IDENTITY & ACCESS FORUM

Powered by SECURE TECHNOLOGY ALLIANCE

AN IDENTITY & ACCESS FORUM EDUCATIONAL BRIEF

What is Identity Assurance?

August 19, 2024

Identity & Access Forum
544 Hillside Road
Redwood City, CA 94062

www.securetechalliance.org

About the Identity and Access Forum

The Identity and Access Forum is a cooperative, cross-industry body dedicated to developing, advancing, and adopting secure identity technologies, including physical and logical access. Through the collaborative efforts of a diverse group of stakeholders, the Forum advocates for market adoption of trusted, user-centric, and interoperable digital identities to ensure safe and seamless access to services across all interactions. The organization operates within the Secure Technology Alliance, an association that encompasses all aspects of secure digital technologies.

Contents

1. Understanding Identity Assurance

What is Identity Assurance?
It is a term that many encounter through work activities and almost everyone does in daily life – but what does it mean and how does it impact you? Why should you care?
This brief, prepared by the Identity & Access Forum of the Secure Technology Alliance, provides a simple, easy to understand explanation for those who are new to the terms associated with identity management, is not intended for subject matter experts or those whose work is centered around identity and its various components, and is the first of several position papers designed to provide an understanding of terminology used in identity. This brief is intended to provide the foundation for future learning.

Why should you care?
It's almost guaranteed that you have or will encounter Identity Assurance when accessing online services or getting a badge to enter a building, perhaps without you knowing it. The concepts of Identity Assurance are intended to protect you, as well as the services that you want to access when engaging with providers that manage those assets, whether for personal use or for business.

Overview
The sections below provide a high-level overview of the three levels of Identity Assurance as adopted and defined in standards published by the National Institute of Standards and Technology (NIST). The closing section provides links to these and additional resources for those seeking more information or a deeper understanding of the term and concepts of "Identity Assurance." The three levels of Identity Assurance cover how and when they are applied, and how service providers determine which level is required to access their managed resources.

While these resources are primarily focused on the United States, similar levels of Identity Assurance are used globally, although there may be slight differences between them. For example, IAL2 may not map directly to the European Level 2. Future educational papers by the Alliance's Identity and Access Forum will expand on the Identity Assurance Levels (IALs), and then explore related assurance levels that further support protected access to a variety of services, i.e., Authentication Assurance Levels (AALs) and Federation Assurance Levels (FALs).

The Three Levels of Identity Assurance
Identity Assurance refers to the unique attributes provided by an individual in order to onboard, register, or enroll with service providers that manage assets that an individual wishes to access. In some cases, service providers may establish or issue some form of logical or physical credential that an individual will use to gain access to the service provider's offerings, such as a unique ID and password, a license, a token, or a physical access card.

The owner of a service, frequently referred to as a Relying Party (RP), will decide whether an individual should be granted access to services provided and what level of assurance that that individual must attain in order to access those services. The required level of assurance is governed by the impacts or risks that might occur if a bad actor's (or unauthorized user's) actions might compromise or degrade access to a service and its data, which may result in damage to assets, or cause financial loss or physical harm to other individuals. Hence, depending on the risk factor, different levels of identity proofing and individual attributes are required when establishing an identity within a Relying Party's purview.

For example:

Identity Assurance Level 1 (IAL1): Social media platforms or streaming services may choose not to require any proof of identity, simply establishing a user ID and password, and ensuring access to those services are paid for. This is because the risk of unauthorized use is low.

Identity Assurance Level 2 (IAL2): Meanwhile, a bank will require in-person proof of identity (e.g., driver's license or passport) when opening a new checking account. This is because the risk of fraudulent activity and financial loss is moderate, since any identity-related compromise is localized to an individual, and not to the financial institution, in most cases.

Identity Assurance Level 3 (IAL3): To gain access to high security areas or websites containing highly sensitive data or physical assets (such as sensitive governmental facilities/rooms or medical record archives). Multiple forms of identity, biometrics (facial photo and/or fingerprints), background checks, and other certification documents may be required for programs such as TSA PreCheck.
Identity Assurance simply provides confidence that the identity provided by the individual to the Relying Party owner of the services is valid and meets the risk level(s) associated with the nature of the resources, assets, data and/or services managed by the Relying Party, to which an individual may gain access.

2. Infographic

The following infographic provides a conceptual summary of the three levels of Identity Assurance.

Levels of Identity Assurance

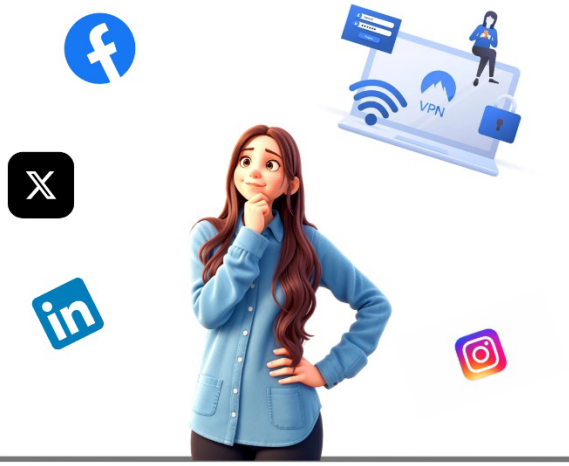
IAL 1 - Low Risk

Meet Sally

Someone is self-asserting that they are Sally through logins and passwords.

There is no requirement to link the person to a specific real-life identity.

This is all remote.



IAL 2 - Moderate Risk

Meet Jack

Jack is providing evidence of who he is with solid identification which can be verified.

IAL2 requires two forms of identification in which one must be a driver license, passport, or other verifiable credential.

Biometrics are optional.

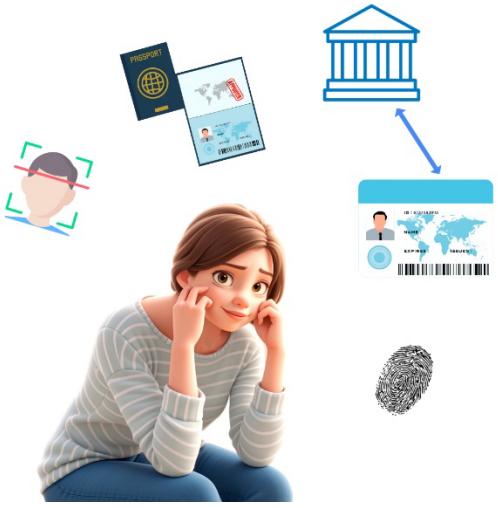
This can be done in person or remotely.

IAL 3 - High Risk

Meet Meghan

Meghan is providing the highest level of identity assurance with solid forms of identification AND a form of biometrics.

This must be done in person or remotely with supervision.



3. Additional Resources

The distinction between the three IALs is very straightforward and determining which level is appropriate is a decision each Relying Party must make based on the information and/or assets an individual is accessing. What risk is associated with wrongful access? What risk is the RP willing to assume?

- Look for more detailed briefs from the Secure Technology Alliance on IALs, AALs, and FALs, and specific use cases in the coming months. Meanwhile, if you want to get involved in the Alliance or the Identity & Access Forum, please visit:
  - https://www.securetechalliance.org/membership-information or https://www.securetechalliance.org/identity-and-access-forum/.

- For additional information on Identity Assurance levels and procedures for enrollment and identity proofing, see the following resources:

  - NIST SP 800-63-3, "Digital Identity Guidelines"
  - NIST SP 800-63A, "Digital Identity Guidelines: Enrollment and Identity Proofing Requirements"
  - NIST FIPS-199, "Standards for Security Categorization of Federal Information and Information Systems"

- IDManagement.gov
  - Digital Identity Risk Assessment Playbook (idmanagement.gov)

- Cyber Insight "Unlocking NIST's Identity Assurance Level 3: The key to Strong Cybersecurity"
  - https://cyberinsight.co/what-is-nist-identity-assurance-level-3/

- Identity Management Institute "Identity Proofing"
  - https://identitymanagementinstitute.org/identity-proofing/

4. Glossary: Terms

For Identity Assurance terms used within this document see below.

- **IAL – Identity Assurance Levels**
- **AAL - Authenticator Assurance Levels**
- **FAL - Federated Assurance Levels**

5. Acknowledgements

Participants
Christine Cobuzzi – Get Group NA
Mark Dale – XTec
Phil Edge – Intercede
Deb Ferril – Ascend
Patrick Kelly - Mastercard
Joel Perez - Get Group NA
Gerry Smith – Identification Technology Partners (IDTP)
Greg Stegall - NextgenID

6. Legal Notice

The Identity & Access Forum endeavors to ensure, but cannot guarantee, that the information described in this document is accurate as of the publication date. This document is intended solely for the convenience of its readers, does not constitute legal advice, and should not be relied on for any purpose, whether legal, statutory, regulatory, contractual, or otherwise. All warranties of any kind are disclaimed, including but not limited to implied warranties of merchantability or fitness for a particular purpose, and warranties of title, noninfringement or regarding the accuracy, completeness, or adequacy of information herein.