A Study on Improvement of the Military IdAM Using Edge-Sovereign Identity (ESI)

Gyudong Park[1], Gi-Yoon Jeon[1] and Jong-Oh Kim[2*]

[1]*Command and Control Systems PMO, Agency for Defense Development, Seoul, Korea*
[2]*Future Innovation Systems Co., Ltd, Daejeon, Korea*
E-mail: iobject@add.re.kr; gyjeon@add.re.kr; jokim@fisys.co.kr
[*]*Corresponding Author*

Received 11 March 2022; Accepted 14 March 2022;
Publication 23 July 2022

Abstract

A framework-level IdAM integration approach requires a stable network infrastructure. Information framework's operation may be significantly restricted when the network is disconnected from the remote IdAM service. Moreover, military networks, especially tactical networks, are volatile, and network disconnection is also high. In this paper, we proposed an Edge-Sovereign Identity (ESI) that expanded the concept of SSI for use in the military field, designed the structure and function of the proposed concept, and demonstrated its usefulness and validity through examples and prototypes.

Keywords: Self-sovereign identity, IdAM, Edge-sovereign identity.

1 Introduction

Authentication and access control, which restrict unauthorized access and allow only authorized access, are fundamental functions of all information

Journal of Web Engineering, Vol. 21_5, 1435–1448.
doi: 10.13052/jwe1540-9589.2153

frameworks and networks. Recently, authentication and access control and identity and authorization management are evolving into an integrated concept or solution called IAM (Identity and Access Management) or IdAM. So far, most information frameworks have built their IdAMs on their own. As a result, the cost of building IdAM became a significant burden on the information framework, and the disadvantage of performing identity management and user login for each information framework occurred. Furthermore, IdAMs built for each information framework are not desirable in terms of security as they make the possibility of cyberattacks high [1].

Since IdAM is virtually a common feature of all information frameworks and networks, it will be easy to solve the above problems by building IdAMs in an integrated manner and allowing multiple frameworks and networks to share them. However, the above issues are mainly related to identity management and authentication functions. On the other hand, it is desirable to perform authorization and access control by the resource owner. Therefore, so far, integration attempts for IdAM have mainly focused on the integration of identity management and authentication.

IdAM integration is possible so that many information frameworks build and share all or some of the functions of IdAM in common or that other information frameworks utilize the parts of the existing information frameworks. For example, in the military field, the U.S. military, led by DISA (Defense Information Systems Agency), is promoting enterprise-wide identity management and authentication service to be shared by all their information frameworks. Meanwhile, in the private sector, there are many cases in which small services utilize or rely on identity management and authentication of extensive services such as Facebook or Kakao talk.

Integration and sharing of IdAMs between information frameworks are possible when there is no conflict of interest and more significant profit based on sufficient trust between information frameworks. Therefore, it is virtually impossible to integrate IdAMs of all information frameworks. So, in the future, many frameworks still have to invest in the cost of building IdAM, and users who use the system will have to endure inconvenience.

In particular, there is an integrated approach from a completely different direction regarding identity management. Self-Sovereign Identity (SSI) allows individuals to fully own and manage their digital identities. Through this, each individual can directly store and collect their identity attribute information in their digital ledger and use it to log in to the systems. Furthermore, SSI integrates framework-specific identity management in the

individual aspect. In this way, the inconvenience of framework-specific identity management can be completely or significantly eliminated. For reference, SSI has recently been attracting more attention due to the advent of blockchain technology, a suitable implementation technology [2, 3].

A framework-level IdAM integration approach requires a stable network infrastructure. Information framework's operation may be significantly restricted when the network is disconnected from the remote IdAM service. Moreover, military networks, especially tactical networks, are volatile, and network disconnection is also high. Therefore, an approach that correctly duplicates the functions of IdAM in preparation for network disconnection is required. For example, it is appropriate to place authentication near users and access control near resources. Furthermore, it is advantageous to establish centralized identity management and authorization, where integrity at the level of all forces or frameworks is essential. However, in this case, identity and authorization management may be restricted in case of network disconnection.

However, one can solve these problems mainly by using the self-sovereign identity. Therefore, in this paper, we first proposed a method to improve the IdAM of the Korean military based on self-sovereign identity. In addition, in this paper, we also proposed an Edge-Sovereign Identity (ESI) that expanded the concept of SSI for use in the military field and designed the proposed concept's structure and function. Finally, we demonstrated its usefulness and validity through examples and prototypes.

2 Related Works

Strengthening personal information protection is a global trend supported by government laws. For example, the EU is enforcing the strengthening of the rights of information subjects, corporate accountability, and clarification of requirements for the transfer of personal information to the EU through the General Data Protection Regulation (GDPR), which took effect on May 25, 2018 [4]. Here, personal information means identity information.

New legislation, including GDPR, may also motivate research or the development of new technologies. [5] explains that the GDPR places higher demands and responsibilities on service providers handling personal data, returning control over personal data to individuals. Moreover, it is evaluated that it is challenging to meet the needs of GDPR with the current implementation of IdAM. In addition, [5] proposed a unique identity information

management platform using blockchain technology, innovative contract technology, and a design concept.

Interest and demand for personal information or identity information protection are increasing, and research and development of required technology are also active. Development of technologies related to identity information protection should consider user convenience and improve identity information protection both. It is not desirable for identity protection improvement technology to add only a burden to the user. Therefore, new technologies should not add or somewhat reduce the burden on users and provide more functions and convenience if there is an additional burden.

In [6], identity attributes are divided into ID and non-ID features. The ID attribute is an attribute that uniquely identifies a target and can be used for authentication of the target. The non-ID attribute is an attribute that can be used further to verify authentication as a characteristic of the target. ID attributes include RFID, QR code, fingerprint, iris, and PUF (Physical Unclonable Function). Examples of non-ID attributes include (biological, physical, chemical) characteristics, behaviour, sociability, disposition, appearance, place, time, etc. In addition, the non-ID attribute can also be used to provide better services to users or perform better access control.

[7] argued that better service can be provided to customers by utilizing behaviour information generated and accumulated from IoT. Furthermore, this study focused on smartphones, one of the representative IoT devices. This is because smartphones track and accumulate owners' online activities and geographic locations in real-time. If a large amount of individual smartphone information can be obtained, the field of application will be endless.

In [8], various challenges related to the construction of IdAM were investigated, classified, and analyzed. Typical examples include inconvenience in managing IDs and passwords by the system, risk of productivity degradation and issuance costs in case of loss of IDs or passwords, and risk of users who have experienced such inconvenience taking notes of IDs and passwords. It is also noteworthy to mention the challenge of improving user convenience that it would be very convenient if the information could be provided according to the user's role.

3 Edge-Sovereign Identity (ESI)

This chapter describes ESI's concept, function, and structure to improve the tactical network IdAM applying the idea of the identity of self-sovereign.

3.1 Concept Extension

Unlike conventional methods, this paper proposes a plan to distribute management and approval authority to individuals or edges (units) for all or part of the non-ID attributes mainly used for explanation rather than identification. For example, an individual's mobile phone number and performance mission corresponds to non-ID attributes.

An individual's mobile phone number is one of the essential identity information managed by almost all organizations, along with the office's wired phone number. In addition, to promptly notify the relevant personnel in an emergency, it is desirable to double the means of personal contact as much as possible. Moreover, individual mission information can be used to quickly find the corresponding number of people. Finally, of course, this information can also be used to improve authentication or access control. Therefore, these additional attributes must be included in the IdAM identity management target.

All individuals have full authority over their cell phones. Moreover, all commanders have the power to assign duties to their subordinates. So, naturally, each individual and commander can also manage the identity attribute information. In addition, it is reasonable to allocate the function to an individual or unit to allow the authority to continue to be exercised even in the event of a network disconnection from remote identity management.

To this end, as shown in Figure 1, this paper proposed the concept of ESI that enables edge-level identity management such as units by expanding the existing individual-level identity management concept.

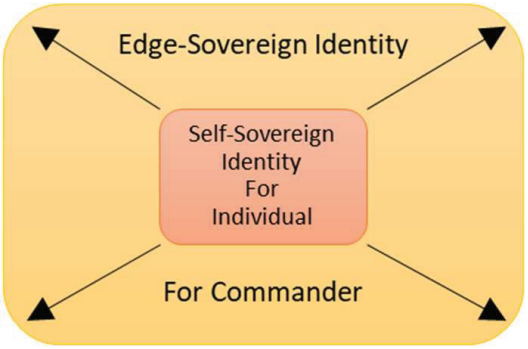

Figure 1 Edge-sovereign identity concept.

3.2 Main Functions

Based on the ESI concept proposed in this paper, it is required to develop the following additional functions to improve the existing IdAM.

3.2.1 Personal identity management

The personal identity information management function allows individuals to manage and store their identity information without any permission. This function consists of a UI (User Interface) and storage. The UI is provided through a personal terminal or an edge network. The storage is located in a private medium such as a smartphone or shared storage in the edge network. For example, the personal identity information management function may manage a mobile phone number owned by an individual.

3.2.2 Identity management at the edge

The identity information management function at the edge manages the identity attributes of the number of members or visitors at the edge level. The identity information management function at the edge also consists of a UI and storage provided at the edge network level. In addition, both UI and storage should be implemented and delivered at the edge network level. For example, the identity information management function at the edge may manage an individual's task or mission.

3.2.3 Identity synchronization

Identity information managed at the individual or edge level should be bottom-up synchronized with a remote central identity information repository. The identity information of the central repository must also be top-down synchronized in whole or in part for redundancy. And the identity information synchronization function should be implemented especially considering the network disconnection and recovery situation.

3.3 Proposed Architecture

Figure 2 shows the improved IdAM framework by applying ESI concepts and functions. The structure proposed in this paper mainly focuses on identity management functions, and other parts are intentionally omitted.

As shown in Figure 2, the proposed structure duplicated the identity management functions at the individual and edge at the edge network level. Through this, even when the central remote identity management module and the network are disconnected, it is possible to manage and utilize the identity

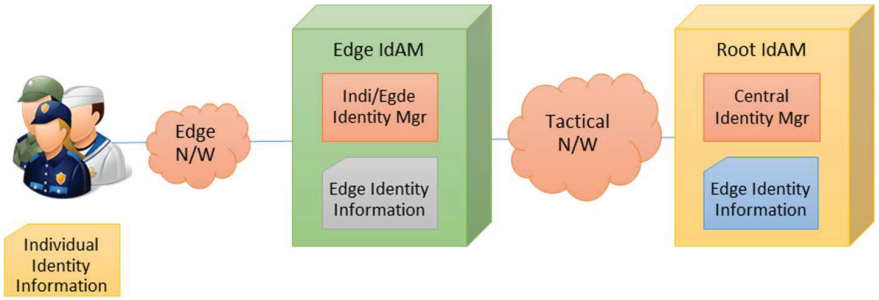

Figure 2 ESI-based tactical IdAM architecture.

attributes continuously. In addition, as a fundamental principle, edge-level identity information could be stored on the edge network, and individual-level identity information is stored on personally owned devices or edge network.

3.4 Operation Example

This section describes the usefulness of the proposed concept, function, and structure of ESI-based tactical IdAM through some operation examples.

3.4.1 Operation continuity

All units must perform their duties in response to all situations, and for this purpose, the mission support system must have operation continuity capabilities. And operation continuity capabilities are mainly realized through redundancy. Therefore, the identity management architecture based on the extended self-sovereign identity concept proposed in this paper can also be one of the approaches for operational continuity management.

Tactical units that rely on tactical or wireless networks may frequently face external network disruption. However, the dual identity management function built at the individual or edge level enables continuous operation regardless of whether the external network is disconnected or not.

However, in an urgent situation where the external network is disconnected, a condition that requires a change of individual mission may occur quite frequently. In addition, new or other unit personnel may be assigned to the unit even when the external network is disconnected. However, even in this case, the ESI-based framework grants temporary access to the system so that the relevant personnel can utilize some functions. Figure 3 shows the difference between the legacy and ESI frameworks in this situation.

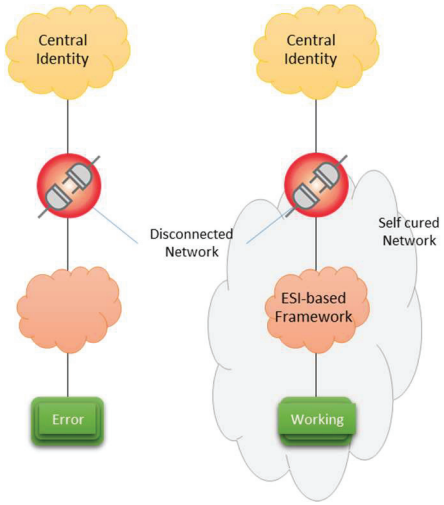

Figure 3 Legacy vs. ESI framework.

3.4.2 Additional authentication and access control

Situations, where users forget their IDs and passwords, occur more often than expected, especially in commercial services. One of the representative solutions to solve this is to utilize the authentication of a third party (communication company) using a mobile phone or smartphone. And additional authentication may be required, especially when accessing sensitive information. If such a situation occurs, it is possible to use a personal mobile phone number for the same purpose.

In the case of the command-and-control system, it is not possible to use carrier authentication because it is not linked to the Internet. However, text message transmission is possible. Therefore, it is possible to perform additional authentication by inputting the received character string into the command control system screen.

Depending on the task performed, users may have different information or functions to access. To this end, the system should be able to recommend information or functions suitable for the user or limit inappropriate information by utilizing the information on the individual's mission of the identity management function. The former may be mainly implemented through a recommendation system, and the latter may be implemented through access control of IdAM. For example, a user with a 'B' task should be significantly restricted in the information and functions they can access compared to a user with an 'A' mission. In addition, detailed tasks such as 'information,'

'operation,' 'firepower,' 'personnel,' and 'logistics' should be able to be assigned separately, and it is necessary to recommend or restrict access to information or functions accordingly.

3.4.3 Data matching

Identity information stored and managed at the individual or unit level in the event of a network disconnection should be transferred, stored and updated in a central remote identity management store when restoring the network.

3.4.4 Authentication and access log information

Suppose user authentication and access log information of multiple units are accumulated and integrated for a long time. In that case, it can be a precious enormous data resource available in the recommendation system or IoB (Internet of Behaviors) technology.

4 Prototype

This paper presents the ESI concept and function feasibility through prototype development.

Figure 4 shows the identity information management screen for each individual. Through this screen, each individual can check basic information such as their mission and update their e-mail and phone number.

Figure 5 shows the edge-level identity information management screen that commanders can use. As shown in Figure 5, the commander can check the identity information of the subordinates and assign a new task or mission to them. And when a subordinate modifies the personal identity

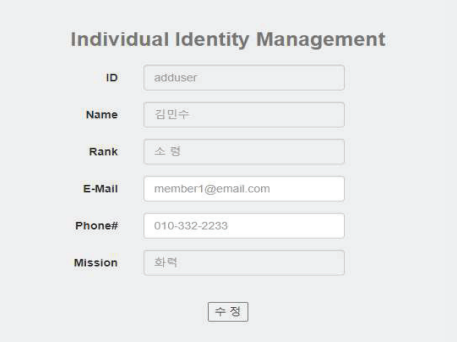

Figure 4 Individual identity management.

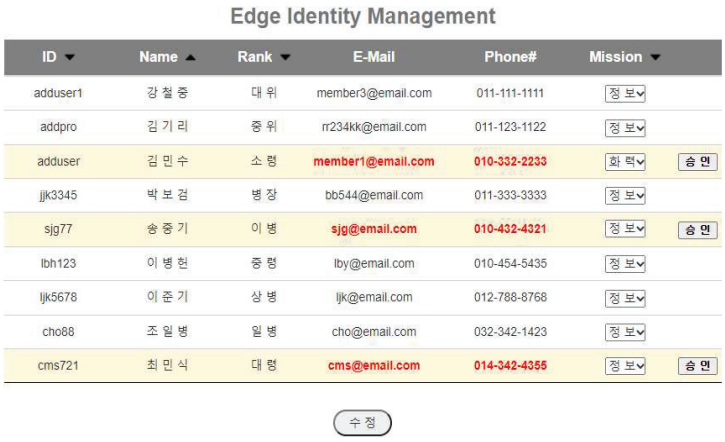

Figure 5 Edge identity management.

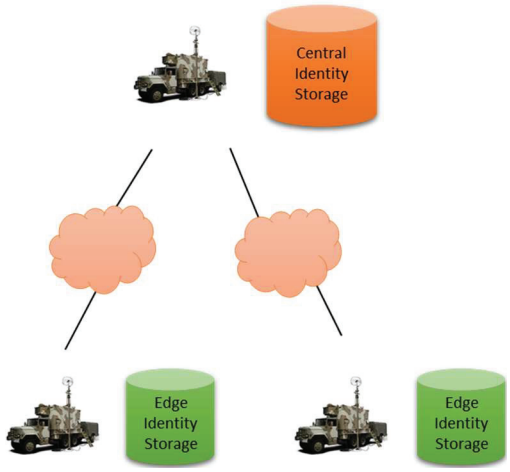

Figure 6 Identity storage implementation and deployment.

information, the modified data is stored in the identity information DB with the commander's approval.

Figure 6 shows the implementation of redundant edge-level identity information storage separated from the central identity information storage to realize the ESI concept. Individual identity storage devices were omitted in the ESI prototype and were integrated and implemented in edge identity information storage. And we also implemented a bidirectional data matching system between central and edge repositories.

5 Conclusion

This paper reviewed IdAM integration efforts to improve efficiency and convenience. In addition, this paper described the necessity of an integrated approach at the system level and the individual level in the military field. And in particular, considering the commander-centric operation concept, which is a characteristic of the military information system, the idea of SSI was extended and proposed to the idea of edge sovereignty. In addition, after designing the structure, function, and procedure of ESI, we presented its usefulness and validity through some examples and a prototype. In addition, the concept and implementation of ESI are expected to contribute to the development of information systems in the military field through subsequent research and development.

Acknowledgments

This research is supported by C2 integrating and interfacing technologies laboratory of Agency for Defense Development (UE201115ED).

References

[1] Andrew Tobin, Drummond Reed, 'The Inevitable Rise of Self-Sovereign Identity', A white paper from the Sovrin Foundation, 2017

[2] Alexander Mühle, Andreas Grüner, et al., 'A Survey on Essential Components of a Self-Sovereign Identity', 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), pp. 97–101, 2020

[3] Michael Kuperberg, 'Blockchain-Based Identity Management: A Survey from the Enterprise and Ecosystem Perspective', IEEE Transactions on Engineering Management, Vol. 67, No. 4, pp. 1008–1027, Nov. 2020

[4] Korea Internet & Security Agency official website http://www.kisa.or.kr /201

[5] Nguyen Binh Truong, Kai Sun, et al., 'GDPR-Compliant Personal Data Management: A Blockchain-Based Solution', IEEE Transactions on Information Forensics and Security, Vol. 15, pp. 1746–1761, 2020

[6] Huansheng Ning, Zhong Zhen, et al., 'A Survey of Identity Modeling and Identity Addressing in Internet of Things', IEEE Journal of Internet of Things, Vol. 7, No. 6, pp. 4697–4710, 2020

[7] Mohd Javaid, Abid Haleem, et al., 'Internet of Behaviours (IoB) and its role in customer services', Sensors International 2, 2021
[8] Peter Haag and Marco Spruit, 'Selecting and implementing Identity and Access Management technologies: The IAM Services Assessment Model', Digital Identity and Access Management, pp. 348–365, 2011

Biographies

Gyudong Park received his Ph. D. degree in computer engineering from Hongik University, Korea, in 2014. He has been working in the Agency for Defense Development (ADD), Seoul, Korea as a researcher since 1998. And his research area includes command and control, interoperability, network, information exchange, and security.

Gi-Yoon Jeon received the MD in POSTECH in 2002 and Ph.D. in Dongguk University in 2021. From 2002 to now, he has been a researcher of Agency for Defense Development (ADD), Seoul, Korea. His research areas of interest are Computer Graphics, AI, IoT/IoB, Human-Robot Interaction.

Jong-Oh Kim received a bachelor's degree from Kyungpook National University in 1990, a master's degree in Electronics from Kyungpook National University in 1992, respectively. From 1992 to 1999, he served as a senior researcher at Electronics and Telecommunications Research Institute (ETRI) in Korea. He is currently working as a CEO at Future Innovation Systems Co., Daejeon. His research areas include Quantum Key Distribution, Data Acceleration, and Security.