Dissecting NIST 800-63 Digital Identity Guidelines

KEY CONSIDERATIONS FOR SELECTING THE RIGHT MULTIFACTOR AUTHENTICATION

HID®

Embracing Compliance

▶ More and more business is being conducted digitally — whether at work as an employee or at home as a consumer or citizen. Yet, the **digital identities** that protect access to these services have not kept pace with that expansion.

The challenges of identifying and authenticating users of network systems are prevalent, as evidenced by the fact that the majority of data breaches are still caused by weak or stolen credentials.

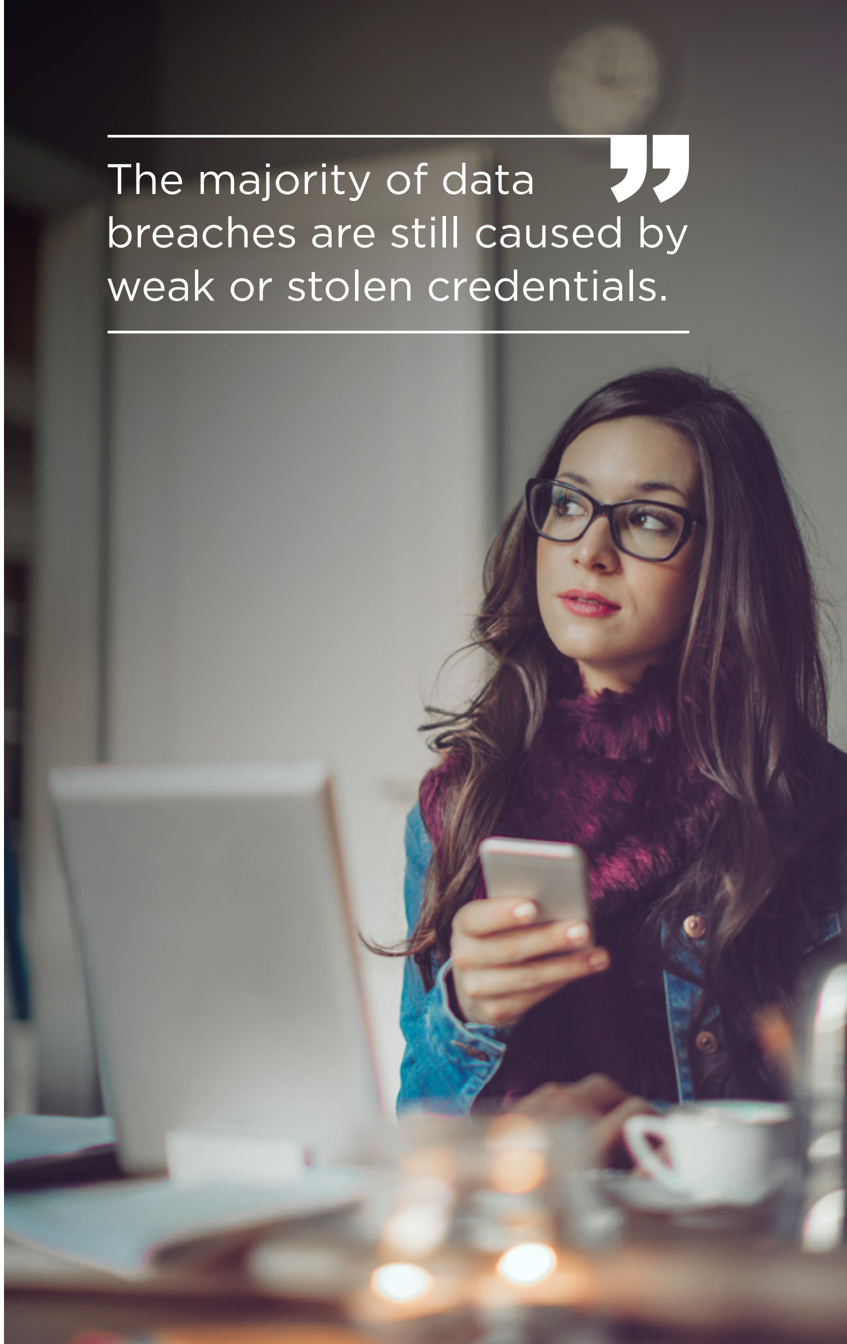
To complicate things, employees, consumers and citizens have different needs in term of convenience, security, cost and user experience. This eBook breaks down the assurance levels, risk considerations and options for becoming NIST 800-63 compliant.

Ensuring Risk-appropriate Security with Diverse Population Needs

To address application and use case challenges, the National Institute of Standards and Technologies (NIST) published Digital Identity Guidelines SP 800-63-3.

SP 800-63 is a set of documents that provides guidelines on how to identify and authenticate users over internal networks or the Internet.

SP 800-63 does not require a set level of security. Rather, it provides a methodology for organizations to determine a level of risk for each application and use case and to provide a set of options to mitigate those risks.



> The majority of data breaches are still caused by weak or stolen credentials.

Levels of Assurance (LOA): Confidence in Digital Identities

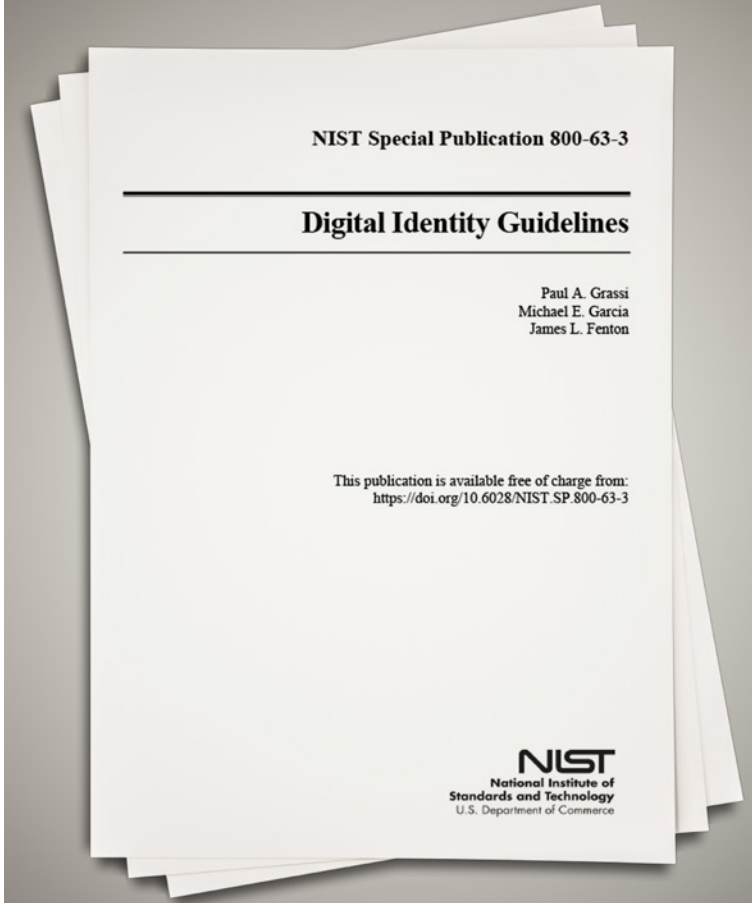
Digital identities do not fit into the "one size fits all" category. Not all applications and use cases require the same assurance level (i.e., security level).

The assurance level is a combination of identity, authentication and federation. SP 800-63 defines a separate assurance level for each of those components, providing greater flexibility to application developers and IT security professionals.

Assurance levels are defined as:

- 1 (low)
- 2 (medium)
- 3 (high)

SP 800-63 then provides a methodology to assign the appropriate level to each component, looking at risk factors covering areas such as inconvenience, financial loss, safety, data breach and others. Once you've determined the assurance level, SP 800-63 provides a list of capabilities that are appropriate for that level.



NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Identity Assurance Level (IAL): The Identity Proofing Process

When you create a digital identity in an IT system, the first question to ask is, ***"How is this digital identity related to a real-world identity?"*** In some cases, you may want to provide anonymity to your users (e.g., a whistle blower application). In others, you may be required to reliably link a digital identity to a real-world person (e.g., "Know Your Customer" requirement for the financial industry).

An Identity Assurance Level provides the flexibility to account for these different scenarios. SP 800-63 defines 3 IALs and the identity proofing processes to collect and validate the identity of the user.

IAL 1	No link to a real-life identity
IAL 2	Evidence to prove real-life identity; can be remote or in person
IAL 3	Physical presence required for identity proofing

Authenticator Assurance Level (AAL): The Identity Authentication Process

Once you've performed identity proofing for a new user, you want to be reasonably sure that subsequent attempts at access to your application are from the right user, and not someone else impersonating the user.

The Authenticator Assurance Level defines the level of assurance that the returning user is who they assert to be.

Not all applications require the same level of assurance. Making an online restaurant reservation does not require the same assurance as accessing your taxpayer information or accessing a power generation system.

SP 800-63 defines 3 AALs and the processes and methods to authenticate the returning user.

AAL 1	**Single or multi factor authentication**
AAL 2	**Multi factor authentication with approved cryptography**
AAL 3	**Hardware based multi factor authentication, with approved cryptography**

Authenticator Types

SP 800-63 allows for many authenticator types, and combining authenticators can increase the assurance level.

Memorized Secret

Look-Up Secret

Out-of-Band Devices

Multi-Factor OTP Device

Single-Factor Cryptographic Software

Single-Factor One-Time Password (OTP) Device

Single-Factor Cryptographic Device

Multi-Factor Cryptographic Software

Multi-Factor Cryptographic Device

Authenticator Assurance Details

SP 800-63 provides detailed requirements for authenticators as well as the systems verifying the authentication and the lifecycle management of the authenticators. Some requirements are specific to the authenticator type and some apply to all types.

Authenticator privacy and usability are also considered. Of note, biometric use for authentication is limited only as part of multi-factor authentication with a physical authenticator. Biometric as part of identity proofing (IAL) does not have such a limitation.

Similarly, risk-based and adaptive authentication techniques can be used to augment the security of the system but cannot be used as a primary or secondary authentication factor.

Use of a Public Switched Telephone Network (i.e., SMS) is considered RESTRICTED, and the risk should be carefully considered before using it for authentication.

FIPS 140-2 LEVEL REQUIREMENT	
AAL 1	Level 1 on the verifier (i.e. relying party)
AAL 2	Level 1 on the verifier and authenticator
AAL 3	Level 1 on the verifier Level 2 overall for multi-factor hardware authenticator (with level 3 for physical security) Level 1 overall for single factor hardware authenticator (with level 3 for physical security)

SP800-53 MAPPING	
AAL 1	Low
AAL 2	Moderate
AAL 3	High

Federation Assurance Level (FAL): Assertions in a Federated Environment

Federation is the process that allows sharing user authentication and user attributes across networked systems. It allows a Relying Party (RP) application to leverage an Identity Provider (IdP) to authenticate users and retrieve users' attributes (e.g., names and addresses).

Federation is useful, for example, when an application wants to let different user populations interact; but the most prevalent use is for cloud applications that want to let their customers control the authentication of their users — providing more control to the customer within the IdP to avoid the need for multiple entries of generic user attributes like names and addresses.

To achieve that goal, the Identity Provider and Relying Party typically exchange assertions. A Federation Assurance Level (FAL) defines how the IdP and RP trust the assertions they exchange.

SP 800-63 defines three FAL levels and the processes to register identities in RPs, and how assertions are protected and presented across the federation.

FEDERATION ASSURANCE LEVEL (FAL)	
FAL 1	RP can receive a bearer assertion, signed by the IdP using approved crytography
FAL 2	Assertion is encrypted so that only the RP can read it
FAL 3	Assertion contains subscriber's proof of possession (i.e. cryptographic signature)

FAL EXAMPLES	
FAL 1	OpenID Connect Basic Client profile or Security Assertion Markup Language (SAML) Web SSO Artifact Binding profile
FAL 2	OpenID Connect ID Token or SAML Assertion encrypted with the RP's public key
FAL 3	Token Binding where token signature is generated from a hardware token

HID and SP 800-63

HID Global offers more authentication options than anyone else and can help your organization achieve SP 800-63 compliance, regardless of the assurance level required.

We can easily accommodate the need for multiple authentication solutions within the same organization when requirements vary by group.

Recent Awards

- 2018 Top Multi-Factor Authentication Solution Provider, *Enterprise Security Magazine*
- 2018 Most Innovative Product for Cyber Security Discovery, *Cyber Defense Magazine*
- 2018 New Product of the Year, *Info Security Product Guide Global Excellence Award*
- 2017 Best IAM and CMS Product, *Security Today Government Security Awards*
- 2016 Best Identity Management Platform, *GSN Homeland Security Awards*
- 2016 Top 10 Fastest Growing Security Companies, *SR 2016 Cyber Security Companies*

HID OFFERS THE MOST AUTHENTICATION OPTIONS FROM ONE TRUSTED SOURCE

FIDO & PKI Smart Card

Push Notification

Virtual Smart Card

FIDO & PKI Smart USB Token

Digital Certificate

One-time Password Token

BlueTooth Token

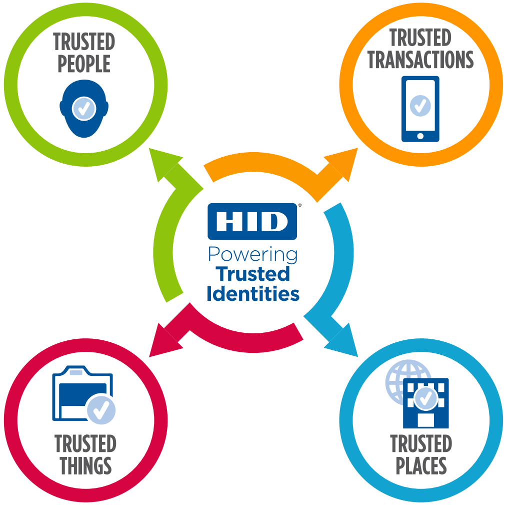
Risk-based

Biometric

Why HID Global?

At HID Global, we *Power Trusted Identities*. That means we take a holistic approach to identity and access management, with the broadest portfolio of user authentication solutions to meet the needs of a variety of industries, across a variety of touchpoints.HID's portfolio includes:

- the widest selection of authenticators
- the broadest portfolio of identity and access management solutions.



Interested in learning more about
Authentication Solutions from HID Global?

LEARN MORE

hidglobal.com

2019-03-19-hid-iams-nist-guidelines-eb-en PLT-04335