Bridging the Gap: Managing Dual Assurance Levels in OpenID Connect

Brendon Vicente R. Silva[1], **Frederico Schardong**[1,2], **Ricardo F. Custódio**[1]

[1]Laboratório de Segurança em Computação (LabSEC)
Universidade Federal de Santa Catarina (UFSC)

[2]Instituto Federal do Rio Grande do Sul (IFRS)

Abstract. *This paper introduces and addresses challenges in managing electronic identity's Level of Assurance (LoA), which has two types: LoA of authentication and LoA of identity. We explore different technical specifications, protocols, and concrete identity providers' strategies for managing these two levels of assurance, highlighting the implications of protocols supporting only a single LoA instead of two. An extension to the OpenID Connect protocol is proposed to support both LoA types, instituting a new claim, the Identity Context Class Reference (ICR). This approach ensures compatibility and versatility with existing technical specifications.*

1. Introduction

With the increasing virtualization of human relationships and subsequent increase in sensitive information stored in digital environments, electronic identities have become indispensable components of computer systems and services. Identity and Access Management (IAM) systems play a crucial role in this scenario.

The Level of Assurance (LoA) is a key concept linked to these systems. It consists of a parameterized indicator expressing the confidence level in user authentication and identification processes [Vale et al. 2022]. Initially, LoA was a single attribute representing the reliability index of an electronic identity [Council of European Union 2014, Burr et al. 2006]. However, this idea has been expanded over time, leading to a more nuanced understanding and a division of the levels of assurance into multiple categories.

In this process, two new LoA were defined: the authentication and identity assurance level [European Comission 2015, Grassi et al. 2017]. The authentication LoA reflects the confidence that the correct user (i.e., the identity owner) possesses the identity at authentication time. Typically, the authentication LoA is defined by the number of authentication factors employed and their reliability level. This LoA is calculated each time a user is authenticated. In contrast, the identity LoA indicates how accurately the attributes within an identity represent its owner; this is mainly determined by which identification methods were used, the volume and reliability of the attributes collection available, and how this data was collected.

While this division provides a more precise definition of aspects related to the electronic identities' trustworthiness, it also implies that more effort is needed to manage the multiple LoA types. The decentralization of LoA directly impacts how they are represented in security protocols common for this environment [Sakimura et al. 2014, Campbell et al. 2015] and how they are managed by Identity Providers (IdPs).

The mentioned points will be a topic of analysis and discussion throughout this paper. The remainder of the paper is structured as follows. Section 2 discusses the technical specifications' approach regarding LoA, emphasizing its categorization; Section 3 explores OpenID Connect, a security protocol used in electronic identification and its relationship with LoA; Section 4 presents examples of real IdPs, showcasing their diverse LoA management mechanisms; Section 5 details an OpenID Connect extension proposal to fully leverages LoA categorization; finally, Section 6 summarizes the content presented, proposing reflections regarding the topic covered.

2. Technical Specifications

Organizations worldwide have developed standards and technical norms to formalize and establish best practices for managing electronic identities. Among the most well-established specifications are the European regulation Electronic Identification Authentication and Trust Services (eIDAS) [Council of European Union 2014] and the American technical standard from the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-63 [Grassi et al. 2017].

Since their conception, both specifications have provided well-established LoA frameworks. It features clear parameters for each level definition, detailed risk analyses, and guidelines for stipulating use cases' minimum LoA. The division of LoA first appeared in the European regulation in September 2015, establishing multiple LoA categories classified as low, substantial, or high [European Comission 2015]. Similarly, in June 2017, NIST published a review of its technical standard, entitled SP 800-63-3, which expanded the concept of LoA by creating new categories. This review introduced the Identity Assurance Level (IAL) and Authentication Assurance Level (AAL), each divided into three levels, numbered from 1 to 3 [Grassi et al. 2017].

3. Existing Protocols

Along with the need to store sensitive information on digital media within the scope of electronic identities, there is a need to transmit it securely. In this scenario, secure protocols emerged specifically for electronic identity transmission and parameterization. Among the most well-established protocols on the market, OpenID Connect has supported electronic identities' LoA since its conception in 2014 [Sakimura et al. 2014]. It does not go into implementation details and, therefore, does not define aspects of how the LoAs scheme should be implemented. However, the protocol provides only one field (originally destined to express the authentication LoA) to transmit the LoA between parties.

In essence, the OpenID Connect protocol does not support the transmission of multiple levels of assurance. However, this does not mean such behavior cannot be achieved. Representing multiple LoA categories implies the need to resort to undocumented methods. Therefore, the decision to provide only one field for communicating the LoA entails the implicit need to use non-standard means of transmitting the LoA (such as embedding issued tokens with extra attributes) or for different categories of LoAs to be summarized in a single value. By not addressing this topic in its documentation, OpenID Connect exempts itself from the responsibility of standardizing how LoA should be managed. As identity specifications, like eIDAS and NIST SP 800-63, do not discuss implementation details, such as integrating security protocols, they do not cover these LoA aspects. While explicit instructions are given on which authentication and identity LoAs can be used together, there is no mention of which resulting value(s) should be communicated as the final assurance level. This information gap implies greater freedom for IdPs, who can institute their own LoA schemes, but also burdens them with greater liability.

4. Identity Providers and Levels of Assurance

The lack of documentation and standardization in managing LoA implies consequences that can be seen in real-life examples. Some identity providers choose to use a single LoA type summarizing diverse aspects of authentication and identity in one value, as seen in the Gov.br [MGISP 2021]. On the other hand, other identity providers have their own management systems. Typically, there is an internal distinction between the multiple LoA categories, but a single value is externalized, resulting from the association of these levels according to some aggregation logic.

Identity providers carry out the process described above at national and international landscapes, as is the case of the Identificação Eletrônica do Registro Civil do Brasil (IdRC) or Denmark's Digital ID (MitID) [Silva et al. 2023, MitID 2024]. In these services, the resulting LoA is the minimum value between the identity and authentication.

Externalizing a single LoA simplifies the integration with IdPs by exempting applications from managing multiple types of LoAs. In other words, this mechanism allows applications connected to identity providers to not worry about defining different requirements for each user authentication and identification aspects. However, this method also has its drawbacks. It provides less transparency regarding the processes involved in LoAs definitions and neglects use cases that could benefit from the multiplicity of LoA.

5. Extending OpenID Connect

In light of the problems presented, possible solutions are discussed to enhance communication between systems in the digital realm and more effectively leverage the advantages of classifying LoA into multiple categories. An alternative to this problem would involve technical specifications, like eIDAS and NIST SP 800-63, to offer clear guidelines for managing LoA categories. For instance, schemes for aggregating and summarizing LoA could be outlined, considering diverse user identification and authentication landscapes.

We propose introducing and standardizing a new attribute within the OpenID Connect protocol: the *Identity Context Class Reference (ICR)*, a case-sensitive string containing a value describing the identity LoA. Like OpenID Connect's Authentication Context Class Reference (ACR), this attribute should contain an absolute URI or an RFC 6711 [Johansson 2012] name, which parties must mutually agree on its meaning.

This approach aims to maintain maximum compatibility with existing systems: extending OpenID Connect with the ICR claim should not disrupt the operations of identity and service providers that opt not to implement it, as systems that do not adopt this claim can continue behaving as they currently do. Although this proposal increases the responsibility required for applications that should stipulate minimum authentication and identity LoA, adopting the ICR claim would allow applications and services connected to IdPs to establish more complex and precise LoA requirements.

6. Final Remarks

The LoA division into multiple categories highlights a gap in the literature concerning the management and definition of LoA processes. The present study seeks to shed light on this subject, presenting implications related to the LoA categorization and mapping diverse use cases. The continuous development of LoA frameworks and their integration into digital identity systems is crucial for maintaining robust and trustworthy electronic identities. While current specifications and protocols provide a solid foundation, it is clear that further standardization and innovation are needed to leverage the benefits of multiple LoA fully. The introduction of the ICR attribute will enhance the OpenID Connect protocol by providing a standardized way to represent a user's level of identity assurance, thereby improving the systems' overall security and reliability.

References

Burr, W., Dodson, D., and Polk, T. (2006). Electronic authentication guideline. Technical Report NIST Special Publication (SP) 800-63 Version 1.0.2, National Institute of Standards and Technology, Gaithersburg, MD.

Campbell, B., Mortimore, C., and Jones, M. B. (2015). Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants. RFC 7522.

Council of European Union (2014). Regulation no 910/2014 of the european parliament.

European Comission (2015). Commission implementing regulation (eu) 2015/1502.

Grassi, P., Garcia, M., and Fenton, J. (2017). Digital identity guidelines. Technical Report NIST Special Publication (SP) 800-63-3, Includes updates as of February 03, 2020, National Institute of Standards and Technology, Gaithersburg, MD.

Johansson, L. (2012). An IANA Registry for Level of Assurance (LoA) Profiles. RFC 6711.

MGISP (2021). Conta gov.br. Available at `https://web.archive.org/web/20240406230209/https://www.gov.br/governodigital/pt-br/identidade/conta-gov-br`, accessed on 13/06/2024.

MitID (2024). About mitid. Available at `https://web.archive.org/web/20240329140510/https://www.mitid.dk/en-gb/about-mitid/`, accessed on 15/06/2024.

Sakimura, N., Bradley, J., Jones, M., De Medeiros, B., and Mortimore, C. (2014). Openid connect core 1.0. *The OpenID Foundation*, page S3.

Silva, B. V. R., Schardong, F., Junior, L. C. V., and Custódio, R. F. (2023). Identificaçao eletrônica do registro civil do brasil. In *Anais Estendidos do XXIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 89–92. SBC.

Vale, C. A., Schardong, F., Barros, M., and Custódio, R. (2022). Touchless authentication for health professionals: Analyzing the risks and proposing alternatives to dirty interfaces. In *2022 IEEE 35th International Symposium on Computer-Based Medical Systems (CBMS)*, pages 459–464. IEEE.