DIGITAL INSANITY: EXPLORING THE FLEXIBILITY OF NIST DIGITAL IDENTITY ASSURANCE LEVELS

Kenneth Myers

Marymount University

19th International Conference on Cyber Warfare and Security (ICCWS)

March 10, 2022

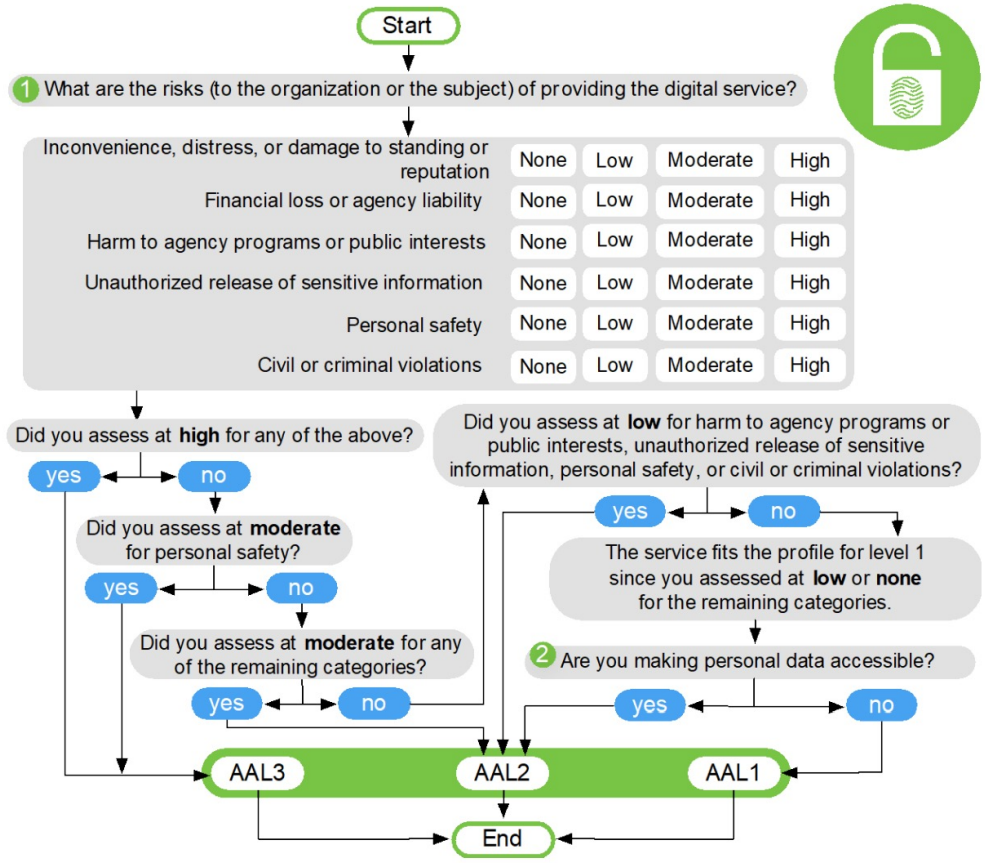
THE CHALLENGE - NIST DIGITAL RISK MANAGEMENT (2017)

Level	Identity	Authenticator	Federation
1	Self Attest	Single Factor	Signed
2	Remote Proofing	SW Multifactor	Signed/Encrypted
3	Supervised Proofing	HW Multifactor	Sign/Encrypt/Verify

RQ1) Provides flexibility to determine assurance levels?
RQ2) Is MFA always required?
RQ3) Does a risk assessment for using phishable MFA match current threats?

"The ability to combine varying xALs offers significant flexibility to agencies, but not all combinations are possible due to the nature of the data collected from an individual and authenticators to protect that data" (Grassi et al., 2017, p.33)

THE QUESTION - DOES IT OFFER FLEXIBILITY?



THE METHOD - DEVELOPED A TOOL

- Developed five test cases to test component and assurance level flexibility.

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

THE RESULTS

✓ Component Flexibility

X Level Flexibility

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

Additional findings:

- All enterprise uses cases should enforce MFA and most likely phishing-resistant MFA.

Abstract accepted to 18th International Conference on Cyber Warfare and Security (ICCWS) – March 2023

- ❑ Convert the spreadsheet into a website.
- ❑ Include a narrative section to explain the harm category.
- ❑ Further explore use cases if all MFA should be phishing-resistant MFA or specific use cases* (could change with new NIST SP).
- ❑ NIST SP 800-63 is about to release a Rev 4 very soon. Proposed changes based on this.

WHAT'S NEXT?

REFERENCES

- Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017, June). *Digital identity Guidelines*. Special Publication, 800(63–3). https://doi.org/10.6028/nist.sp.800-63-3