

IDENTITY & ACCESS FORUM

Powered by  SECURE TECHNOLOGY ALLIANCE

AN IDENTITY & ACCESS FORUM EDUCATIONAL BRIEF

Digital Identity vs. Digital ID

October 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.

Copyright ©2024 Identity & Access Forum and Secure Technology Alliance. All rights reserved. Comments or recommendations for edits or additions to this document should be submitted to: info@securetechalliance.org.

Contents

About the Identity and Access Forum	2
1. Introduction	4
2. Historical Perspective.....	5
3. What is Digital Identity?.....	6
4. What is Digital ID?	6
5. Digital Identity, Digital ID, and Identity Assurance Relationship Graphic.....	8
6. Acknowledgements	9
7. Legal Notice	10

1. Introduction

A famous (and still relevant) cartoon from 1993 (Figure 1) insightfully portrayed Internet online anonymity, which exemplified the potential needs for actually verifying who or what is actually on the other end of online and offline digital transactions. With the arrival and increased adoption of Digital Identities and using Digital Identifiers (Digital IDs) to access online and other services, trusting, and verifying end users is essential to combat fraud and misuse.



Figure 1 – Trust is a constant challenge ¹

Linking a Digital Identity to an individual through identity information, and optionally a biometric strengthens the level of assurance or trust levels at the creation of Digital Identities and using Digital IDs. Other mechanisms can be used to provide a greater level of assurance in addition to traditional methods.

The stronger the connection of the individual to a Digital Identity, the lower the risk to providers accepting them to provide access to their trusted services.

This paper intends to define and clarify the various manifestations of Digital Identities that a person or non-person (e.g., device) entity may have, and the various Digital Identifiers/IDs that a Digital Identity may possess in order to gain access to desired services and other resources. Future projects will explore each of these areas in detail.

¹ Cartoon credited to Peter Steiner, 1993, [The New Yorker](#)

2. Historical Perspective

For the past seventy years, a person's identity has been defined through international treaties. The "descriptors" following a person's name in Passports were formalized by a 1947 United Nations treaty pertaining to international airplane passengers. Equivalent requirements were made law within the U.S. as driver's license requirements, most recently updated by the REAL ID Act regulations.

That identity is used by the federal and by state governments for benefits and taxes and includes both biographical data and a physical residence address. Physical descriptors including a digital record of the license holder's face are required under the REAL ID Act.

The first digital identities began in the 1950s as universities and businesses began using computers to maintain accounting and other production services. Those digital identities were for computer users to allow system managers to restrict access to employees' abilities to input data, generate reports, and maintain computer operations.

Beginning in the 1990s, internet service providers began providing email and internet access to allow people to communicate through services accessible via browsers and software applications (apps). These evolved to the current time where millions of users own one or more Digital Identities and may have multiple Digital IDs for accessing buildings, their computers, and online services.

3. What is Digital Identity?

Digital Identity is a broader concept encompassing all aspects of an individual's or entity's online presence and information. Digital Identity is your online persona, spread across multiple platforms. It is the means through which a person, device, or organization can make its virtual identities portable.

- **Identity** – Unique Person (Individual) or Non-Person Entity (e.g., organizations, hardware devices, software applications, and information artifacts)
- **Digital Identity** – An individual's persona within a specific digital context. A Digital Identity is the unique representation of an individual engaged in a logical or physical digital service transaction. Digital Identity is always unique in the context of a digital service.

Components:

- **Attributes:** Personal data such as name, date of birth, email address, professional credentials/qualifications, etc.
- **Behavioral Data:** Online activities, purchase history, and browsing patterns.

Usage:

- Used broadly in various contexts, such as social media, online banking, e-commerce, and other online services where distinction of individuals is required.
- Helps in creating a personalized user experience and enhancing security through distinguishing individualized access to services.

Characteristics:

- Broader Ecosystem of Issuers (not necessarily government-issued).
- Can be fragmented across different platforms and services.
- Dynamic and can change over time based on user behavior and updates.

4. What is Digital ID?

Digital ID is a specific, verified form of digital identity used for official purposes. It is your official authenticated digital representation, such as a digital passport or driver's license. A Digital ID is an authenticatable/verifiable set of attributes (potentially in the form of a “Credential”, online account, or a token) associated with a Digital Identity. Provider(s) of Services, (Relying Parties or Digital ID Verifiers) authenticate the Digital IDs. This allows individual subjects to leverage their rights and privileges associated with logical and/or physical digital services within Relying Parties’ governing authentication and authorization policies.

During transactions when accessing a Relying Party's services, a Digital ID is used to link an individual to their Digital Identity.

Components:

- **Verified Information:** Personal details verified by an Issuing Authority, such as biometric data, government-issued ID numbers, and official documentation.
- **Authentication Mechanisms:** Secure methods to prove the authenticity of the digital ID such as digital signatures, cryptographic keys, or biometric verification.

Usage:

- May be used for official purposes requiring high levels of security and trust, such as e-government services, financial transactions, and access to secure facilities.
- Facilitates online transactions and interactions that require proof of identity, often ensuring compliance with legal and regulatory standards.

Characteristics:

- Issued and certified by a recognized authority, this may be a government.
- Controlled by the Issuing Authority or Relying Party.

Where Do Biometrics Fit in?


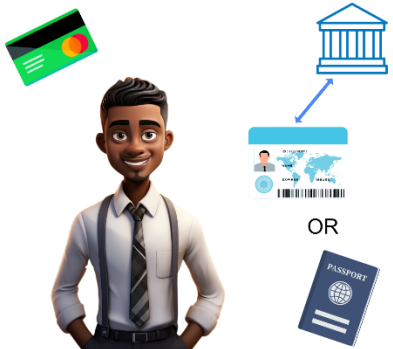

Biometrics serve as a critical tool for ensuring that the identity being presented is the correct individual, enhancing the security and trustworthiness of digital interactions.

- **In Digital Identity:**
 - Biometrics may enhance security and user convenience in a digital environment.
 - They are one of many factors contributing to a user's overall digital identity.
- **In Digital ID:**
 - Biometrics are essential for the creation and verification of secure, government-issued digital identities.
 - They may provide an additional layer of trust and are often used in official and high-security contexts.

5. Digital Identity, Digital ID, and Identity Assurance Relationship Graphic

The following infographic provides a conceptual summary of the three levels of Identity Assurance and examples of Digital Identities and associated Digital IDs. For more information and/or understanding of Identity Assurance Levels see [What is Identity Assurance?](#)

Levels of Identity Assurance

<p>IAL 1 - Low Risk</p> <p>Meet Sally</p> <p>Someone is self-asserting that they are Sally through logins and passwords.</p> <p>There is no requirement to link the person to a specific real-life identity.</p> <p>This is all remote.</p>		<p>Examples: Social media, content streaming service, etc.</p> <p>Digital Identity: Online service account, payment info, etc.</p> <p>Digital ID: Username and password</p>
	<p>IAL 2 - Moderate Risk</p> <p>Meet Jack</p> <p>Jack is providing evidence of who he is with solid identification which can be verified.</p> <p>IAL2 requires two forms of identification in which one must be a driver license, passport, or other verifiable credential.</p> <p>Biometrics are optional.</p> <p>This can be done in person or remotely.</p>	<p>Examples: Building/room access, online business or Government accounts</p> <p>Digital Identity: Moderate specific identity info and attributes, etc. in RP System of Records, as required.</p> <p>Digital ID: One or more Tokens, Smartcards, Digital Certificates, etc.</p>
<p>IAL 3 - High Risk</p> <p>Meet Meghan</p> <p>Meghan is providing the highest level of identity assurance with solid forms of identification AND a form of biometrics.</p> <p>This must be done in person or remotely with supervision.</p>		<p>Examples: Highly secure facility/room, TSA PreCheck, etc.</p> <p>Digital Identity: Stronger specific identity info, attributes, background check status, etc. in RP System of Records, as required</p> <p>Digital ID: One or more Tokens, Smartcards, Digital Certificates, biometrics, and other form factors that can be used to authenticate Digital Identities</p>

Copyright 2024 - Secure Technology Alliance - All Rights Reserved

6. Acknowledgements

Participants
Andreas Aabye - Visa
Pedro Barreda – Veridos
Christine Cobuzzi – Get Group NA
Mark Dale – XTec
Deb Ferril – Ascend
Won Jun - Intercede
Tom Lockwood – Vestige Digital
JB Milan - HID
Neville Pattinson - Thales
Gerry Smith – IDTP
Henk van Dam - FIME
Brian Zimmer - Idsecuritynow

7. 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.