Digital Insanity: Exploring the Flexibility of NIST Digital Identity Assurance Levels

Kenneth Myers
School of Technology and Innovation, Marymount University, Arlington, Virginia, USA

Kmm57090@marymount.edu

Abstract: NIST Special publication 800-63-3 present a new risk management concept on digital identity. It includes various harm categories to determine an appropriate assurance level for identity proofing, authentication, and federation. These three distinct approaches are highlighted to give flexibility in protecting systems. This paper explores if this is a realized flexibility through developing a tool to test assurance level and component flexibility. It also identifies appropriate MFA levels given different levels of risks and makes three recommendations to help improve adoption of the NIST digital identity guidelines.

Keywords: Assurance Level, Digital Identity Risk Assessment, Digital Identity, Identity Proofing, Authenticator, Federation

1. Introduction

Digital identity risk management is a new field of risk management. It ensures that the right person has access at the right time and supplements existing NIST Risk Management Framework processes. NIST first introduced Digital identity risk management through the third revision of Special Publication 800-63 in 2017. Similar to other risk management frameworks, it identifies specific controls based on an assessed adverse impact level. This identity risk management framework is unique because it dissects digital identity assurance into three elements: identity, authenticator, and federation assurance levels.

1. Identity assurance - identity proofing process.
2. Authenticator assurance - authentication process.
3. Federation assurance - assertion in a federated environment.

The reason for the dissection is that "combining proofing, authenticator, and federation requirements into a single bundle sometimes have unintended consequences and can put unnecessary implementation burden on the implementing organization" (Grassi, Garcia and Fenton, 2017, p.17). Another benefit is the flexibility in using higher assurance authentication without requiring high assurance identity proofing based on the risk assessment.

- Research question 1 - Does dissecting digital identity into specific components make the component risk assessment more flexible?
- Research Questions 2- Should all transactions use an MFA?
- Research Question 3 - Should all transactions use phishing-resistant MFA?

This dissection approach in identity control families is like other risk management frameworks.

- NIST Risk Management Framework control family.
- Cyber Security Framework subcategory.
- Center for Internet Security Critical Security Controls control group.

Within the NIST digital identity guidelines is a digital identity risk management outlining impacts per harm category. There are six harm categories used to determine an appropriate assurance level.

1. Potential for inconvenience, distress, or damage to standing or reputation.
2. Potential impact on financial loss.
3. The potential impact of harm to agency programs or public interest.
4. The potential impact of unauthorized sensitive information release.
5. Potential impact on personal safety.
6. The potential impact of civil or criminal violations.

Who should conduct this risk assessment, such as the application owner, a risk professional, or a cross-functional team? A user must select a risk level from low to high within each harm category. Low means limited, short-term, while high means severe long-term impact. NIST includes a flow chart to help determine a level and shortcuts, but the process could be more intuitive.

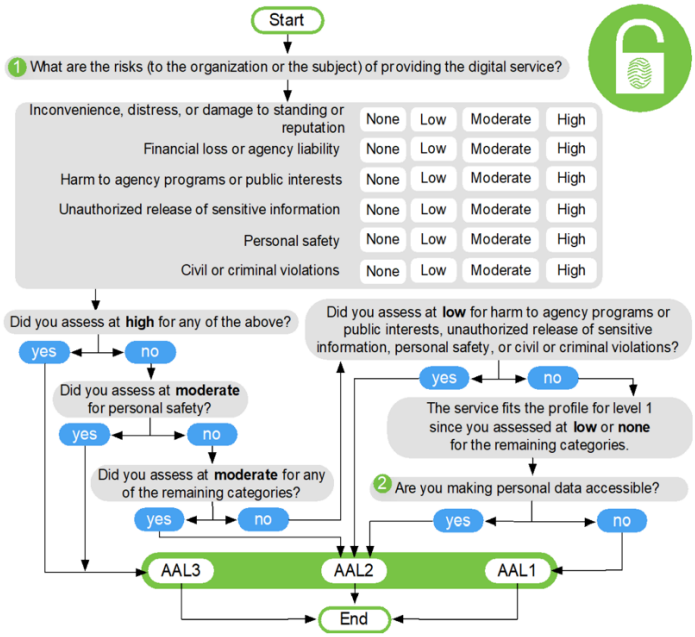

Figure 1: NIST 800-63-3 Authenticator Assurance Level Flow Chart (Grassi, Garcia and Fenton, 2017)

In 2020, the Identity, Credential, and Access Management Subcommittee formed a digital identity risk assessment working group to develop an identity risk assessment playbook. This playbook (GSA, 2021) outlines a process to conduct a risk assessment and record the findings in a risk acceptance statement. The playbook also contains more intuitive flow charts.

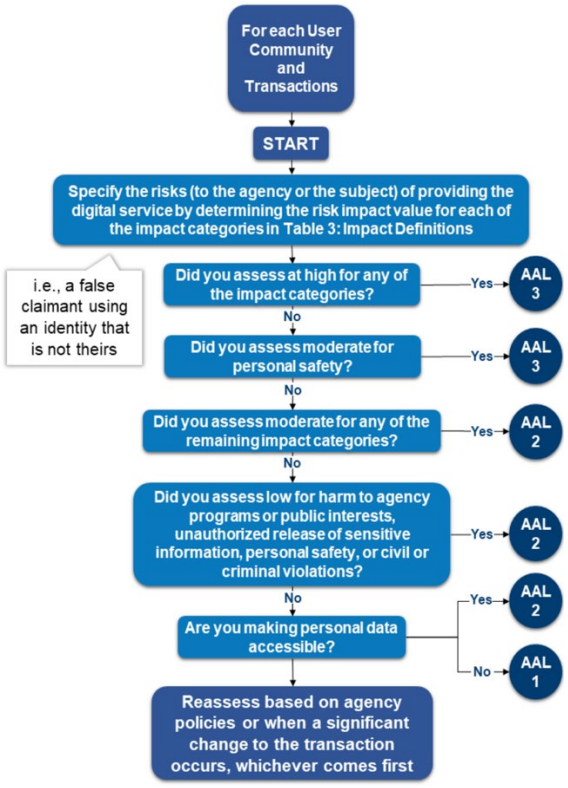

Figure 2: GSA Digital Identity Risk Assessment Playbook Authenticator Assurance Level Flow Chart (GSA, 2021)

The following section highlights adoption trends identified through a literature review.

2. Literature Review

Adopting the NIST Digital Identity Risk Management guidelines appears limited both within the Federal Government and outside. Federal agencies must implement Digital Identity Risk Management and any successive versions according to Office of Management and Budget Memo 19-17 (2019). One may assume agencies have fully adopted these NIST identity guidelines. However, an OMB memo does not have the same authority as a public law like the Federal Information Security Management Act (FISMA). FISMA requires agencies to implement the NIST Risk Management Framework to authorize IT systems (S.2521, 2014). Despite this, there is some indication of government-wide adoption similar to the NIST Risk Management Framework or the Federal Risk and Authorization Management Program. A few leading indicators of government and industry use point to this assessment.

- Other NIST risk management frameworks have multiple agency or industry adoption examples. Nine other languages have translated the NIST Cybersecurity Framework (2022)! The Digital Identity Framework has limited informative resources but does include a frequently asked question sheet, implementation resources, and conformance criteria.
- OMB memo 19-17 points to idmanagement.gov for a list of trusted services that align with NIST 800-63-3. The trust services page on idmanagement.gov only lists identity credentialing services (GSA, 2022a). There needs to be a list of services at various assurance levels.
- NIST requires an MFA when personal information is stored and when self-asserted (Grassi, Garcia and Fenton, 2017, p. 31). A quick scan of publicly available federal login sites that require a user's personal information to create an account, such as recreation.gov, some sba.gov login sites (Capital Access Financial System and Shuttered Venue Operators Grant, and Restaurant Revitalization Award Portal), and the federal training website fedvte.usalearning.gov allow someone to create an account or login without using an MFA. There is also a large number that does enforce MFA through integration with login.gov.

Some organizations have published supplemental material as well.

- MITRE (2020) published a methodology for unsupervised remote identity proofing (identity assurance level 2) and supervised remote in-person proofing (identity assurance level 3).
- NSA (2020) published a fact sheet that assessed multi-factor authenticator solutions to an Authenticator Assurance Level.
- The DoD ICAM Reference Design (2020) includes digital identity assurance levels.

Some vendors also have supplemental material on how their products align with the NIST guidelines.

- Microsoft (2022a) published a detailed approach to implementing authenticator assurance levels.
- Forgerock (2021) published a white paper on their product alignment with identity, authenticator, and federal assurance levels.

One common trend in almost all materials is a need for more clarity in assessing an assurance level. In other words, all material helps explain each level and conformance criteria on each level, but little to help explain how to determine a level. This is necessary because multiple examples of companies choosing the wrong authenticator type exist. Not all MFA are secured equally.

A very prevalent attack today is an MFA bypass or fatigue attack. This technique uses repeated push notifications to fatigue the user into accepting the request (Cimpanu, 2022). This new attack is used throughout 2021. Another typical authenticator attack is an MFA interception attack. This attack style intercepts an MFA piece of knowledge, such as an SMS pin or mobile application one-time PIN (Jansen, 2021), for an attacker to replay. An MFA interception is sometimes combined with a SIM jacking attack so that an SMS pin will arrive on an adversary's device. These types of authenticators are Authenticator Assurance Level 2.

Microsoft highlights specific accounts that are attractive for credential theft (2022b). These accounts include the following.

1. Administrator accounts with escalated security privileges, such as domain accounts or help desk personnel.
2. Manager accounts to approve access requests or other higher-risk transactions.
3. Very Important People include executives, legal staff, product planners, and researchers.

These higher-risk accounts roughly align with the same account types identified in the U.S. Government Privileged Identity Playbook (2022). These risky accounts should have the strongest authenticator or Authenticator Assurance Level 3. What about general user accounts? As mentioned earlier, following the NIST risk criteria, the risk of a general user account is most likely an Authenticator Assurance Level 2, which is susceptible to phishing. The following section outlines the research approach to explore the research question.

3. Research Method

One identified drawback of the NIST digital identity guidelines is the complicated nature of conducting an assessment. This is consistent in both the NIST guidelines, but also in the Digital Identity Risk Assessment Playbook. This paper developed a simple, excel-based tool to make the process more user-friendly. The tool's purpose is to test and verify the flexibility of the three identity components. This tool has the following features.

1. A consolidated assessment interface that combines identity, authentication, and federation assurance levels.
2. A user adjusts a set of drop-down menus to pick the desired risk level.
3. A calculation to automatically determine the correct assurance level based on the NIST digital identity guidelines flow charts.
4. A terminology tab of harm categories and risk descriptions.

Test 5 - PII Yes, Personnal safety moderate				2	1	1
Is PII or PHI collected and does it need to be validated?	Yes & I Don't Know			2		
Impact Category	Select Impact Definition*	Impact Level		IAL	AAL	FAL
Inconvenience, distress, or damage to standing or reputation to the agency	t worst, limited, short-term inconvenience, distress, or embarrassment to any part	Low		1	1	1
Financial loss or agency liability	r inconsequential financial loss to any party, or at worst, an insignificant or incons	Low		1	1	1
Harm to agency programs or public interests	Not Applicable	Not Applicable		1	1	1
Unauthorized release of sensitive information	Not Applicable	Not Applicable		1	1	1
Personal safety to users	Not Applicable	Not Applicable		1	1	1
Civil or criminal violations	Not Applicable	Not Applicable		1	1	1

Figure 3: NIST 800-63-3 Digital Identity Risk Assessment Tool

A series of test conditions were used in the tool to test the flexibility of both the components and the assurance levels.

- Component flexibility is the potential to test each component independently.
- Assurance level flexibility is the potential to test each assurance level's independence from the other.

Six test cases were developed and run through the tool. Only two variables are tested on whether the transaction included Personally Identifiable Information (PII) and one randomly chosen harm category and level.

1. Includes PII, All categories low or N/A
2. No PII, Any category moderate except personal safety.
3. Includes PII, Sensitive information high
4. Includes PII, Financial Loss high
5. Includes PII, Personal safety moderate
6. No PII, All categories low or N/A

The following section provides the test results and analysis.

4. Analysis

The following results were determined using the tool.

Table 1: Risk Assessment Results

Test Case	Identity Assurance Level	Authenticator Assurance Level	Federation Assurance Level
#1. Includes PII, All categories low or N/A	2	2	1
#2. No PII, Any category moderate except personal safety.	2	2	2
#3. Includes PII, Sensitive information high	3	3	3
#4. Includes PII, Financial Loss high	3	3	3
#5. Includes PII, Personal safety moderate	3	3	3
#6. No PII, All categories low or N/A	1	1	1

Two interesting observations from the tests.

1. There is component flexibility. They can do this if someone wants to assess only one or two of the three components.
2. There does not appear to be assurance-level flexibility. If an assessed harm category is high or moderate, this level persists through the identity components.

To answer research question 1, dissecting digital identity into specific components does give component flexibility but not level flexibility. The two remaining research questions are answered through the literature review and the test results. The only test cases where MFA (Authenticator Assurance Level 2) was not required were test cases where no personal data and no risk in the transaction. It is a recommendation from the Digital Identity Risk Assessment Playbook not to consider a login based on these indicators (GSA, 2021). The question of whether all accounts should use phishing-resistant MFA points to yes. Most current forms of MFA, including various one-time pins, are susceptible to MFA interception and fatigue-style attacks. A phishing-resistant authenticator disrupts adversary in the middle tactics to steal credentials.

This research paper arrived at three additional recommendations.

1. If the federal government wants wide adoption, consider including the NIST digital identity guidelines in public law or convert it to a FIPS publication. Either approach would require federal agencies to implement digital identity risk management.
2. Given the susceptibility of most Authenticator Assurance Level 2 authenticators, NIST should update their guidelines only to specify phishable MFA options for non-enterprise use cases. In contrast, phishing-resistant MFA should be used for all enterprise or low to moderate-risk transactions.
3. Since the harm categories are consistent across each assurance level, consolidate the risk determination flow charts.

5. Conclusion

This research explored the risk management subfield of digital identity. It tested the flexibility of the component approach but also the assurance levels. Six test cases were developed and tested and found a need for more flexibility in assurance levels. This paper also explored two additional research questions if all accounts need MFA and if all accounts should only use phishing-resistant MFA. Multiple attack techniques highlight the susceptible nature of one-time pin and push notifications to compromise. Additionally, the NIST risk assessment highlights that all transactions with PII and low to moderate risk should have MFA.

This research makes three additional recommendations.

1. If the federal government wants wide adoption, consider a public law that requires federal agencies to implement digital identity risk management.
2. Given the susceptibility of most Authenticator Assurance Level 2 authenticators, NIST should update their guidelines only to specify phishable MFA options for non-enterprise use cases. In contrast, phishing-resistant MFA should be used for all enterprise or low to moderate-risk transactions.
3. Since the harm categories are consistent across each assurance level, consolidate the risk determination flow charts.

This research can be further extended through continued development of a tool into a public website resource or into a GitHub code repository. Additionally, explore whether two authenticator assurance levels, phishable and phishing—resistant are a more modern approach.

Acknowledgements

I want to thank my cyber risk professor, Dr. Michelle Liu, for mentoring me through the development of this paper.

References

Cimpanu, C. (2021) *Russian hackers bypass 2FA by annoying victims with repeated push notifications*. *The Record by Recorded Future*. Available at: https://therecord.media/russian-hackers-bypass-2fa-by-annoying-victims-with-repeated-push-notifications/ (Accessed: December 2, 2022).

DoD. (2020) *Department of Defense Enterprise ICAM Reference Design*. DoD CIO. Available at: https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD_Enterprise_ICAM_Reference_Design.pdf (Accessed: December 1, 2022).

Forgerock. (2021) *ForgeRock and NIST Special Publication 800-63-3*. Available at: https://www.forgerock.com/resources/whitepaper/forgerock-and-nist-special-publication-800-63-3 (Accessed: November 20, 2022).

Grassi, P. A., Garcia, M. E., and Fenton, J. L. (2017). *Digital identity Guidelines*. Special Publication, 800(63–3). Available at: https://doi.org/10.6028/nist.sp.800-63-3/ (Accessed: November 20, 2022).

GSA. (2021, November 17). *Digital Identity Risk Assessment Playbook*. FICAM Architecture. Available at: https://playbooks.idmanagement.gov/playbooks/dira/ (Accessed: December 2, 2022).

GSA. (2022a, September 21). *Trust Services*. idmanagement.gov. Available at: https://www.idmanagement.gov/buy/trust-services/ (Accessed: November 22, 2022).

GSA. (2022b, September 25). *Privileged Identity Playbook*. idmanagement.gov. Available at: https://playbooks.idmanagement.gov/playbooks/pam/ (Accessed: November 22, 2022).

Jansen, W . (2021, January 12). Abusing cloud services to fly under the radar. Available at: https://research.nccgroup.com/2021/01/12/abusing-cloud-services-to-fly-under-the-radar/ (Accessed: November 23, 2022).

Microsoft. (2022a, September 15). *Azure Active Directory identity standards overview - Microsoft Entra*. Microsoft Learn. Available at: https://learn.microsoft.com/en-us/azure/active-directory/standards/standards-overview/ (Accessed: November 23, 2022).

Microsoft. (2022b, June 8). *Attractive Accounts for Credential Theft*. Microsoft Learn. Available at: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/attractive-accounts-for-credential-theft (Accessed: November 26, 2022).

MITRE. (2020, May 1). *Enrollment and Identity Proofing Practices Statement Templates*. MITRE. Available at: https://www.mitre.org/news-insights/publication/enrollment-and-identity-proofing-practices-statement-templates/ (Accessed: November 25, 2022).

NIST. (2022, November 9). *Cybersecurity Framework Version 1.1*. NIST. Available at: https://www.nist.gov/cyberframework/framework-documents/ (Accessed: November 21, 2022).

NSA. (2020, September 22). *Selecting Secure Multi-factor Authentication Solutions*. Cybersecurity Information. Available at: https://media.defense.gov/2020/Sep/22/2002502665/-1/-1/0/CSI_MULTIFACTOR_AUTHENTICATION_SOLUTIONS_UOO17091520.PDF (Accessed: November 27. 2022)

OMB. (2019, May 21). *Memorandum 19-17 Enabling Mission Delivery through Improved Identity, Credential, and Access Management.* Executive Office of the President. Available at: https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf (Accessed: November 27, 2022).

S.2521 - 113th Congress (2013-2014): Federal Information Security Modernization Act of 2014. (2014). Available At: https://www.congress.gov/bill/113th-congress/senate-bill/2521/ (Accessed: November 23, 2022).