UDC: 342.738.037:004.6.056.52/.53
Professional paper:

A COMPARATIVE STUDY OF IDENTITY ASSURANCE: KANTARA, EIDAS, AND REFEDS PERSPECTIVES ON LOA

Vjollca SHEMSHI[1], Boro JAKIMOVSKI[2]

[1] Faculty of Natural Sciences and Mathematics, University of Tetova, Republic of North Macedonia*
[2] Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University in Skopje, Republic of North Macedonia
[*](vjollca.shemshi@unite.edu.mk)

Abstract

In the contemporary era marked by the pervasive use of digital devices, safeguarding electronic identity has become indispensable for ensuring secure and dependable interactions within federated systems. This paper undertakes a comparative analysis of identity assurance frameworks, with a specific focus on the perspectives provided by Kantara, eIDAS, and REFEDS systems concerning Levels of Assurance (LoA), which involves examining various aspects of their identity assurance frameworks, standards, and implementations.

Although Kantara, eIDAS, and REFEDS share a common goal of increasing identity assurance and trust in federated systems, they differ in their scope, regulatory mandates, LoA frameworks, and approaches to adoption and implementation. Understanding these differences is essential for organizations looking to navigate the complex landscape of identity management and choose the most appropriate frameworks for their specific needs.

Through a meticulous review of each framework, this study delves into the foundational principles, methodologies, and implementations underpinning identity assurance within federated systems. By scrutinizing the perspectives of Kantara, eIDAS, and REFEDS, this analysis elucidates the similarities, distinctions, strengths, and limitations of each framework in tackling identity assurance challenges.

Furthermore, this study explores the implications for future research and development in federated identity management, providing higher security of the electronic identities of users of federated systems. By fostering a deeper understanding of identity assurance frameworks, this comparative analysis contributes to the advancement of secure and trusted digital interactions in various organizational systems.

Keywords: Electronic identity, Federation systems, Level of Assurance (LoA), Kantara, eIDAS, REFEDS.

1. Introduction

An electronic identity is a collection of electronically stored user identity attributes that uniquely describe a person seeking to be part of a trusted system.

Level of Assurance (LoA) is a critical concept that enables organizations to assess the risk associated with electronic identities and decide on the required level of authentication (Mikael Linden (CSC), 2017). *LoA* represents the level of confidence in the accuracy and reliability of the electronic Identity. It defines the degree to which the electronic identity is verified, authenticated, and secured. The higher the *LoA*, the greater the level of trust in the electronic identity and the lower the risk of identity theft.

2. Evaluating Security Levels in Digital Identity

2.1. Insights from the Kantara Initiative: The Kantara *initiative* is built to ensure the reliability of users' electronic identities and personal data. The core of the Kantara initiative is the *Identity Assurance Framework (IAF) (Initiative, Kantara Identity Assurance Framework).* This framework, known as the *Kantara Initiative Identity Assurance Framework (KIAF)*, is a

https://doi.org/10.62792/ut.jnsm.v9.i17-18.p2827

comprehensive set of criteria, processes, and practices for evaluating and ensuring the trustworthiness of digital identity systems and services.

Within the Kantara Initiative to manage and validate digital identities, various entities play essential roles that contribute to the creation of trusted digital identity ecosystems. These include *Identity Providers (IdP)*, *Credential Service Providers (CSP)*, and other entities that collaborate to ensure the security and reliability of digital identity management. These service providers facilitate the issuance and verification of digital credentials, enabling individuals to access online services securely (Vjollca Shemshi, 2023).

Level of assurance in Kantara

The Kantara Identity Assurance Framework defines different levels of assurance *(LoA)* ranging from user identity identification, authentication methods, credential management, and other factors that help organizations and users understand the level of trust they can have in a certain identity system or service (Ian Neilson, 2019).

In the *Kantara Identity Assurance Framework (IAF)*, there are different levels of security, often referred to as **Assurance Levels (Als)** (Initiative, Kantara Identity Assurance Framework)**,** which indicate the strength of security provided by an identity system or service. These levels help users and organizations understand the level of trust they can place in a particular identity solution. While specifics may vary based on implementation and context, typical security levels at *Kantara IAF* include (Broeder, 2012):

- **Security Level 1 (AL1):** includes the lowest security level. This includes minimum requirements for identity verification and authentication. Authentication mechanisms in AL1 rely on one-factor authentication, such as passwords or simple PINs. Multi-factor authentication (MFA) is not required at this level.
- **Security Level 2 (AL2):** means a moderate level of security. This implies that there is a moderate level of confidence in the accuracy of the claimed identity and in the processes used to establish and verify it. For example, in AL2, an identity verification process may include document verification, biometric authentication, or knowledge-based authentication methods.
- **Security Level 3 (AL3):** represents a significant level of confidence in the accuracy of the user's identity and the processes that will be used to verify it. This level includes advanced identity verification methods, strong cryptographic authentication, in-person verification with multiple forms of identification, biometric authentication, and comprehensive background checks.
- **Security Level 4 (AL4):** AL4, if defined within the framework, means the highest level of security. May include more stringent identity verification, authentication and security requirements.

eIDAS Framework

In the European Union, the *eIDAS* regulation defines criteria for assessing the strength of authentication methods used to verify a user's digital identity ((JANET) & V. Nordh (University of Gothenburg) W, 20.05.2010). These criteria are based on the *Levels of Assurance (LOA)* defined by eIDAS, which consist of low, substantial and high levels of assurance. these levels conform to *ISO 29115* definitions (COMMISSION, 2015).

Analyzing Security Levels Under the eIDAS Regulation

- **Low assurance (LOA 2):** This assurance level corresponds to Level 2 in the ISO 29115 definitions. It represents a basic level of trust in the electronic identification credential used to confirm the identity of a physical entity. While it provides some security, it may not involve rigorous proof-of-identity processes or strong authentication mechanisms.
- **Substantial security (LOA 3):** Substantial security complies with Level 3 in the ISO 29115 limitation. At this level, there is a higher level of confidence in the identification of electronics. It has stricter identity verification procedures and stronger authentication methods to verify an individual's identity.
- **Substantial security (LOA 3):** Substantial security complies with Level 3 in the ISO 29115 limitation. At this level, there is a higher level of confidence in the identification of electronics. It has stricter identity verification procedures and stronger authentication methods to verify an individual's identity.

REFEDS Assurance Framework

REFEDS (Research and Education Federations) has developed a framework to standardize assurance levels of identity assertions within the global research and education community. This framework, known as the *REFEDS Security Framework (RAF),* includes various security profiles that specify requirements and practices for different *Levels of Security (LoA)* (Wolfgang Hommel, 2016). These profiles ensure that identity assertions meet specific security, privacy and trust requirements, facilitating secure and interoperable access to online resources and services (REFEDS).

The REFEDS Assurance Profiles

Profiles include low, medium, and high levels of security, each with distinct criteria for identity authentication, credential issuance, and authentication strength (Jule Anna Ziegler, 2021).

- **REFEDS Low Level -** this security level is similar to Kantara's first security level. Basic authentication is therefore required which may include self-asserted identity or verification through a minimal set of user attributes. Basic credential issuance and management practices apply, focusing on one-factor authentication (eg, username and password) being sufficient.
- **REFEDS Medium Level -** This level corresponds to the second level of the Kantara framework. At this level, users require moderate security. Stronger identity verification processes are required, such as government-issued ID verification or personal verification. At this level, multi-factor authentication (MFA) is appropriate to provide a higher level of security.
- **REFEDS High Level -** The high level of identity security in REFEDS matches the third level of identity security in Kantara. This level includes users who access high-security or sensitive services. Rigorous identity authentication is required, including full verification of the user's identity through multiple and trusted sources. Strong multi-factor authentication, potentially including biometric factors or hardware tokens.

3. Comparative analysis of levels of assurance (LoA): Kantara, eIDAS, and REFEDS

Kantara, eIDAS and *REFEDS* play crucial roles in the field of digital identity and trust services, but they operate in different contexts and domains, ensuring secure and reliable identity verification processes (Ian Neilson, 2019). This comparison chart provides an overview of how *Kantara, eIDAS* and *REFEDS* define and implement *Levels of Assurance (LoA)* in their respective frameworks.

Table 1. An overview of how Kantara, eIDAS and REFEDS define and implement Levels of Assurance (LoA) in their respective frameworks.

Aspect	Kantara Initiative	eIDAS	REFEDS
Scope	Global, multi-sector	European Union, electronic transactions	Global, research and education sectors
Loa Definition	Four levels (LoA 1 to LoA 4), flexible based on application	Three levels (Low, Substantial, High), legally defined	Defined assurance profiles (Basic, Medium, High)
Identity Proofing	Varies by LoA, from self-assertion to in-person verification	Varies by LoA, strict identity verification for higher levels	Varies by profile, from self-assertion to in-person
Credentials	Robust processes including issuance, maintenance, revocation	Secure issuance and management, enhanced at higher LoAs	Varies by profile, from basic to robust management
Authentication	Single-factor to multi-factor authentication (MFA)	Single-factor to strong MFA, depending on LoA	Varies by profile, from single-factor to strong MFA
Assurance Profile	LoA 1: Basic self-assertion, single-factor auth		- Basic: Minimal proofing/authentication
	LoA 2: Moderate verification, basic MFA	Low: Basic security, low-risk applications	Medium: Moderate security, government ID, MFA
	LoA 3: Strong verification, robust MFA	Substantial: Strong proofing, secure credential management	High: High security, in-person verification, MFA
	LoA 4: Very strong proofing, highest MFA	High: Rigorous proofing, strong MFA	

Kantara focuses on developing global standards and certifications for identity assurance. eIDAS provides a regulatory framework within the EU for electronic identification and trust services, ensuring mutual recognition and legal enforceability. REFEDS addresses the unique needs of the research and education community, promoting interoperability and best practices for identity federations around the world. Together, they contribute to the safe, reliable and interoperable use of digital identities across different sectors and regions.

Evaluating Identity Assurance

If we deepen a comparison between the Kantara Initiative, eIDAS and REFEDS systems, it becomes clear that their security levels exhibit different characteristics and methodologies. Each system is designed to address specific needs and requirements, resulting in differences in how they approach identity security (Vjollca Shemshi, 2023). The following figure describes their unique characteristics and methodologies, highlighting these differences.

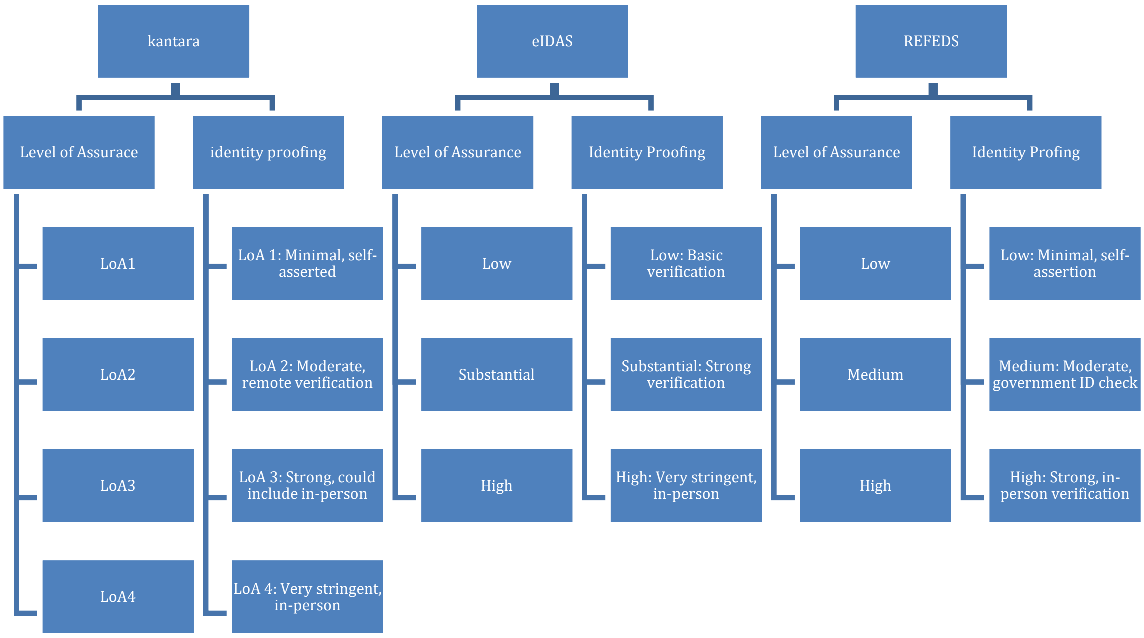

kantara
Level of Assurance
LoA1
LoA2
LoA3
LoA4
identity proofing
LoA 1: Minimal, self-asserted
LoA 2: Moderate, remote verification
LoA 3: Strong, could include in-person
LoA 4: Very stringent, in-person
eIDAS
Level of Assurance
Low
Substantial
High
Identity Proofing
Low: Basic verification
Substantial: Strong verification
High: Very stringent, in-person
REFEDS
Level of Assurance
Low
Medium
High
Identity Profing
Low: Minimal, self-assertion
Medium: Moderate, government ID check
High: Strong, in-person verification

Figure 1. The unique features and methodologies of Kantara, eIDAS and REFEDS, highlighting the differences between them

Kantara, eIDAS and REFEDS provide strong frameworks for authentication at different levels of security. Each emphasizes the importance of secure identity verification and offers different authentication methods ranging from basic one-factor authentication to advanced multi-factor authentication tailored to their specific contexts and user needs (Initiative, Identity Assurance Framework, 2021). By comparing these systems, one can appreciate the combined approaches they take to ensure secure and reliable digital interactions, which are shown in the figure below:

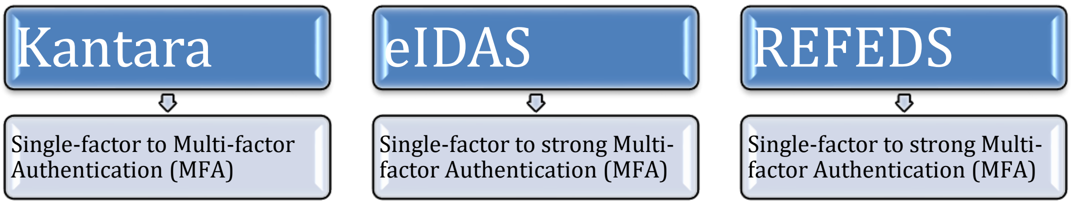
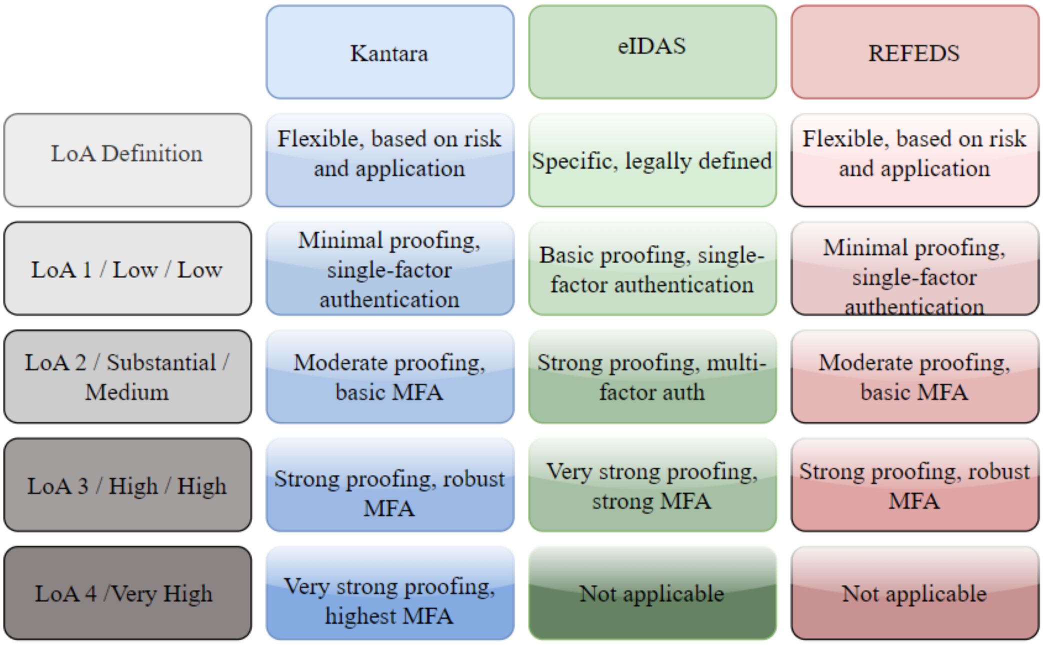

Kantara
Single-factor to Multi-factor Authentication (MFA)
eIDAS
Single-factor to strong Multi-factor Authentication (MFA)
REFEDS
Single-factor to strong Multi-factor Authentication (MFA)

Figure 2. Combined approaches leveraging Kantara, eIDAS and REFEDS systems to ensure secure and reliable digital interactions

4. Intersection of Security Standards: Kantara, eIDAS, and REFEDS

By comparing the security commonalities, it becomes clear that Kantara, eIDAS and REFEDS have distinct approaches tailored for their specific purposes, which aim to ensure strong identity verification, secure credential management and security processes. strong authentication to maintain trust in digital identity (Jesus Carretero, Vasile-Cabezas, & Garcia-Blas, 2018).

Kantara's levels are flexible, allowing for different levels of authentication and verification. The eIDAS levels are adapted based on the EU regulation, are strict and specify strict methods for each level. REFEDS profiles are designed for specific research and education needs and offer flexibility tailored to academic requirements.



	Kantara	eIDAS	REFEDS
LoA Definition	Flexible, based on risk and application	Specific, legally defined	Flexible, based on risk and application
LoA 1 / Low / Low	Minimal proofing, single-factor authentication	Basic proofing, single-factor authentication	Minimal proofing, single-factor authentication
LoA 2 / Substantial / Medium	Moderate proofing, basic MFA	Strong proofing, multi-factor auth	Moderate proofing, basic MFA
LoA 3 / High / High	Strong proofing, robust MFA	Very strong proofing, strong MFA	Strong proofing, robust MFA
LoA 4 /Very High	Very strong proofing, highest MFA	Not applicable	Not applicable

Figure 3. Kantara, eIDAS and REFEDS approaches for identity verification and authentication

Each framework provides distinct approaches to identity verification and authentication tailored to their specific goals and objectives. Kantara's flexible and scalable model contrasts with the legally enforced and strict standards of eIDAS, while REFEDS offers a balanced approach suitable for academic and research environments (Working, 2021). These differences underscore the importance of context and specific needs when choosing and implementing an identity assurance framework.

5. Conclusions

The comparative analysis between Kantara, eIDAS, and REFEDS highlighted services in different areas that aim to ensure safe and reliable identity authentication. Kantara offers flexibility for different sectors, eIDAS offers a regulated approach for the EU and REFEDS addresses the specific needs of the research and education communities. Understanding their unique approaches and security commonalities is essential to advancing secure digital interactions and increasing identity assurance across diverse organizational environments.

This comparative overview highlights how Kantara, eIDAS, and REFEDS approach identity security, tailored to their specific environments, but with the common goal of ensuring robust, secure, and trusted digital interactions.

Understanding these differences is essential to choosing the appropriate framework to meet the specific security requirements of different organizational environments.

Our future work will focus on developing a robust and reliable system that uses variable security levels to address different security needs.

By implementing a scalable approach to security, our goal is to increase the flexibility and effectiveness of identity assurance mechanisms. This will include a comprehensive assessment of existing frameworks, the integration of advanced authentication technologies, and the establishment of best practices for dynamically managing security levels.

References

[1] (JANET), J. H., & V. NORDH (UNIVERSITY OF GOTHENBURG) W, S. (. (20.05.2010). DELIVERABLE DS3.3.1: EDUGAIN SERVICE DEFINITION AND POLICY INITIAL DRAFT. PROJ DELIVERABLE. 21.

[2] Broeder, D. (2012). *Federated identity Menagement for Research Collaborations CERN-OPEN 2012-006.* Retrieved from http://cds.cern.ch/record/1442597/files/CERN-OPEN-2012-006.pdf

[3] COMMISSION, T. E. (2015, 09 08). *Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002

[4] Ian Neilson, D. G. (2019). Comparison Guide to Identity Assurance Mappings for Infrastructures.

[5] Initiative, K. (2021, 06 8). *Identity Assurance Framework.* Retrieved from https://kantarainitiative.org/identity-assurance-framework/

[6] Initiative, K. (n.d.). *Kantara identity Assurance Framework.* Retrieved from Kantara IAF-1400 Service Assessment Criteria v5.0 : https://kantarainitiative.org/confluence/display/LC/Identity+Assurance+Framework

[7] Initiative, K. (n.d.). *Kantara Identity Assurance Framework.* Retrieved from https://kantarainitiative.org/confluence/display/LC/Identity+Assurance+Framework

[8] Jesus Carretero, G. I.-M., Vasile-Cabezas, M., & Garcia-Blas, J. (2018). Federated Identity Architecture of the European eID System. *ieeexplore.ieee.org*.

[9] Jule Anna Ziegler, U. S. (2021). Making Identity Assurance and Authentication Strength. *International Symposium on Grids & Clouds 2020, ISGC2021*.

[10] Mikael Linden (CSC), N. v. (2017, 04 01). Deliverable DNA3.1:Differentiated LoA recommendations for policy and practices of identity and attribute providers, applicable to research use cases. p. 22.

[11] REFEDS. (n.d.). *REFEDS Assurance Framework and Single-Factor profile in public consultation.* Retrieved from https://refeds.org

[12] Vjollca Shemshi, B. J. (2023). Raising the Trust in Research and Education Digital Services Using Levels of Assurance Profiles. 551-8.

[13] Wolfgang Hommel, M. G. (2016). Level of Assurance Management Automation for Dynamic Identity Federations based on Vectors of Trust. *PIK - Praxis der Informationsverarbeitung und Kommunikation*.

[14] Working, A. A. (2021, 08 24). *REFEDS Assurance Framework Implementation Guidance for the InCommon Federation.* Retrieved from

[15] https://spaces.at.internet2.edu/display/InCCollaborate/Consultation+for+REFEDS+Assurance+Framework+Implementation+Guidance+for+the+InCommon+Federation