access decisions. ICAM operations may be carried out at the DoD information system, DoD component, COI, or local level, depending on the situation. Identity management for mission partner organizations may be done outside of DoD. Information systems may also make use of capabilities provided by services that are run at various levels, depending on the operating requirements.

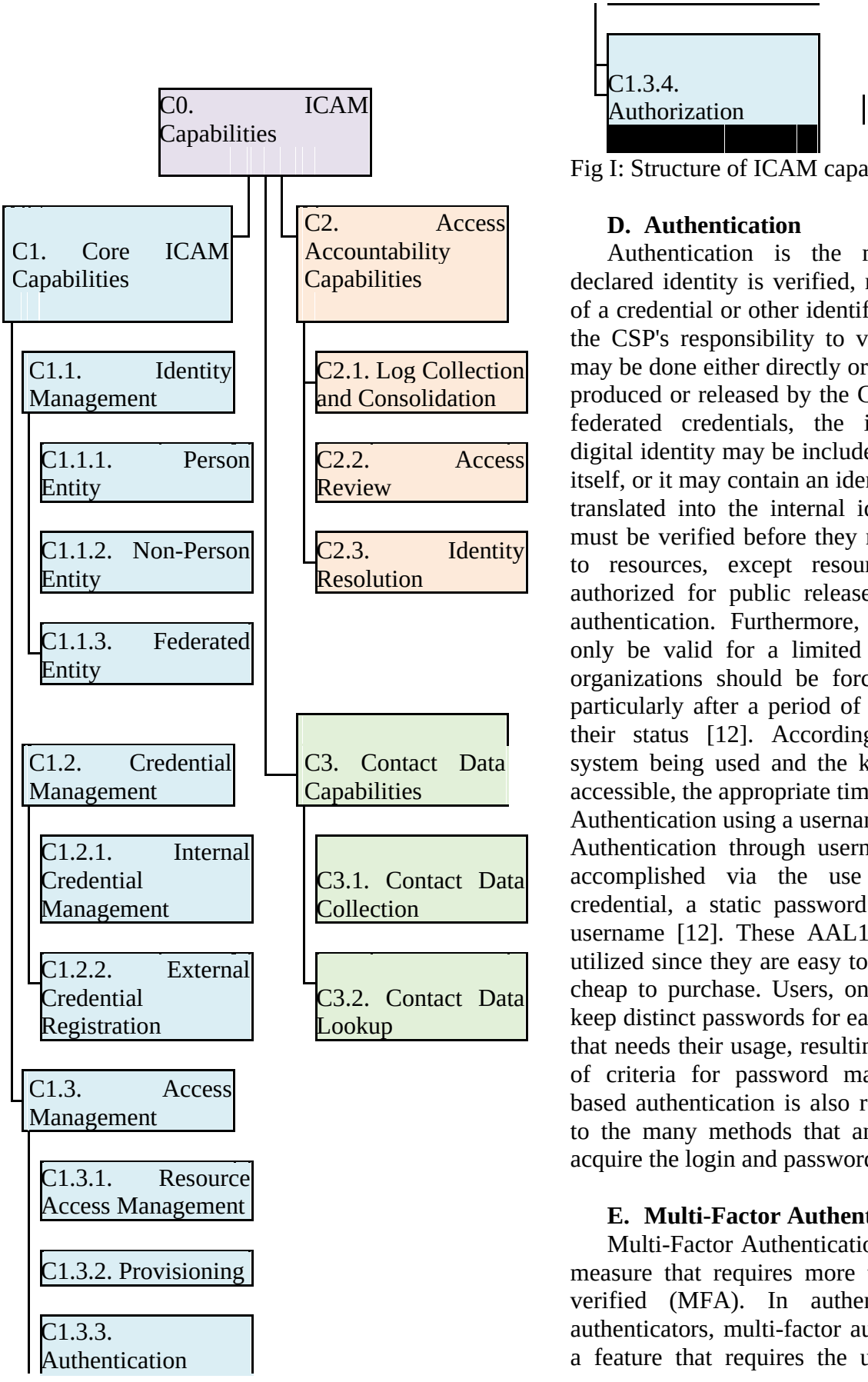

Fig I: Structure of ICAM capabilities

D. Authentication

Authentication is the method by which a declared identity is verified, most often via the use of a credential or other identification document. It is the CSP's responsibility to verify credentials. This may be done either directly or via the use of artifacts produced or released by the CSP. When it comes to federated credentials, the identification for the digital identity may be included inside the credential itself, or it may contain an identification that must be translated into the internal identifier [12]. Entities must be verified before they may be granted access to resources, except resources that have been authorized for public release, which do not need authentication. Furthermore, authentication should only be valid for a limited amount of time, and organizations should be forced to re-authenticate, particularly after a period of inactivity, to maintain their status [12]. According to the information system being used and the kind of resource being accessible, the appropriate time will be determined.

Authentication using a username and password

Authentication through username and password is accomplished via the use of a single factor credential, a static password that is linked to the username [12]. These AAL1 credentials are often utilized since they are easy to maintain and are very cheap to purchase. Users, on the other hand, must keep distinct passwords for each independent system that needs their usage, resulting in a complicated set of criteria for password management. Password-based authentication is also regarded as unsafe due to the many methods that an attacker may use to acquire the login and password combination [12,13].

E. Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a security measure that requires more than one factor to be verified (MFA). In authentication systems or authenticators, multi-factor authentication (MFA) is a feature that requires the use of more than one

unique authentication factor to complete the authentication process successfully. Some additional authenticators might include authenticating the device in addition to the user, necessitating the user to enter a one-time password retrieved from a smartphone or mobile application, sending a code to the user outside of the communication network, or validating a cryptographic token acquired by the user, among other possibilities [14]. MFA may be accomplished via the use of a single authenticator that offers many factors or through the use of a set of authenticators that each gives a distinct component.

Certificate-Based Authentication

Certificate-based authentication depends on the cryptographic characteristics of public-key encryption, where the usage of a private encryption key can be confirmed using a public decryption key, and if the private key cannot be calculated even if the public key is known. Identifiers are linked to public keys via the use of public-key certificates, which are issued by public key infrastructure (PKI) 14,15]. In cryptographic components under the ownership of the entity specified in the certificate, private keys are safeguarded against unauthorized access. They are called AAL2 because private keys may be produced and secured in software cryptographic modules that allow copying of the private key to be made. When using AAL3, private keys are produced and secured in hardware cryptographic modules, which provide considerably better security against attack than software cryptographic modules. Private keys may also be created and stored using hybrid methods, in which the key is first produced in a software cryptographic system and then transferred to a hardware cryptographic module, with the software copy being erased in the process. Although this hardware-backed method is not completely AAL3 compatible, it is considerably more secure than AAL2 software-based PKI [15]. Public key cryptography will have to use cryptographic algorithms that are compliant with current NIST, CNSS, and Department of Defense specifications. Additionally, in contrast to the IAL and AAL, credential strength is determined by the safeguards put in place by the CSP to prohibit the issue of credentials without authorization. Physical and logical restrictions surrounding accessing the CSP, cryptographic security of any keys used by the CSP to create credentials, and checks and balances for people who either manage the system or are allowed to approve the issue of credentials are all examples of these safeguards. In the case of DoD-managed CSPs, the evaluation of these controls is part of the permission to operate process, and it is also included in the approval review process for external CSPs [15].

F. Benefits

The Department of Defense reaps substantial advantages from the deployment and use of DoD enterprise ICAM services. The most significant advantage is consistency [16]. Where a business ID connected to one or more authorized credentials is given to the entities, attributes and other details about a business may be consistently deployed throughout the DoD, and access choices can be based primarily on these data models [16]. Since systems adopting DoD enterprise ICAM services are devoted to those tasks, they may devote more time and attention to policy compliance, accuracy, and overall system performance. The Department of Defense can save expenses associated with duplication of services for implementation and integration, as well as reduce duplicate licensing fees for the same set of users, by centrally controlling and deploying enterprise ICAM services [16]. Using DoD enterprise ICAM capabilities also results in a more positive user experience, which is particularly important for individual entities. The use of enterprise ICAM solutions results in reduced credentials to maintain, as well as a standard set of procedures to follow when registering and validating attribute values in the database. Access to information may be requested and obtained via enterprise services, which can also offer a standardized procedure [16,17]. Furthermore, the use of DoD enterprise ICAM capabilities contributes to increased cybersecurity for the military. De-provisioning an asset that is no longer permitted DoD resources at the time of certification can lead to immediate limited access to all services that rely heavily on enterprise ICAM solutions. Checking activities across Department of Defense information systems may also help in the development of possible internal threats or external credential theft more quickly and precisely [17].

IV. FUTURE OF IAM IN THE UNITED STATES

Identity management is at the core of digital transformation and the next generation of corporate information technology in the United States. Identity systems and services used by the Department of Defense are expected to undergo significant improvements over the next 5 years, with the accompanying changes expected to be just as disruptive as the emerging technologies, applications, and ecosystems that they support. It is this reliable and regular way of collecting, organizing, and sharing information that serves as the basis for Identity as a Utility (IaaU) [17]. Because corporate data is usually housed in many different silos, data sharing, and coordination of updates across these storage facilities has historically become a fundamental pillar of many systems, with origins in contemporary IAM concerns such as user account creation. The United States and the Department of Defense see collaboration with its allies as strategically important (DoD). This kind of cooperation is becoming more important in the Pacific theater, where the Department of Defense must share potentially sensitive material with its allies and important partners efficiently and securely. Nevertheless, various degrees of access to information is afforded to each collaboration 17,18]. The right degree of access must be established for each nation and engagement. Every nation, organization, and coalition with which the United States partners has its own rules and procedures for Identity and Access Management. As a result, not only must the United States adhere to national policy and regulations, but it must also adhere to the regulatory limitations and international laws of other nations [18]. IAM providers use acquisition, collaboration, and R&D methods to expand their product range and market position. Oracle Corporation, IBM Corporation, CA Technologies, NetIQ Corporation (Micro Focus), HID Global Corporation, and others are among the businesses that have dominated the industry in recent years.

V. IAM BENEFITING ORGANIZATIONS GLOBALLY

Many organizations, especially those with several branches, have benefitted from sophisticated information and access management systems. IT Asset Management services help companies in operating following framework modifications. The identity and access management market is divided into the following end-user segments: banking, financial services, information technology, energy, oil and gas, academia, civil service and utilities, healthcare, and manufacturing. Defense, logistics, and residential safety and security are some of the other areas 19]. Many federal agencies in the United States have implemented stringent authentication requirements for their workers, such as the use of hardware-based personal identity verification cards, for them to get access to government information technology infrastructure and networks [18]. Many regulatory changes and more rigorous government standards are pushing businesses and government agencies to update their internal control infrastructures. According to HIPAA regulations, healthcare companies must guarantee the mobility of health insurance and patient confidentiality. Companies must educate staff on security measures, appoint one person in charge of HIPPA compliance and implementation, secure electronic access to patient information, and take appropriate actions to restrict disclosure of health information.

VI. CONCLUSION

This paper involved a study of how Identity and Access Management alternatives are beneficial to a multinational information-sharing environment. The main focus was on the multinational information-sharing environment like the department of defense. An IAM which is well designed and well-managed will minimize friction when it comes to data exchange while also assisting in the provision of the degree of security necessary. An ineffective and fragmented IAM operation will delay and obstruct the progress of the mission. These changes are reflected in the context in which governments function. Furthermore, as policymakers see the importance of delivering cost-effective, integrated applications that benefit the community, the quantity of data shared will grow. A reduced public

workforce will imply one person utilizing technologies that collect data from shared resources holistically, and that can perform many jobs that many people used to do. However, this needs a strong identity and access management system. Identity and access management will be crucial for the future of the government's operations.

REFERENCES

[1] H. Kim, "Biometrics, is it a viable proposition for identity authentication and access control?", Computers & Security, vol. 14, no. 3, pp. 205-214, 1995.

[2] V. J. Symons, “A review of information systems evaluation: content, context and process,” Eur. J. Inf. Syst., vol. 1, no. 3, pp. 205–212, 1991.

[3] P. H. Kubicek, “Governance of Interoperability in Intergovernmental Services Towards an Empirical Taxonomy,” in Proceedings of the 2nd International MultiConference on Society, C ybernetics and Informatics, Volume III, 2008, pp. 100–105.

[4] J. González, M. Rodríguez, M. Nistal and L. Rifón, "Reverse OAuth: A solution to achieve delegated authorizations in single sign-on e-learning systems", Computers & Security, vol. 28, no. 8, pp. 843-856, 2009.

[5] J. Balmer and S. Greyser, "Managing the Multiple Identities of the Corporation", California Management Review, vol. 44, no. 3, pp. 72-86, 2002.

[6] J. Ziemann, Architecture of Interoperable Information Systems - An Enterprise Model-Based Approach for Describing and Enacting Collaborative Business Processes. Berlin: Logos Verlag, 2010.

[7] L. Martin, "Identity-based Encryption: From Identity and Access Management to Enterprise Privacy Management", Information Systems Security, vol. 16, no. 1, pp. 9-14, 2007.

[8] E. Zavadskas, A. Kaklauskas, M. Gikys and N. Lepkova, "A multiple criteria decision support web-based system for facilities management", International Journal of Internet and Enterprise Management, vol. 2, no. 1, p. 30, 2004.

[9] E. Damiani, S. De Capitani diVimercati and P. Samarati, "Managing multiple and dependable identities", IEEE Internet Computing, vol. 7, no. 6, pp. 29-37, 2003.

[10] K. Flieder, "Identity- und Access-Management mit EAI-Konzepten und -Technologien", Datenschutz und Datensicherheit - DuD, vol. 32, no. 8, pp. 532-536, 2008.

[11] L. S. Flak and J. Rose, “Stakeholder Governance: Adapting Stakeholder Theory to E-Government,” Commun. Assoc. Inf. Syst., vol. 16, pp. 642–664, 2005.

[12] G. Goth, "Identity management, access specs are rolling along", IEEE Internet Computing, vol. 9, no. 1, pp. 9-11, 2005.

[13] Å. Grönlund, "Electronic identity management in Sweden: governance of a market approach", Identity in the Information Society, vol. 3, no. 1, pp. 195-211, 2010.

[14] H. J. Scholl, H. Kubicek, and R. Cimander, “Interoperability, Enterprise Architectures, and IT Governance in Government,” in Electronic Government, vol. 6846, M. Janssen, H. J. Scholl, M. A. Wimmer, and Y. Tan, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 345–354.

[15] G. Larson and G. Pepper, "Strategies For Managing Multiple Organizational Identifications", Management Communication Quarterly, vol. 16, no. 4, pp. 528-557, 2003.

[16] T. Martens, "Electronic identity management in Estonia between market and state governance", Identity in the Information Society, vol. 3, no. 1, pp. 213-233, 2010.

[17] J. A. Zachman, “A framework for information systems architecture,” IBM Syst. J., vol. 26, no. 3, pp. 276–292, 1987.

[18] M. Velicanu, "Identity Management in University System", SSRN Electronic Journal, 2009.

[19] F. J. Armour, S. H. Kaisler, and S. Y. Liu, “A big-picture look at enterprise architectures,” IEEE IT Prof., vol. 1, no. 1, pp. 35–42, 1999.