Designing Authorization Procedures for Multi-channel and Public Participation-Based System Architecture for Civil Registration and Population Data

A Setiawan, YY Kerlooza
Department of Magister Information System, Faculty of Post Graduate, Universitas Komputer Indonesia, Bandung, Indonesia
Email: *ageng.setiawan@gmail.com

Abstract. This paper aims to propose authorization scenarios for updating population data systems that involve public participation through several different telecommunications channels, called Multi-Channel and Public Participation (MPP)-Based Population Administration System. This paper reveals a number of important technical aspects that arise and must be considered in the authorization scenario. This paper also discusses broadly the authorization techniques that have been used separately in many previous cases. Conformity methods between behaviour of important technical aspects of MPP-Based Population Administration System and authentication methods that are commonly used in system implementations is the base for supporting the implementation of authorization scenarios. The proposed authorization scenario is to utilize a combination of Claim-Based and Multi-Factor authentication techniques because it has a match between important aspects and technical authentication. The combination of authentication techniques in the authorization procedure is able to verify and validate and determine the role of those who wish to collaborate in the service process.

1. Introduction
Population administration, is a series of structuring and controlling activities in the issuance of documents and population data through population registration, civil registration, management of population administration information and the utilization of results for public services and the development of other sectors. Population Administration Information System, hereinafter abbreviated as SIAK is an information system that utilizes information and communication technology that has been built by the government since 2006. The flow of monolithic reporting authorization and hierarchy where the reporting of population events is carried out by the applicant itself starting from the lowest regional apparatus, namely RT to sub-district. The disadvantages of the current population data updating system are:

- Reporting depends on the active role of the applicant;
- Reporting will stop if the party is unable to attend;
- Reporting is very vulnerable to forgery;
- Verification and validation reporting is done manually;
- Low reporting validity

Multi-Channel and Public Participation (MPP) Architecture - Based Population Administration System [1] tried to improve this weakness by proposing the involvement of active public participation in every population incident (birth, death, relocation) utilizing the availability of telecommunications
infrastructure in Indonesia. Initial reporting of a population event can be carried out by community leaders who have the authority and competence in related fields, such as health. Figure 1 is a Multi-Channel and Public Participation (MPP) Architecture - Base Population Administration System.

Figure 1 shows that Multi-Channel architecture is designed in every population reporting event (birth, death, relocation) involving public participation with manual media reporting and utilizing sms telecommunication channels and web or internet protocol. The advantages of utilizing the MPP-Based Population Administration System architecture are as follows:

- Reporting involves the participation of authorized public figures;
- Verification & Validation involving authorized public figures;
- Low forgery rate;
- Verification & Validation Reporting is done using telecommunication channels;
- Reporting Validity Increases.

By involving community leaders in the flow of reporting on population incidents, new issues of authorization and authentication emerged. The procedure for authorization and authentication in updating the current population data is based on the validity of the physical letter through the signature
and stamp of the officially appointed official. This is a major cause of low data validity because it is easy to manipulation [1]. Therefore, a good and appropriate authorization procedure is needed to support the implementation of the MPP-Based Population Administration System architecture. This paper discusses broadly the authorization techniques that have been used separately in many previous cases. This research aims to propose authorization procedure scenario consider the process based on claim based and multi-factor authentication in involving public participation using telecommunications channels or manually.

2. Method
The MPP-Based Population Administration System architecture that has been discussed previously raises aspects and possibility of authentication method which can support system implementation. Figure 2 proposed authorization procedure MPP-Based Population Administration System architecture.

![Figure 2. Proposed authorization procedure (aspect and authentication).](image)

Figure 2 describe a process starting from reporting by an authorized party carried out through the system authorization stage first. Furthermore, the public is authorized both in a system that can carry out the process of verification and validation of reports on a claim basis process. Following are the aspects that form the basis of authorization and authentication methods that are generally used in supporting authorization from public participation.
2.1. Aspect of MPP-Based Population Administration System architecture
The aspect that determine the successful implementation of authorization procedures hence it requires more in-depth research. Emerging aspects are based on the applicant and public participation in reporting and validating reports and communication channels used. The following are aspects that arise based on Multi-Channel architecture:

A. Public Participation or Multi-People
MPP-Based Population Administration System is designed to involve public participation in SIAK data updates. In involving the public, appropriate authentication techniques are needed therefore they are appropriate in determining roles and functions. In a system, access control is a very important part, which is directly related to system security hence a Role Base Access Control (RBAC) is needed [2]. RBAC embodies high elasticity and access to dynamic control systems because it consists of four user elements, namely: role, permission, function, and validating the effectiveness and practicality of the system.

B. Multi-Channel Telecommunication Channels
MPP-Based Population Administration System is designed to utilize the Short Message Service (SMS) telecommunication channel and Internet data channel in involving public participation both as a reporting channel and validation or verification in SIAK data updates. With the utilization of telecommunication channel canals that are directly related to the availability of equipment owned by the participating public, authentication becomes Multi-Factor. Utilization of telecommunications channels is widely used by large organizations in performing services [3] [4].

C. Polylith Semi-Hierarchy Reporting
The MPP-Based Population Administration System architecture in reporting events or cases is designed to be carried out by anyone (Polylith) and follow-up reporting follows administration reporting after passing the reporting validation stage (Semi-Hierarchy). The Polylith Semi-Hierarchy reporting model is widely applied by organizations that prioritize service [5].

D. Polylith Semi-Hierarchy Validation
The MPP-Based Population Administration System architecture in event reporting validation is designed to involve authorized public participation (Polylith) and has a function and area suitability. In the validation process, authorization procedures determine which actor has the right to carry out validation in accordance with a predetermined arrangement as a top priority and alternative if unable to for some reason. The validation procedure also considers the position of the report in the service administration (Semi-Hierarchy). The Polylith Semi-Hierarchy validation model is widely applied by organizations that prioritize service [6].

E. Claim-Based process
The MPP-Based Population Administration System architecture is in the reporting process, validation and follow-up reports are based on an event claim. For the determination of public figures in the validation process also based on the affiliation of claims of events with the authority given based on functions and roles. Broadly speaking, it can be called Claim-Based process. So that in the process utilizing a Public Key Authentication that can be a unique token or session key that is bound and appears based on the event claim that has Time to live (TTL) to maintain the suitability of events and follow-up activities.

2.2. Authentication Method
Authentication is the process of recognizing and determining whether someone's identity, user or something [7]. Authentication technology provides access control for the system by checking to see whether user credentials match the credentials in the authorized user database or on the data authentication server. Based on these aspects, it is necessary to determine the right authentication
method. The following are some of the common Authentication solutions used in developing applications:

A. **Single Factor Authentication (SFA)**

SFA is a process for securing access to a given system, such as a network or website, which identifies those who request access through only one credential category [8]. The most common example of SFA is password-based authentication. Password security depends on the perseverance of the system administrator or the user who set up the account. Best practices include making strong passwords and ensuring that no one can access them. Most of verification currently uses this type of authentication method. Single-Factor Authentication (SFA) was mostly adopted by the community due to its simplicity and user friendliness [9] [10].

B. **Two Factor Authentication (2FA)**

Two-factor authentication (2FA), sometimes referred to as two-step verification or two-factor authentication, is a security process where users provide two different authentication factors to verify themselves to better protect user credentials and resources that users can use in accessing the system [7]. Two-factor authentication provides a higher level of assurance than the authentication method that relies on one-factor authentication (SFA), where the user only provides one factor - usually a password or passcode. The two-factor authentication method depends on users who provide passwords and also the second factor, usually either security tokens or biometric factors such as fingerprints or face scanning [11] [12] [13].

C. **Multi Factor Authentication (MFA)**

Multi-Factor Authentication (MFA), is a security system that requires more than one authentication method from an independent credential category to verify the user's identity for logins or other transactions [14]. Another definition is a computer access control method in which users are only given access after successfully presenting separate evidence to the authentication mechanism [15]. Usually at least the following two categories: knowledge (something they know); ownership (something they have), and default (something they have). Multi-Factor Authentication (MFA) was proposed to provide a higher level of safety and facilitate continuous protection of computing devices as well as other critical services from unauthorized access by using more than two categories of credentials [16]. The aim of the MFA is to create layered defences and make it more difficult for unauthorized people to access targets such as physical location, computing devices and networks or databases. If one factor is compromised or damaged, the attacker still has at least one more barrier to violate before successfully breaking into the target. All two-factor authentication (2FA) is multi-factor authentication (MFA), but not all MFAs are 2FA.

D. **Claim Based Authentication (CBA)**

Claims-Based Authentication (CBA) is the process of using credentials (claims) that contain authentication information in one of the many possible authentication protocols to establish the identity of the parties who wish to collaborate [17]. Claim-based identity is a way of authenticating end users, applications, or devices to other systems with steps that are abstract from entity-specific information while providing data that controls it for appropriate and relevant interactions [18].

3. Results and Discussion

The MPP-Based Population Administration System authorization procedure discussed earlier has several matches between supporting aspects and authentication methods commonly used in system implementation. This similarity is supported by research on authentication methods that have been done before. Table 1 is conformity between important technical aspects and authentication methods.
Table 1. Aspect of Authorization Procedure.

| Authorization Aspect                  | SFA | 2FA | MFA | CBA |
|---------------------------------------|-----|-----|-----|-----|
| Multi-People                          | √   | √   | √   | √   |
| Multi-Channel Telecommunications      |     |     |     |     |
| Polylith Semi-Hierarchy Reporting     |     |     |     | √   |
| Polylith Semi-Hierarchy Validation    |     |     |     | √   |
| Claim-Based Process                   |     |     |     | √   |

Table 1 is a matrix of similarities between aspects and methods of authentication based on criteria, the number of factors in authentication, interaction and public attachment in report claims. Assessment is based on the authentication criteria discussed earlier. Utilization of Claim-Based and Multi-Factor authentication techniques that are able to verify and validate and determine the roles of those who wish to collaborate in the service process. The combination of authentication method also able to handle collaboration in the service process.

The authorization procedure described earlier required in-depth research on content and encrypted type of package information of authentication both for multi-factor and claims-bases. Size of data package also become consideration.

4. Conclusion

Based on the proposed authorization procedure and the suitability between aspects of authorization and authentication solutions, it can be concluded that the combination of the Multi Factor Authentication and Claim Based Authentication techniques can support the authorization procedure in the implementation of the MPP-Based Population Administration System architecture.

Acknowledgements

We would like to express my deep and sincere gratitude to my research supervisor, Dr. Yusrlila Y. Kerlooza, S.T., M.T., for giving me the opportunity to do research and providing invaluable guidance throughout this research.

References

[1] Kerlooza, Y., Setiawan, A., & Asrianto, R. (2018, October). Towards Smart Society: A Study on Multi-Channel and Public Participation-Based System Architecture for Civil Registration and Population Data in Indonesia. In 2018 International Conference on ICT for Smart Society (ICISS) (pp. 1-5). IEEE.

[2] Li, F., & Wu, H. (2015, August). Design and Implementation of Authorization System Based on RBAC. In 2015 7th International Conference on Intelligent Human-Machine Systems and Cybernetics 1, pp. 502-504). IEEE.

[3] Nicoletti, M., & Bernaschi, M. (2019). Forensic analysis of Microsoft Skype for Business. Digital Investigation, 29, 159-179.

[4] Petsas, T., Tsirantonakis, G., Anthanasopoulos, E., & Ioannisidis, S. (2015, April). Two-factor authentication: is the world ready?: quantifying 2FA adoption. In Proceedings of the eighth European workshop on system security (pp. 4). ACM.

[5] Lapor!, “Lapor! - Layanan Aspirasi dan Pengaduan Online Rakyat.” [Online]. Available: https://www.lapor.go.id/. [Accessed: 30-Jan-2019].

[6] Wankmueller, J. (2018). U.S. Patent No. 9,911,121. Washington, DC: U.S. Patent and Trademark Office.

[7] Burrows, M., Abadi, M., & Needham, R. M. (1989). A logic of authentication. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 426(1871), pp. 233-271.
[8] Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Computers & Security, 30(4), pp. 208-220.

[9] Konoth, R. K., van der Veen, V., & Bos, H. (2016, February). How anywhere computing just killed your phone-based two-factor authentication. In International Conference on Financial Cryptography and Data Security (pp. 405-421). Springer, Berlin, Heidelberg.

[10] Kim, J. J., & Hong, S. P. (2011). A method of risk assessment for multi-factor authentication. Journal of Information Processing Systems, 7(1), 187-198.

[11] Acemyan, C. Z., Kortum, P., Xiong, J., & Wallach, D. S. (2018, September). 2FA Might Be Secure, But It’s Not Usable: A Summative Usability Assessment of Google’s Two-factor Authentication (2FA) Methods. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (62(1), pp. 1141-1145). Sage CA: Los Angeles, CA: SAGE Publications.

[12] Schneier, B. (2005). Two-factor authentication: too little, too late. Communications of the ACM, 48(4), 136.

[13] Wang, D., He, D., Wang, P., & Chu, C. H. (2014). Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. IEEE Transactions on Dependable and Secure Computing, 12(4), 428-442.

[14] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography, 2(1), 1.

[15] C. Webber, “Two-Factor (2fa) vs. Multi-Factor Authentication (MFA) - Definition & Differences,” Secure Thinking by Centrify, 27-Jun-2016. [Online]. Available: https://blog.centrify.com/2fa-mfa-difference/. [Accessed: 31-Jan-2019].

[16] Scheidt, E. M., & Domangue, E. (2005). U.S. Patent No. 6,845,453. Washington, DC: U.S. Patent and Trademark Office.

[17] Simpson, W. R., & Chandersekaran, C. (2013). Claims-based authentication for a web-based enterprise (No. IDA-NS-D-5091). Institute for Defense Analyses Alexandria Va.

[18] Chi, Y., Qin, Y., Li, S., & Li, G. (2018, October). A Design of Cross-Realm Authentication Scheme in Openstack Based on Declaration. In 2018 IEEE 18th International Conference on Communication Technology (ICCT) (pp. 1148-1153). IEEE.