NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ENHANCING IDENTITY AND ACCESS MANAGEMENT IN THE U.S. NAVY VIA MIGRATION TO MORE MODERN STANDARDS OF AUTHENTICATION

by

Robert S. Baxter and Carlos S. Martinez Jr.

June 2020

Thesis Advisor: John D. Fulp
Co-Advisor: Gurminder Singh

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
ENHANCING IDENTITY AND ACCESS MANAGEMENT IN THE U.S. NAVY VIA MIGRATION TO MORE MODERN STANDARDS OF AUTHENTICATION

5. FUNDING NUMBERS

6. AUTHOR(S) Robert S. Baxter and Carlos S. Martinez Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

This thesis investigated the current digital authentication methods used by the U.S. Navy, reviewed new and alternative methods, and then offered suggestions regarding how the Navy could improve the robustness of its digital authentication ecosystem. Digital authentication is a critical security control useful for reducing operational risks to computer networks. Digital authentication entails any of various standards by which an entity (human or machine) can provide corroboration of its proclaimed identity in a manner and form that can be processed in a digital environment. The suggested authentication methods were ranked according to the strength of security and usability within the DoN infrastructure. From this research, a set of tables was established to tabulate useful metrics that were identified to determine the strengths and weaknesses of each authentication method when compared with the others. This facilitated a more granular analysis of the selected authentication methods. Our recommendation articulates a four-tier approach based on risk-management principles; with Tier 1 being the most secure, yet most costly and least usable, and Tier 4 being the least secure, yet least costly and most usable. The four tiers articulated are Tier 1—CAC-based PKI method, Tier 2—FIDO2-based PKI method, Tier 3—2FA method, and Tier 4—password-only method.

14. SUBJECT TERMS
digital authentication, authentication, information security, Common Access Card, CAC, authenticator threats, privacy, usability, authenticator types, Public Key Infrastructure, PKI, Multi-Factor Authentication, MFA

15. NUMBER OF PAGES
89

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

ENHANCING IDENTITY AND ACCESS MANAGEMENT IN THE U.S. NAVY VIA MIGRATION TO MORE MODERN STANDARDS OF AUTHENTICATION

Robert S. Baxter
Lieutenant Commander, United States Navy
BA, University of North Florida, 2009

Carlos S. Martinez Jr.
Lieutenant, United States Navy
BS, Southwest Texas State University, 2001
BS, The University of Southern Mississippi, 2009

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
June 2020

Approved by: John D. Fulp
Advisor

Gurminder Singh
Co-Advisor

Thomas J. Housel
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis investigated the current digital authentication methods used by the U.S. Navy, reviewed new and alternative methods, and then offered suggestions regarding how the Navy could improve the robustness of its digital authentication ecosystem. Digital authentication is a critical security control useful for reducing operational risks to computer networks. Digital authentication entails any of various standards by which an entity (human or machine) can provide corroboration of its proclaimed identity in a manner and form that can be processed in a digital environment. The suggested authentication methods were ranked according to the strength of security and usability within the DoN infrastructure. From this research, a set of tables was established to tabulate useful metrics that were identified to determine the strengths and weaknesses of each authentication method when compared with the others. This facilitated a more granular analysis of the selected authentication methods. Our recommendation articulates a four-tier approach based on risk-management principles; with Tier 1 being the most secure, yet most costly and least usable, and Tier 4 being the least secure, yet least costly and most usable. The four tiers articulated are Tier 1—CAC-based PKI method, Tier 2—FIDO2-based PKI method, Tier 3—2FA method, and Tier 4—password-only method.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. IDENTIFICATION AND AUTHENTICATION (I&A)....2
1. Identification (Non- I&A Context)....3
2. Identification (I&A Context)....3
3. Authentication....3
B. FUNDAMENTAL METHODS OF AUTHENTICATION....3
1. The Classics (Know, Have, Are)....4
2. The Classics Reconsidered....5
C. TERMINOLOGY....6
1. Registration/Enrollment....7
2. Identity....7
3. Credential....7
4. Claimant....7
5. Relying Party (RP)....7
6. Authenticator....8
7. Authentication....8
8. Verifier....8
9. Token....8
D. REFERENCE MODEL....8
1. Registration/Enrollment....9
2. Identity....9
3. Credential....9
4. Claimant....9
5. Relying Party (RP)....9
6. Authenticator....10
7. Authentication....10
8. Verifier....10
9. Token....10

II. AUTHENTICATION SYSTEM MAJOR CONCERNS....11
A. CURRENTLY DEFINED U.S. FEDERAL DIGITAL AUTHENTICATION ECOSYSTEM....11
B. AUTHENTICATOR ASSURANCE/VERIFIER REQUIREMENTS....12
C. PERMITTED AUTHENTICATOR TYPES....14
D. REAUTHENTICATION....15
E. AUTHENTICATION RISKS....15

F. USABILITY 17

III. CURRENT U.S. NAVY DIGITAL AUTHENTICATION POLICY AND PRACTICES 21
A. POLICY 21
1. PIV—Authentication 22
2. DOD Certificate Policy 23
3. CAC 24
B. NAVY-WIDE IMPLEMENTATION 27

IV. MODERN/IMPROVED DIGITAL AUTHENTICATION METHODS 29
A. AUTHENTICATION STANDARDS 29
1. FIDO Alliance 29
2. OpenID Connect/OAUTH 2.0 35
3. CAC 37
B. AUTHENTICATION PRODUCTS/VENDORS 38
1. RSA 38
2. Cyber Ark 39
3. Yubico 39
4. Okta 40
C. AUTHENTICATION METHODS COMPARISON 41

V. IMPROVING U.S. NAVY DIGITAL AUTHENTICATION 47
A. CURRENT DON AUTHENTICATION ENVIRONMENT 47
1. Distribution of CAC to DoN Personnel 47
2. DON Instructions Governing Present Authentication Policies 48
B. RECOMMENDATIONS FOR ENHANCED DON-WIDE AUTHENTICATION 49
1. Tier-1 (CAC) 50
2. Tier-2 (FIDO2) 51
3. Tier-3 (2FA (Password + Device)) 52
4. Tier-4 (PW only) 53
C. SUMMARY 54

VI. SUMMARY AND FUTURE WORK 55
A. SUMMARY 55
1. Standardizing the Terminology 56
2. Methods That Were Considered and Why 57
3. Primary Guidance for Evaluating the Contenders 58

4. Metrics of Comparison 59
5. Ranking and Recommendations 60
B. FUTURE WORK 61
1. Concern with the Novelty of FIDO2 61
2. Further Research to Shore Up Vulnerabilities that May Exist 62

LIST OF REFERENCES 63

INITIAL DISTRIBUTION LIST 69

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. DOD CAC Topology. Source: [17]. 24

Figure 2. PKI Key Exchange. Source: [19]. 26

Figure 3. FIDO Support by Web Browser. Source: [26]. 31

Figure 4. FIDO CTAP-1 Overview. Source: [28]. 32

Figure 5. WebAuthn/CTAP Architecture. Source: [30]. 33

Figure 6. FIDO UAF Standard. Source: [28]. 35

Figure 7. Okta Adaptive MFA Supported Standards. Source: [52]. 41

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. AAL Summary of Requirements. Source: [6]. 14

Table 2. Usability Considerations. Source: [6]. 19

Table 3. Security Attributes of Methods 45

Table 4. Security Attributes of Methods with DoN Usability “Penalties” Considered 46

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

2FA	Two-Factor Authentication
AAL	Authenticator Assurance Level
AC	Attribute Certificates
APL	Approved Product List
BLE	Bluetooth Low Energy
CA	Certificate Authority
CAC	Common Access Card
CIA	Confidential, Integrity, Availability
CMVP	Cryptographic Module Validation Program
CP	Certificate Policy
CSP	Credential Service Provider
CTAP	Client to Authenticator Protocols
DISA	Defense Information System Agency
DOD	Department of Defense
DODI	Department of Defense Instruction
DODIN	Department of Defense Information Network
DON	Department of the Navy
ECC	Elliptic-Curve Cryptography
FedRamp	Federal Risk and Authorization Management Program
FIDO	Fast Identity Online
FIPS	Federal Information Processing Standard
FMR	False Match Rate
HPSD	Homeland Security Presidential Directive
I&A	Identification and Authentication
IAM	Identity and Access Management
MFA	Multi-Factor Authentication
MITM	Man in the Middle
NFC	Near-Field Communications
NIPRNET	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology

NPE	Non-Person Entity
OGA	Other Governmental Agencies
OIDC	Open ID Connect
OPM	Office of Personnel Management
OTP	One-Time Password
PIN	Personal Identification Number
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RP	Relying Party
RSA	Rivest-Shamir-Adleman
RT	Rainbow Table
SIPRNET	Secret Internet Protocol Router Network
SP	Special Publication
SSO	Single Sign on
QR	Quick Response
UAF	Universal Authentication Framework
UCAPL	Universal Capabilities Approved Products List
USB	Universal Serial Bus
USN	United States Navy
W3C	World Wide Web Consortium

ACKNOWLEDGMENTS

We have a multitude of parties to recognize for the blood, sweat, and tears that were expended while working on this thesis. We have to start by thanking our advisor and mentor, J.D.Fulp. From choosing the daunting task of working with two guys that had no clue what they wanted to write about to giving it to us straight when we strayed to encouraging us when we really needed it, he was integral to the completion of this thesis.

And most importantly, we are forever grateful to our wives, Ashley and Myrna. Thank you for listening to our rants about authentication methods, impending corrections, and formatting issues. This thesis would not have been completed without the continued support that you selflessly provided.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Digital authentication is a crucial factor for maintaining strong network and computer security. The ability to authenticate the identity of the sender/originator is of the utmost importance for maintaining the integrity of the Department of the Navy (DoN) networks, and the confidence that the information sent and received is not modified or compromised. Authentication is needed to ensure integrity, one of the key components of the CIA (confidential, integrity, availability) triad, and is paramount and vital to the DoN's mission. Authentication can occur between humans or non-person entities (NPEs). This thesis will use the words "it," "claimant," and "subscriber," as dictated by context or source citation, to represent the entity being authenticated. Note that the usage of "it" is included, given that NPEs are also subject to authentication.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3 series addresses technical requirements for, and guides federal agencies through, the correct implementation of digital-based authentication. The NIST SP800-63-3 series, titled Digital Identity Guidelines, includes NIST 800-63A: Enrollment and Identity Proofing, and NIST 800-63B: Authentication and Life cycle Management. These NIST documents contain information that can guide the Navy's information professionals to choose, implement, and configure authentication tools more effectively.

Threats posed to the U.S. Federal digital authentication ecosystem are constantly evolving, thus requiring credential service providers (CSPs) to adapt as necessary. The online ecosystem is constantly challenged by attackers. This ecosystem must be as secure as feasible, while also being able to support the information operations for which it was designed.

Modernizing current digital authentication standards is an essential factor for keeping up with the provocative nature and mentality of an ever more sophisticated threat. Methods of authentication that will be explored are biometric-based and secret-based, with the goal of determining the most effective means of providing digital authentication within the DoN.

This thesis will focus on the Navy's current policies for digital authentication and how it is currently implemented. Moreover, it will attempt to identify institutional practices and

standards that can be established to modernize and fortify authentication practices in an effort to mitigate dynamic cyber threats.

The primary research question of this thesis is: what Identity and Access Management (IAM) improvements are currently available that could be adopted to improve the overall cybersecurity posture of U.S. Navy network enclaves? Secondary research questions are:

- What is the current state of digital authentication in the DoN?
- What are the prominent digital authentication improvements that are either not utilized, or are under-utilized, by the DoN?
- What is the cost/benefit analysis for likely digital authentication improvements for the U.S. Navy?

Any sincere consideration of authentication and the myriad standards devised to provide it requires basic understanding of the attendant terminology. As the terminology in this domain lacks universal standardization, the ensuing sections of this chapter endeavor to establish the terminology to be used in this work.

A. IDENTIFICATION AND AUTHENTICATION (I&A)

NIST Special Publication 800-53, titled "Security and Privacy Controls for Federal Information Systems and Organizations" [1], lists 18 security control families. One of these families is Identification and Authentication (IA). The IA family plays a critical role as it relates to at least two of the other security control families: access control (AC) and audit and accountability (AU). This is due to the fact that both AC and AU implementations are dependent upon the availability of secure IA solutions. According to Homeland Security Presidential Directive 12 [2], a "secure and reliable form of identification" will have the following:

> (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. [2]

1. Identification (Non- I&A Context)

The term identification is used in two different contexts: one that considers it in isolation, and one which considers it as a direct prelude to authentication. We refer to the former as the non-I&A context. In the non-I&A context, identification indicates technologies developed to identify unknown individuals. A classic case of this is law enforcement agencies that attempt to put names on faces that have been captured on still photos or motion video feeds. This type of identification is not in scope for this research.

2. Identification (I&A Context)

When an identity is freely proffered by an entity seeking to be authenticated, we refer to this as identification in the I&A context. In essence, the proffering of an identity is desired as it simplifies the authentication task to a 1-to-1 matching problem; as opposed to a many-to-1 problem which would result if the entity seeking authentication did not claim a specific identity at the outset.

3. Authentication

According to NIST 800-63-3 [3], authentication is the process employed to *validate* the identity proffered by an entity (whether human or NPE). The publication goes on to state that

> Digital authentication is the process of determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate. Successful authentication provides reasonable risk-based assurances that the subject accessing the service today is the same as that which previously accessed the service [3].

Authentication is critical to ensure a requesting entity is authorized to access a specific piece of information, thus preventing potential unauthorized disclosures.

B. FUNDAMENTAL METHODS OF AUTHENTICATION

Though there are many technical variations to how digital authentication can be accomplished, the fundamentals are fairly straight-forward. Those fundamentals are discussed here, along with two points that provide clarification going forward.

1. The Classics (Know, Have, Are)

There are three classic methods, also known as factors, that can be utilized to authenticate: something known (e.g., password), something possessed (e.g., badge or cryptographic key), or some unique physical trait or feature (i.e., biometrics). When an entity uses two or more of these classic methods, it is referred to as multi-factor authentication (MFA).

a. Know (Private but Not Secret)

The classic "know" form of authentication causes some confusion as the term "know" is used in two fundamentally different ways. In one way, authentication is performed by proving knowledge of private—but not secret—information. This is commonly referred to as "knowledge-based authentication." Since "knowledge" is included in the name of this authentication method, it is often conflated with the classic "know" factor which entails proving that some *secret* information is known.

A classic example where knowledge-based authentication is used, is for persons wanting to check their credit scores. When a person requests his score from a credit agency (e.g., Equifax), he is presented with several questions related to his—private but not secret—financial history; such as: "with which of these institutions have you ever obtained a loan?," or "at which of these addresses have you ever lived?"

According to NIST 800-63A [4], NIST does not recommend knowledge-based authentication methods to conduct authentication. This is due to two main issues; the attacker's ability to research answers to knowledge-based questions, and the fact that the answers to such questions typically never change and are thus subject to replay attack years after they may have been exposed. An example that elicits both of these weaknesses is seen in a password recovery question asking, "what was the make and model of your first car?" NIST does; however, accept knowledge-based authentication for helping to *resolve* identities during the enrollment process of the identity management life-cycle. Since enrollment is not in scope for this research, knowledge-based authentication is not discussed further in this work.

b. Know (Secret)

The other way in which the classic "know" form of authentication is performed, is by an entity proving knowledge of a secret that has been pre-registered, usually as part of account setup, with the authenticating party. Passwords and PINs are the most common examples of the "know" factor of authentication. This usage of "know" as a form of authentication *is* within the scope of this research.

c. Have

This form of authentication is commonly referred to as "something you have," and requires the entity requesting authentication to be in custody of some object (e.g. RSA token or smart card). This will ultimately be used for proof of possession of a secret.

d. Are

Commonly referred to as a "something you are" form of authentication, biometrics can be used as a method to authenticate. Biometric methods are comprised of both physical and behavioral characteristics. Examples of physical biometric characteristics are fingerprints and facial features/geometry; whereas keyboard typing metrics is an example of a behavioral characteristic.

2. The Classics Reconsidered

In the opinion of Fulp [5] the classics—*know*, *have*, *are*—can be categorized in a less confusing way. Fulp offers that all three of these classic factors are ultimately "have" requirements. The entity wishing to be authenticated must either: *have* the password (a secret), *have* the hardware token capable of generating a secret, or *have* a particular biometric trait, feature, or characteristic. With all three factors, the entity is ultimately being authenticated by proving he/she/it is in possession of some pre-registered secret or biometric. Using this simplified view, then, all authentication methods—barring those that are "knowledge-based" and use private, but not secret, information—can be categorized as either biometric- or secret-based.

a. Biometric

The NIST 800-63B precludes the use of biometrics as a *singular* method for authentication because "the False Match Rate (FMR) does not provide confidence in the authentication of the claimant by itself. In addition, FMR does not account for spoofing attacks. Biometric comparison is probabilistic, whereas the other authentication factors are deterministic" [6]. Despite these issues, biometrics is often used in conjunction with proving possession of secrets, resulting in strong MFA implementations [6].

b. Secret

Secret-based methods entail the entity proving he/she/it possesses either a symmetric secret (e.g., key, PIN, password, etc.) that is shared by the authenticating party, or an asymmetric secret (e.g., private key) that corresponds to a certified public key that is available to the authenticating party.

An example implementation of secret-based authentication is by way of an out-of-band (OOB) device. According to NIST 800-63B [6], an OOB device is a "physical device that is uniquely addressable and can communicate securely with the verifier over a distinct communications channel, referred to as the secondary channel" [6]. One example of an OOB device implementation of secret-based authentication is for the verifier to send a temporary (secret) PIN to the claimant's pre-registered telephone number or e-mail. Another example is to utilize applications on a mobile device to scan a barcode or Quick Response (QR) code sent by the verifier. The claimant authenticates by proving possession of the sent PIN or QR code back to the verifier [6].

C. TERMINOLOGY

Given the importance of a standardized lexicon for efficient discourse within any complex domain of study, we present nine terms that are essential for understanding and communicating issues of digital authentication. The descriptions below also align with the NIST 800-63-3. It is important to note; however, that digital technologies, including authentication, continue to evolve, which may result in their attendant terms being used inconsistently among the user/developer population.

1. Registration/Enrollment

The process used to verify, or establish, the identity of a person when she is being initially entered into a digital authentication system is called registration or enrollment. For example, Alice Jones is hired by the Acme consulting firm. During enrollment Alice provides proof of her name (verify), and then is given a unique identity (establish) that is unique within the Acme domain, such as akjones@acme.org. This process enters Alice into the identity management life-cycle at Acme. Part of this process will also entail Acme establishing secrets, and possibly biometrics, to be used for authenticating Alice [3].

2. Identity

A unique name/label determined by a CSP to describe the claimant for a frame of reference; for example, akjones as the unique username for Alice Jones within the Acme consulting firm.

3. Credential

A credential is "an object or data structure that authoritatively binds an identity - via an identifier or identifiers to at least one authenticator possessed and controlled by a claimant" [3]. For example, Alice's digital certificate containing the public key that corresponds with the authenticator private key (e.g. CertAlice).

4. Claimant

The entity being authenticated. The term claimant is used as it conveys the notion that an entity is merely "claiming" a particular identity; the 'I' of "I&A," but must undergo authentication in order to prove it. Use of this term to describe an entity implies that the entity has already completed registration/enrollment within the domain/system in which the authentication is being conducted.

5. Relying Party (RP)

The relying party is the entity that has a security-related interest in the truthfulness of a claimant's declaration of a particular identity; typically for the purposes of access control or audit and accountability.

6. Authenticator

The term authenticator is used to represent whatever is being presented by the claimant to satisfy the authentication criteria utilized by the verifier; for example, a password. The term "token" was used in previous versions of the SP800-63-3, but this has since been changed to the term "authenticator," which will be the term used throughout this thesis.

7. Authentication

The process employed to *verify* the identity of a claimant by an entity (whether human or NPE).

8. Verifier

The entity performing the authentication. Note this role may coincide with that of the RP if it is the RP that is performing the authentication. When the roles of RP and verifier are separate, then the verifier performs the authentication on behalf of the RP. As a simple example, the DMV (verifier) verifies identities and "certifies" them, along with a date of birth attribute, via a driver license (credential). A bar owner (RP) then relies upon driver licenses to avoid the risk of losing his liquor licenses by selling to minors.

9. Token

A digital object presented to a claimant by a verifier that serves as proof verifiable by a 3rd party RP that the claimant has been authenticated by the verifier. In this context the token is a unique string of characters bound to a claimant, and proves to the RP that the claimant is who it says it is. Unlike a key exchange infrastructure, a claimant will not share the token bound to them with another claimant. Note that this term can be confused with the term credential, as they are often used to represent similar digital objects. For example, the driver license scenario described in the previous paragraph—the license could be referred to as either a token or a credential.

D. REFERENCE MODEL

Here we present a hypothetical reference model to illustrate the typical contextual usage of the terms introduced above. The model is simplistic so as to enhance clarity of the

terms, and does not introduce or explain implementation details of any particular authentication system or standard.

1. Registration/Enrollment

Upon joining the Navy, Bob is required to provide several documents to prove his identity (e.g., birth certificate and driver's license). Once the Navy is satisfied with this initial identity confirmation, they enter Bob into their personnel database and issue him a digital certificate.

2. Identity

In Bob's digital certificate, his unique (within the Navy) identity is established as Bob#.Navy; where # represents a number sufficient to make this Bob unique among all other Bob's in the Navy. Bob's regular name, "Bob," is retained as an attribute of his entire digital personnel record (i.e., part of Bob's persona), but his digital authentication transactions require usage of his unique Bob#.Navy identity.

3. Credential

This is the digital certificate created for Bob during enrollment. This credential associates the identity Bob#.Navy with a particular public key; a public key for which Bob was given the corresponding private key for his safe-keeping.

4. Claimant

In the execution of Bob's duties, he needs to access a secure Navy website. When Bob connects to the website, he is claiming to be the entity associated with the identity Bob#.Navy; that is, Bob is acting in role of a claimant in the I&A context.

5. Relying Party (RP)

The Navy website is charged with securing resources by way of access controls that are implemented via permissions associated with each user identity. Thus, the website is reliant upon the verification of Bob's claimed identity in order to affect its access control-based security policy.

6. Authenticator

The website sends Bob a challenge (random string of symbols), which he encrypts with the private key (an example of an authenticator) that is associated with the public key in his digital certificate (the credential).

7. Authentication

Bob sends the encrypted challenge back to the website. The website, acting as both the verifier and the RP, will decrypt the encrypted challenge to ensure the decrypted result matches what was originally sent to Bob. In the case of a match, Bob is authenticated and provided website access according his permissions; else Bob's request is rejected.

8. Verifier

Since the website conducted the authentication process, it was not only the RP, but also the verifier in this example.

9. Token

To explain the term token, the scenario must be changed slightly, in that the RP (website) is *not* also the verifier. Instead, the verifier is some other system, device, or organization. With this change in mind, authentication proceeds as follows. Bob contacts the website with his claim to be Bob#.Navy. The RP website forwards this claim to a designated verifier which conducts the same challenge-response protocol described above. If the authentication is successful, the verifier creates a token that attests to the identity verification. This token is itself authenticatable via some mechanism, for example being digitally signed by the verifier. At this point, one of two things can happen: 1) the verifier sends the token directly to the RP, or 2) the verifier sends the token to the claimant, who would then be expected to send it to the RP, but as was mentioned Chapter I.C.9, there will be no sharing of a token between claimants.

II. AUTHENTICATION SYSTEM MAJOR CONCERNS

Traditional methods for the authentication of users is an increasing cause for concern and has amplified issues requiring attention from the DOD. The current authentication ecosystem provides reasonable options to secure networks. However, as cyber actors evolve in their approach, it becomes necessary for the DOD to modernize its methods of authentication.

This chapter will highlight the guidelines in place to construct a more secure authentication environment than what is currently in-place, discuss security levels required and corresponding authenticator types for each, and the overall usability for approved authentication methods.

A. CURRENTLY DEFINED U.S. FEDERAL DIGITAL AUTHENTICATION ECOSYSTEM

The U.S. Federal Government digital authentication ecosystem is governed by Homeland Security Presidential Directive (HPSD)-12, which states that the Department of Commerce will establish a standard for the Federal Government to implement secure and reliable forms of identification. Part 3 of this document states that secure and reliable identification "can be rapidly authenticated electronically" [2]. NIST, which is part of the U.S. Department of Commerce, issued the special publication (SP) series 800-63 regarding digital identity. The SP 800-63 series sets the standard for the Federal Government to conduct digital authentication. The following documents are included in the 800-63 series:

- NIST SP 800-63-3: Digital Identify Guidelines
- NIST SP 800-63A: Digital Identity Guidelines—Enrollment and Identity Proofing
- NIST SP 800-63B: Digital Identity Guidelines—Authentication and Life cycle Management.

Furthermore, the Department of Defense (DOD) has its own directives, which stem from these NIST publications. DOD Instruction (DODI) 8520.03 is the DOD's instruction for

"Identity Authentication for Information Systems" [7], while DODI 8500.01E is for "Cybersecurity" [8]. These DOD documents are discussed further in Chapter III of this thesis.

B. AUTHENTICATOR ASSURANCE/VERIFIER REQUIREMENTS

A claimant is required to use a protected channel when authenticating itself. This ensures the confidentiality of the authenticator used and aids in preventing a Man in the Middle (MitM) attack. The NIST guidance also requires that verifiers have "hardware cryptographic modules validated at a specific FIPS 140 level" [6]. Federal Information Processing Standard (FIPS) 140 defines four security levels for cryptographic modules, with Level 1 being the lowest and Level 4 being the highest.

The FIPS 140-2 [9], "specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system." The requirements for these 4 levels cover a wide range of technical specifications. "The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2 and other cryptography based standards" [9]. Once CMVP has validated a product, it can be implemented by Federal agencies for the protection of sensitive information [9].

At Security Level 1, there is no requirement for physical security mechanisms, and "basic security requirements are specified for a cryptographic module (e.g., at least one Approved algorithm or Approved security function shall be used)" [9]. At Security Level 2, physical security is enhanced by "adding the requirement for tamper-evidence" [9]. At this level, role-based authentication is required "in which a cryptographic module authenticates the authorization of [the claimant] to assume a specific role and perform a corresponding set of services" [9]. Security Level 3 adds more physical protection by adding mechanisms that will detect and respond to physical access or the modification of the module [9]. Moreover, it "requires identity-based authentication mechanisms, enhancing the security provided by the role-based authentication mechanisms specified for Security Level 2" [9]. The highest level of security is Security Level 4. At this level, the physical security provides a complete "envelope" of protection, given "penetration of the

cryptographic module enclosure from any direction has a very high probability of being detected" [9].

This thesis will use the term verification or verifier as is described in Chapter I.C.8 as the entity performing the authentication. The word validate or validation will be used to describe the "process of demonstrating that the system under consideration meets in all respects the specification of that system" [10].[1]

The NIST SP800-63B describes three authenticator assurance levels (AAL) from AAL1 to AAL3. AAL1 is the least secure, while AAL3 is the most secure. When personally identifiable information (PII) or personal information that characterizes the information for which authentication is required, the NIST SP800-63B requires AAL2 at a minimum.

The NIST manual states that AAL1 will provide "some assurance that the claimant controls an authenticator bound to the subscriber's account." This authentication level can be either single or multi-factor. To successfully authenticate itself, the claimant must "prove possession and control of the authenticator through a secure authentication protocol" [6]. The NIST publication states AAL1 requires a FIPS 140 Level 1 for Government agency verifiers.

According to NIST 800-63B [6], AAL2 provides the claimant with higher confidence than AAL1 that the claimant controls the authenticator that is attached to the claimant's account. The NIST publication states that AAL2 requires a FIPS 140 Level 1 for Government agency authenticators *and* verifiers. This is more secure than AAL1, because unlike AAL1 which requires a FIPS 140 Level 1 for only the verifier, AAL2 also requires the authenticator to be FIPS 140 Level 1.

AAL3 is the highest level of authenticator assurance levels listed in the NIST SP800-63B. This level "provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account" [6]. According to NIST 800-63B [6], this is implemented by requiring the proof of possession of a key (secret) and a

[1] The authors of this thesis believe the word "verification" in Table 4-1 in NIST SP 800-63B should be "validation."

cryptographic protocol. At this level, a hardware-based authenticator will be used. The NIST publication states that AAL3 requires a FIPS 140 Level 2 for MFA, while the less secure FIPS 140 Level 1 is allowed for single-factor cryptographic devices and verifiers. And regardless of those factor considerations, the publication specifies a minimum of FIPS Level 3 for the *physical* security requirements of all authenticators at AAL3. FIPS Level 3 for physical security requires "automatic zeroization when accessing the maintenance access interface [and] Tamper response and zeroization circuitry [and] Protected vents" [9].

C. PERMITTED AUTHENTICATOR TYPES

Table 1 is a representation of the permitted authenticator types, FIPS 140 requirements, and reauthentication requirements for each AAL level.

Table 1. AAL Summary of Requirements. Source: [6].

Requirement	AAL1	AAL2	AAL3
Permitted Authenticator Types	Memorized Secret; Look-Up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device	MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorized Secret plus: • Look-Up Secret • Out-of-Band • SF OTP Device • SF Crypto Software • SF Crypto Device	MF Crypto Device; SF Crypto Device plus Memorized Secret; SF OTP Device plus MF Crypto Device or Software; SF OTP Device plus SF Crypto Software plus Memorized Secret
FIPS 140 Verification	Level 1 (Government agency verifiers)	Level 1 (Government agency authenticators and verifiers)	Level 2 overall (MF authenticators) Level 1 overall (verifiers and SF Crypto Devices) Level 3 physical security (all authenticators)
Reauthentication	30 days	12 hours or 30 minutes inactivity; MAY use one authentication factor	12 hours or 15 minutes inactivity; SHALL use both authentication factors

D. REAUTHENTICATION

It is crucial for a claimant to reauthenticate a session after a given period of time. This reauthentication time is the amount of time before a claimant will need to authenticate again. The maximum reauthentication interval for AAL1 is 30 days, and any authenticator can be used to reauthenticate. The maximum reauthentication interval for AAL2 is 12 hours of activity or 30 minutes of inactivity, and the claimant needs to present either a "memorized secret or biometric" authenticator to reauthenticate. The maximum reauthentication interval for AAL3 is 12 hours of activity or 15 minutes of inactivity, and MFA authentication methods are required to reauthenticate [6].

E. AUTHENTICATION RISKS

According to Todorov [11], attackers will attempt to penetrate devices and networks that require authentication. There are many ways an attacker can attempt to gain access to a system, including attempts to bypass the authentication process entirely. For example, if the attacker has physical access then the attacker may be able elevate privileges. Once the attacker escalates privileges, he or she can find the application that requires authentication and modify it to accept the attacker's username and password. This is more difficult to conduct on servers, given that servers typically have limited physical access. However, an attacker can attempt to bypass authentication protocols on a server by trying to guess a URL that is logically "behind" the login screen on a website [11]. Additionally, if the attacker has physical access, he or she may be able to access information without performing the intended authentication requirement, by bypassing the local authentication measures that were imposed by the operating system [11]. Attackers could also "shoulder surf" and attempt to observe a claimant entering his or her authenticator (e.g., password) into the system.

Many software and hardware vendors use default passwords on their equipment. If an attacker is able to determine the hardware or software being utilized in the authentication process, the attacker can use these default passwords to observe whether the passwords were changed after being installed [11].

When a claimant attempts to authenticate itself using authenticators, the authentication request is performed by processes that are running on behalf of the user, which may have escalated privileges [11]. This lends itself to attackers who can find a security hole. If the attacker is able to find the security issue, it may be possible to conduct a stack overflow attack. Successfully doing so may force an application to execute code of the attacker's choosing, and to do so with the more elevated privileges of the user who—as is often the case—is running the overflowed process in a privileged mode (i.e., system administrator) [11].

An attacker can also guess the username and password by conducting reconnaissance. For example, an attacker can look at the organization's email addresses and observe that all e-mails are first name (.) last name followed by the organization. The attacker can guess that the username is going to be the same format as the beginning of the e-mail address. An attacker can also attempt to use brute-force techniques through a password cracking application that will cycle through potential passwords that are combinations of dictionary words and characters.

Rainbow tables (RT) can be used to expedite password discovery when only the hash of the password is known to the attacker. Since RTs capture a great deal of pre-hash work for a given password space (alphabet and length specific), they allow the discovery of password collisions much more quickly than would be possible if the attacker was relegated to finding a collision via brute-force, with no previous hash work having been processed and stored. A simplistic example is offered here. Assume Bob's password is "apple" and the attacker observes the hash of Bob's password (assume the hash is "b5d68a3q"). The attacker enters the appropriate RT with "b5d68a3q" and a collision is found (assume it is "banana"). This (hypothetical example) assumes the "apple" and "banana" both hash to the same hash value (i.e., they collide) given the hash function being employed. Under these circumstances, the attacker may use "banana"—though *not* Bob's password—to authenticate as Bob. Further discussion of RTs is outside the scope of this research.

Attackers can also replay authenticators (directly) or data (e.g., packet payloads) that contain the processed output of a previously generated authentication reply. As an

example, when static authentication is used, an attacker could replay the password. This requires the attacker to be able to observe the traffic between claimant and server. If the claimant sends an encrypted text to authenticate, the attacker can present the captured encrypted text to the server to authenticate itself. To avoid these replay attacks, many authentication techniques involve a challenge-response mechanism. With such a mechanism,

> the authenticator will generate a random string and will present it as a challenge to the [claimant]. The [claimant] will typically manipulate the server challenge in some way and will typically encrypt it using the user password or a derivative as the key, or generate a hash based on the challenge and the user password [11].

Another threat to authentication is the ability for attackers to downgrade authentication strength. In this scenario, an attacker acting as a MitM, modifies the traffic between claimant and server to a weaker authentication protocol or mode. As a result, this could possibly display the plaintext password or other usable authenticators that the attacker could harvest [11].

The last threat to authentication entails social engineering, wherein the attacker convinces the claimant to reveal their authenticators through an e-mail or telephone inquiry. An example of this technique is when the attacker deceives the claimant, thereby causing the claimant to either pass its authenticators to a false website or provide its authenticators via a phone call [6].

F. USABILITY

Usability is a significant consideration in authentication standards. The NIST SP 800-63B states that the goal of usability is to be able to access information as intended [6]. An organization cannot make it so difficult to access information that claimants are unable to access the information in a timely manner. For example, if the log on process takes too much time, this will reduce the effectiveness of the entire authentication ecosystem. NIST recommends conducting an evaluation of usability to ensure the usability is appropriate and does not result in claimants attempting to develop workarounds that will ultimately reduce the value of the authentication methods and procedures [6].

NIST recommends specific usability considerations for each of the different authenticator types. These are summarized in tabular form in Table 2. For a memorized secret, the more difficult the requirements are, the more likely a claimant will not be able to recall the password. Authentication should allow a cut and paste functionality for memorized secrets “this facilitates the use of password managers, which are widely used and in many cases increase the likelihood that users will choose stronger memorized secrets” [6]. When using look-up secrets the authenticator should consider the length and complexity of the secret. The longer and more complex it is, the more difficult it will be to input. Out-of-band usability should take into account that the claimant will have to go back and forth between screens; for example, on both a smart phone and computer. It is also recommended that an out-of-band device should have to be unlocked before the claimant is able to view the secret. For multi-factor OTP devices, NIST recommends that there is a reasonable grace period for the claimant to enter the OTP before it expires. Single-factor and multi-factor cryptographic software should present recognizable terminology and names to claimants, so as to more clearly convey which cryptographic key is expected. Security personnel involved in choosing appropriate authentication implementations should be aware that for single-factor and multi-factor cryptographic devices, a single physical input could be an issue because plugging a device into a USB port that is located on the back of a computer, or using a laptop with limited USB ports, could affect the usability of the device. Table 2 summarizes the considerations NIST recommends for usability for various authenticator types.

Table 2. Usability Considerations. Source: [6].

Usability Consideration	Memorized secrets	Look-up Secrets	Out of Band	Single Factor OTP Device	Multi-Factor OTP Device	Single Factor Cryptographic Software	Single Factor Cryptographic Device	Multi-Factor Cryptographic Software	Multi-Factor Cryptographic Device
Typical Usage									
Authenticator availability – authenticators readily in user's possession	◆	◆	◆	◆	◆	◆	◆	◆	◆
Plain language for user facing text (e.g., instructions, prompts, notifications, error messages)	◆	◆	◆	◆	◆	◆	◆	◆	◆
Legibility of user facing text or text entered by users	◆	◆	◆	◆	◆	◆	◆	◆	◆
Unmasked text entry		◆	◆	◆	◆				
Support text entry – length of 64 characters, copy and paste	◆								
Delayed masking during text entry	◆								
Adequate time allowed for text entry	◆	◆	◆	◆	◆				
Entry errors – need clear and meaningful feedback	◆	◆	◆	◆	◆				
Minimum of 10 attempts allowed	◆	◆	◆	◆	◆				
Remaining allowed attempts – need clear and meaningful feedback	◆	◆	◆	◆	◆				
Form-factor constraints	◆	◆	◆	◆	◆	◆	◆	◆	◆
Location and availability of a direct computer interface such as a USB port				◆	◆		◆		◆

Table 2 (cont). Usability Considerations

Usability Consideration	Memorized secrets	Look-up Secrets	Out of Band	Single Factor OTP Device	Multi-Factor OTP Device	Single Factor Cryptographic Software	Single Factor Cryptographic Device	Multi-Factor Cryptographic Software	Multi-Factor Cryptographic Device
Physical input required (such as pressing a button)				◆			◆		
Cryptographic keys need for descriptive and meaningful names						◆		◆	◆
Complexity and size of the prompts		◆							
Authentication to secondary device to access the authentication secret			◆						
Continuous hardware connection not required									◆
Intermittent Events									
Reauthentication due to user inactivity	◆	◆	◆	◆	◆	◆	◆	◆	◆
Fixed periodic reauthentication	◆	◆	◆	◆	◆	◆	◆	◆	◆
Provisions for technical assistance	◆	◆	◆	◆	◆	◆	◆	◆	◆
Provisions to create and change memorized secrets	◆								

III. CURRENT U.S. NAVY DIGITAL AUTHENTICATION POLICY AND PRACTICES

In this chapter, we present current policies and practices that both inform and guide the U.S. Navy in its pursuit to implement and leverage modern technologies. In today's digital environment, the amount and sensitive nature of the information that DoN users are storing and sharing requires increased security. The DOD policy mandates that the DoN implement requirements set forth in DOD Instruction 8500.01, which "assigns responsibilities, and prescribes procedures for implementing identity authentication of all entities to DOD information systems" [7].

A. POLICY

Due to an increase in threats against the DOD's networks and critical information systems, it was mandated that "commanders and supervisors at all levels, including the operational level, to lead engagements in improving cybersecurity readiness across the force" [12]. Based on recent reporting and lessons learned of network compromises, there was evidence of systemic shortfalls in the implementation of basic cybersecurity requirements policies, directives, and orders department-wide [12].

Information stored on DOD systems is accessed and shared by a large number of users, and the data must be secured such that claimants are only allowed to access information for which they have a mission-related need to know. Further, it is important to audit the actions of authorized users so as to ensure their compliance with an organization's security policies. Both of these issues, access-control and audit, are supported by a requisite I&A policy and its attendant processes and procedures.

The sections that follow describe the current authentication methods being leveraged by the DoN and how they are being implemented. Of main concern to the DoN are: 1) the Personal Identity Verification (PIV) program, 2) the DOD Certificate Policy, 3) the DOD-issued Common Access Card, and 4) the Public Key Infrastructure. Since the most effective intrusions take advantage of known vulnerabilities, all personnel must understand the roles necessary to maintain a robust defensive posture.

1. PIV—Authentication

Per HSPD-12, PIV authentication is required, "in order to establish more uniform standards for issuing government identity credentials" [2]. PIV authentication applies to all government personnel, government contractors, and government-controlled facilities. Its usage facilitates authorization-based access control to claimants, subsequent to a smart card-based authentication. The standard set forth by the FIPS 201-2, outlines the architecture and technical requirements to support smart card-based authentication.

PIV should be used for:

- All authentication for all *privileged* users including servers, networks, and applications;
- All *network* authentication for *all* users;
- All application authentication for *all* users of an application that protects or contains sensitive information; and
- Physical access to facilities and buildings. [13]

PIV credentials are made up of digital certificates, key pairs, a unique pin, and in some cases biometrics. When combined into a single credential, they can provide the capability to leverage MFA for DoN networks and applications [13].

An operationally functional PIV system is made up of three main components; the PIV Front-End Subsystem, the PIV Card Issuance and Management Subsystem, and the PIV Relying Subsystem. FIPS 201-2 further explains what each subsystem is responsible for:

> **PIV Front-End Subsystem:** PIV Card, card and biometric readers, and PIN input device. The PIV cardholder interacts with these components to gain physical or logical access to the desired Federal resource.
>
> **PIV Card Issuance and Management Subsystem:** the components responsible for identity proofing and registration, card and key issuance and management, and the various repositories and services (e.g., public key infrastructure (PKI) directory, certificate status servers) required as part of the verification infrastructure.
>
> **PIV Relying Subsystem:** the physical and logical access control systems, the protected resources, and the authorization data. [10]

2. DOD Certificate Policy

The United States DOD X.509 Certificate Policy (CP) lays out the current DOD CP. The introduction states that:

> programs that carry out or support the mission of the DOD require services such as authentication, confidentiality, technical non-repudiation, and access control. These services are met with an array of network security components such as workstations, guards, firewalls, routers, in-line network encryptors [sic], and trusted database servers. [14]

The CP further states that, "the use of public key certificates will not add any security services in a poorly designed system." DOD Instruction 8520.02 further states that it is DOD policy that:

- The DOD shall implement a DOD-wide PKI to maintain the certificate life cycle, including, but not limited to, issuance, suspension, and revocation. The DOD shall issue certificates to DOD PKI Certificate Eligible Users in accordance with United States Department of Defense X.509 Certificate Policy. The DOD PKI also shall support requirements for group, role, information systems, device, and code signing certificates. The DOD PKI shall provide first and third-party key recovery for private keys associated with encryption certificates.
- The DOD shall only rely on certificates that are issued by the DOD PKI or by a DOD approved PKI for authentication, digital signature, or encryption. DOD mission partners shall use certificates issued by the DOD External Certification Authority (ECA) program or a DOD approved PKI, when interacting with the DOD in unclassified domains.
- The DOD shall establish and maintain a cross certification with the Federal PKI to comply with FIPS 201-1. The DOD shall facilitate the issuance of any new PKI certificates necessary to comply with Federal or Office of Management and Budget issuances or mandates and be consistent with DOD implementation plans. DOD PKI shall comply with FIPS 201-1for mandatory certificates issued on the CAC.
- PKIs operating under the purview of the DOD are approved for use for their intended purpose and environment.
- The effective implementation of the CP will depend on the reliability of the cryptographic keys, reliable management of the current infrastructure, and procedural implementation by personnel overseeing the operation. [15]

3. CAC

The CAC is a smart card that satisfies MFA and is used to ID U.S. military, DOD civilians, and vetted contractors. It is approximately the size of a credit card and can store 144K of data on an integrated circuit chip. The CAC contains specific, "abbreviated data relating to your work functions or benefits and privileges provided as a uniformed member of the Armed Forces, U.S. Public Health Service, or NOAA, DOD Civilian, or DOD Contractor" [16], and a digital image of the cardholder's face, fingerprints, PII, and the PKI certificates associated with the user. In January of 2011, the Social Security Number was removed from the CAC and replaced with the DOD identification number. Figure 1 visually maps the physical characteristics of a DOD issued CAC.

Figure 1. DOD CAC Topology. Source: [17].

When the CAC is inserted into a reader and the enabling PIN is entered, the reader will invoke middleware protocols to authenticate the claimant and grant or deny access. For continued resource access, the CAC must remain inserted. The user then removes the card at the termination of his/her session.

The CAC allows personnel *logical* access to DOD networks and, in some cases, *physical* access to government facilities. The CAC makes use of PKI certificates to authenticate the identity of the cardholder, and allows the claimant to encrypt and cryptographically sign emails and other data.

Smart card technology underpins the physical platform upon which PIV and CAC/PKI functionality rely upon. A smart card is a credit card-sized platform that according to DODI 8520.03 [7], is made up of multiple integrated circuits and can use one or a combination of the following technologies:

- magnetic stripe
- bar code (linear or two dimensional)
- non-contact and radio frequency transmitters
- integrated circuit chip
- biometric information
- encryption and authentication information
- photo identification. [7]

The current DOD CAC is a smart card and offers strong authentication by achieving AAL3 [6]. This is based on the information provided in Chapter II.B, that describes the different levels of authentication (AAL1 through AAL3). Cryptographic keys and other restricted authentication details are kept on the card and remain protected, "physically and logically," making it difficult to compromise. The DOD CAC meets the DOD's requisite authentication standards, and can produce, save, and use asymmetric encryption keys (i.e., Rivest-Shamir-Adleman (RSA) and/or Elliptic-Curve Cryptography (ECC)) [18]. According to Double Octopus [18], a smart card is used to execute cryptographic algorithms through a microprocessor. Smart cards are connected to a host computer, and software on the host computer interacts with the cryptographic processing onboard the card to authenticate the claimant (card owner) during any of various smart card-enabled authentication transactions [18]. However, smart card implementation can be costly due to such issues as software installation, the requirement to obtain compatible card readers, and the need for a physical card.

PKI is made up of a "framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates" [15]. A Certification Authority (CA) acts as a trusted intermediary, issuing certificates and keys to confirm the identities of claimants exchanging information. Figure 2 illustrates the request and use of a public key.

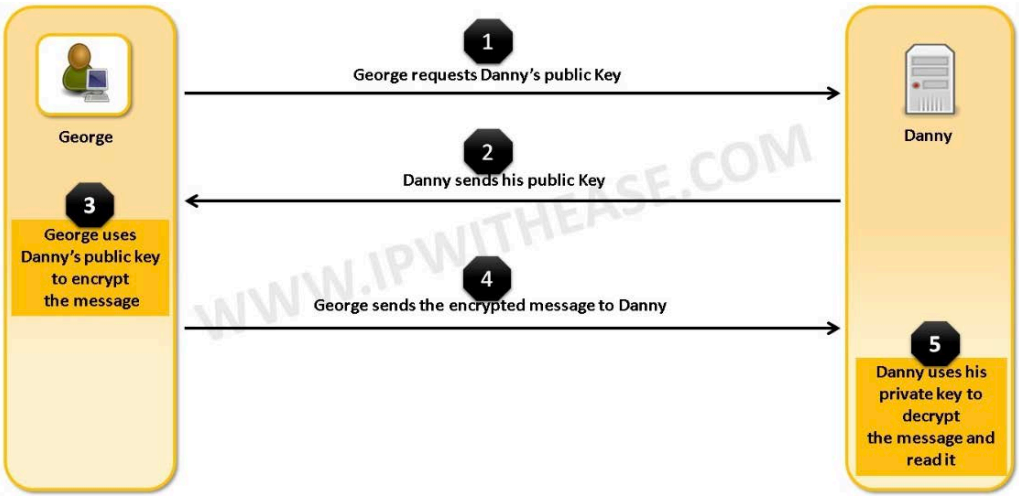

Figure 2. PKI Key Exchange. Source: [19].

Utilizing asymmetric cryptography methods, PKI employs software and encryption technologies to associate a unique digital signature to a specific claimant. This signature is included inside of the digital certificate that contains the owning claimant's public key. In this way, a claimant's public key is cryptographically *bound* to the registered claimant. This technology is designed to make "counterfeiting" (i.e., attacker impersonates a claimant) very difficult to achieve. Assuming then that the claimant's *private* key remains (by policy and design) only in the claimant's possession, then the stage is set for asymmetric-based digital authentication as follows. First, the user (now acting in the role of claimant) declares its identity to the verifier. Second, the verifier sends a random challenge to the claimant. Third, the claimant encrypts the challenge with its private key, and returns it to the verifier along with the claimant's digital certificate. Last, the verifier authenticates the claimant by ensuring that the certified public key in the certificate can correctly decrypt the encrypted challenge.

As described in NIST SP 800-32 [20], PKI allows entities to electronically exchange digital information with the confidence that:

- The person or process identified as sending the transaction is actually the originator.
- The person or process receiving the transaction is the intended recipient.
- Data integrity has not been compromised. [20]

B. NAVY-WIDE IMPLEMENTATION

The DoN policy for implementation of services related to identification and authentication is outlined in "DOD Instruction 8520.03, Identity Authentication for Information Services." The introduction from this document provides that:

> identity authentication for information systems and networks within the DOD must be conducted in a manner that provides confidentiality by mitigating against unauthorized access; provides integrity that protects against unintentional or malicious change; and provides availability of data for all DOD mission partners and users. [7]

It goes on to mention that in order "to perform proper authentication, information system owners must use identity authentication procedures that consider the importance and sensitivity of the information in a system, and recognize the threats and vulnerabilities to the system" [7]. The DoN uses PIV and CAC/PKI to authenticate claimants; these are described in the following paragraphs.

PIV—Per FIPS 201-2, lays out the implementation requirements for the use of PIV cards, and asserts that cards "must be personalized with identity information for the individual to whom the card is issued, in order to perform identity verification both by humans and automated systems" [10].

CAC—Per DOD Directive 5144.02, DOD Instruction 8520.03 implements "use of the DOD Common Access Card, which is the DOD personal identity verification credential, into identity authentication processes in DOD information systems where appropriate" [7].

PKI Certificate Policy—Per DOD Directive 5144.1, DOD Instruction 8520.02 lays out instructions to "establish and implement policy, assign responsibilities, and prescribe procedures for developing and implementing a DOD-wide PKI and enhancing the security of DOD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption" [15].

The objectives of this research, was to: 1) establish foundational principles of digital-based identification and authentication (I&A), 2) summarize existing related technologies, 3) summarize applicable DoN policy, 4) explore nascent I&A technologies

and initiatives, then 5) proffer recommendations for improving existing DoN I&A implementations based upon our observations. The preceding chapters have delivered items 1-3. Chapters IV and V will address items 4 and 5, respectively.

IV. MODERN/IMPROVED DIGITAL AUTHENTICATION METHODS

Within the past decade, security companies have been working to eliminate the practice of using passwords during the authentication process in order to move to a more secure infrastructure: specifically, a passwordless authentication ecosystem. According to the Fast Identity Online (FIDO) Alliance, over 80% of data breaches are attributed to cracked passwords [21]. As was discussed in Chapter II, passwords are an inherent vulnerability given that users tend to either reuse passwords, create variations of them, or create weak passwords for ease of remembrance. We note that although many of the authors referenced throughout this chapter use the term "credential" for the secrets used to conduct proof-of-possession of a secret-based authentication, we continue our usage of the NIST-preferred term: "authenticator" to avoid confusion.

A. AUTHENTICATION STANDARDS

With the development of newer and more technologically advanced authentication standards, new requirements are being levied on organizations to increase the strength of their authentication methods. The FIDO Alliance, in concert with the World Wide Web Consortium (W3C), is collaborating on technologies that are interoperable with popular software, and leverage hardware already in use by the DOD. In "Authentication in the Age of GDPR" [22], the author explains that the evolving authentication ecosystem, which incorporates third-party validation, exists for the purpose of decreasing vulnerabilities and costs for execution throughout the DOD [22].

The sections that follow will explore the following authentication standards and technologies: FIDO, OAUTH 2.0/OPENID CONNECT (OIDC), and CAC.

1. FIDO Alliance

The FIDO Alliance states it is an "open industry association with the focused mission; authentication standards to help reduce the worlds' over reliance on passwords" [23]. This alliance is comprised of multiple large organizations that are stakeholders in the securing of e-commerce, to include: Amazon, Apple, Facebook, Google, RSA, Yubico,

Wells Fargo, and NIST. In “Universal Second Factor Overview” [24], the FIDO Alliance describes their mission is to develop more secure online authentication standards by creating technical requirements, pursuing worldwide distribution, and certifying the underlying FIDO protocols to a global standard. According to the FIDO Alliance, their core efforts are: “1) ease of use, 2) privacy and security, and 3) standardization” [24]. FIDO standards were designed to protect privacy. “The protocols do not provide information that can be used by different online services to collaborate and track a user across the services” [25]. However, FIDO infrastructure provides options for “binding” a FIDO2 authenticator with an identity.

The next three sections will address the three different FIDO standards, all of which use public key cryptography. The first two, Client to Authenticator Protocols (CTAP) 1 and 2, utilize various technologies, to include: near field communications (NFC), Bluetooth Low Energy (BLE), software, or secured cryptographic capabilities [24]. In many of the suggested implementations of these technologies, the preferred platform for performing the underlying protocols are Universal Serial Bus (USB) devices. In contrast, the third standard, FIDO Universal Authentication Framework (UAF), relies on devices such as mobile phones or tablets. All three FIDO standards require that the claimant register the device to the specific service(s) it will be used to authenticate with. According to “How FIDO Works- Standard Public Key Cryptography and User Privacy” [25], “authentication is done by the client [claimant] device proving possession of its private key to the service by signing a challenge sent by the service. The client’s [claimant’s] keys can be used only after they are unlocked locally on the device by the user” [25]. Figure 3 displays the current compatibility between these standards and several common web browsers.

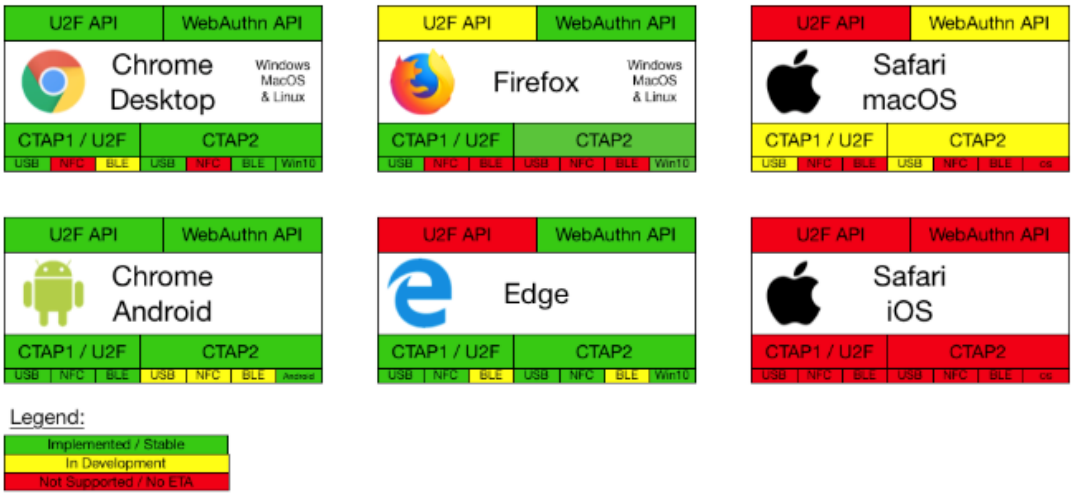

Figure 3. FIDO Support by Web Browser. Source: [26].

a. CTAP-1 (FIDO U2F)

CTAP-1, previously referred to as FIDO Universal Second Factor (U2F), is one proposed standard for providing the second factor of any MFA process wherein the first authenticator is the standard password. CTAP-1 is compatible with any relying party (RP) that supports this standard [24].

Figure 4 displays the process in which CTAP-1 conducts authentication, following registration of the device. First, a claimant inputs a username and password. Then the claimant plugs in a CTAP-1 USB device (or other approved devices) into the computer's USB port. In "Emulating U2F Authenticator Devices" [27], the author explains,

> Then the service formulates a challenge towards the authenticator device containing a key handle and a challenge. The authenticator device signs the challenge with the key associated with the specified handle and returns the result to the service. The service can now check the signature and match the used certificate against its user database. In case of a match, the authentication succeeds [27].

The CTAP-1 standard requires a physical "test of user presence" [24], which detects and confirms the user physically has the device. It is also used to ensure "that a signature happens only with the user's permission… [and] that malware cannot exercise the signature when the user is not present" [24].

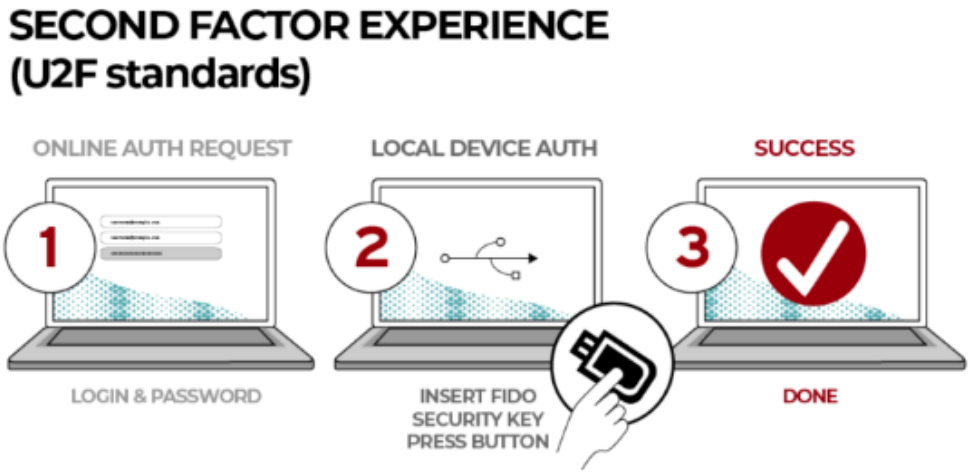

Figure 4. FIDO CTAP-1 Overview. Source: [28].

As of March 2020, the security company Yubico was the only vendor to receive FIPS 140-2 validation for their multi-protocol security key that supports CTAP-1. The validated security key meets AAL3 standards [29]. CTAP-1 devices use an X.509 attestation certificate during registration. Attestation certificates, also known as attribute certificates (AC), are, as described by [20], certificates that are cryptographically bound to their respective (owner) claimant, and which include select claimant attributes that enable access-related decisions. These certificates can be used for access control. Additionally, [20] states "ACs may also be used in the context of data origin authentication service and a non-repudiation service. In these contexts, the attributes contained in the AC provide additional information about the signing entity" [20]. ACs do not, however, facilitate authentication, because ACs do not contain claimant public keys [20]. Non-certified devices without an attestation certificate can still be accepted if the relying party consents to it [24].

b. CTAP-2 (FIDO 2)/WebAuthn

CTAP-2 is comprised of the FIDO Alliance's newest collection of specifications to enhance a passwordless ecosystem. CTAP-2 supports the use of existing specifications, making it compatible with CTAP-1 and FIDO UAF. CTAP-2 allows the claimant to "easily authenticate to online services in both mobile and desktop environments" [30].

This type of authentication mitigates the risk of replay attacks, phishing attacks, and the threat of password compromises. Authenticators are different with each website, and never leave the device on which they were installed. Additionally, the authenticators are never stored on a server [26]. CTAP-2 gives claimants the ability to use capabilities organic to their chosen/available device, or to use a FIDO security key. This provides a level of convenience to the claimants and allows them to choose what best satisfies their needs. In the CTAP-2 standard, the RP uses an X.509 certificate to verify attestation [31].

In concert with CTAP-2, the WebAuthn web application programming interface (API) enables the use of public key authentication, promoting a passwordless environment. In March 2019, the W3C recognized WebAuthn as an official web standard [32]. W3C develops "standards to ensure the long-term growth of the Web" [33].

Web Authentication, known as WebAuthn, is the API between the claimant and the RP. It is designed to grant claimants the ability to access internet accounts using a device of the claimants' choice [32]. CTAP-2 leverages WebAuthn specifications to construct a strong authentication standard. According to the FIDO Alliance, "WebAuthn enables online services to use FIDO Authentication through a standard web API that can be built into browsers and related web platform infrastructure" [30]. The CTAP-2/WebAuthn architecture is illustrated in Figure 5.

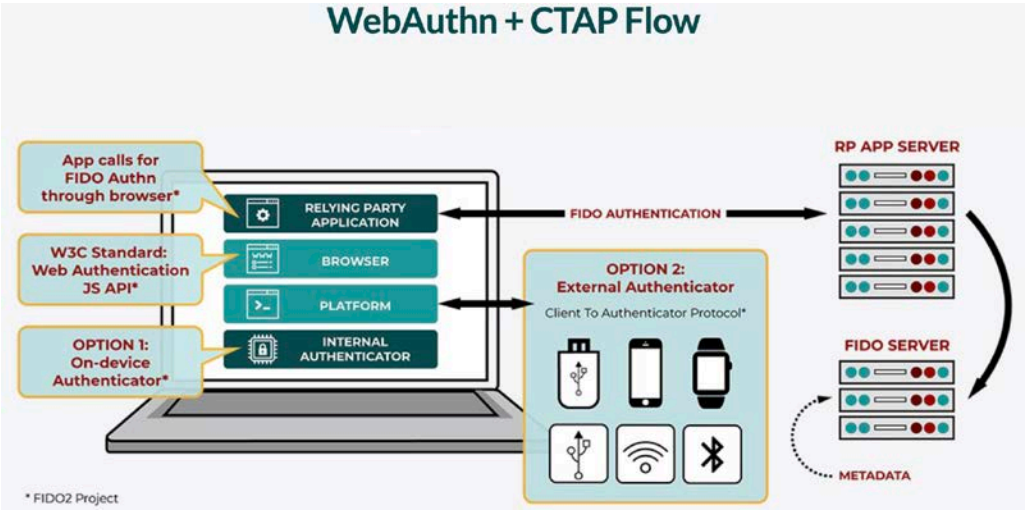

Figure 5. WebAuthn/CTAP Architecture. Source: [30].

Further, WebAuthn allows for claimant credentials to be integrated into major web browsers enabling the credential management API to, "create and register a public key credential for a website, and authenticate to a website by proving possession of the corresponding private key" [34]. According to Brand [34], this will strengthen the notion of a passwordless ecosystem by facilitating the following:

1. Low friction and phishing-resistant two-factor authentication (to be used in conjunction with a password)
2. Passwordless, biometrics-based re-authorization
3. Low friction and phishing-resistant 2FA without a password (to be used for passwordless accounts). [34]

Leveraging WebAuthn will allow claimants to register a credential to the chosen website, and also enable a website to authenticate a claimant and secure proof that the correct claimant is being communicated with [34]. In "Web Authentication: What It Is and What It Means for Passwords [35], WebAuthn is based on the FIDO UAF standard. WebAuthn handles "registration and authentication to a web application. The credentials created through the WebAuthn API rely on strong cryptographic principles and asymmetric encryption" [35].

c. FIDO UAF

According to FIDO Alliance [36], the FIDO Universal UAF is the standard that allows for password-less authentication, while still leveraging the ability to use MFA (i.e., a password is not one of the factors). FIDO UAF can work with CTAP-1, CTAP-2, or independently. FIDO UAF architecture is compatible with any RP that accepts the UAF standard. Once the UAF device (e.g., mobile phone or tablet) is registered, claimants will no longer need to use their password to authenticate to that service. Instead, the user will only need to authenticate to the local UAF device (i.e., the device in his/her presence and under his/her control) using one of the implemented non-password authenticators. FIDO UAF supports multiple authenticators for MFA (e.g. PIN + biometric) [28]. FIDO UAF uses an X.509 attestation certificate during registration [36]. Figure 6 depicts the FIDO UAF operation (assuming the device is already registered).

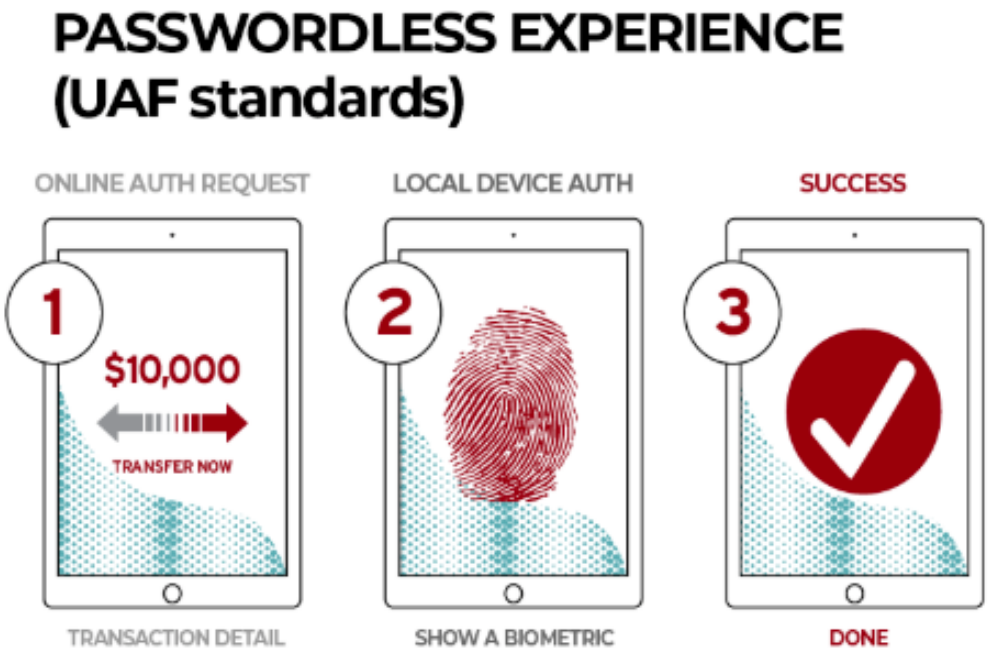

Figure 6. FIDO UAF Standard. Source: [28].

2. OpenID Connect/OAUTH 2.0

Prior to the advent of OAuth, the only method to share information between applications was for the claimant to authenticate directly and independently to each application involved [37]. According to Hardt [38], OAuth 2.0 and OIDC share mutually beneficial features that enable the "brokering" of claimant authentication among multiple applications. This "brokering" is facilitated by establishing login sessions with profile information related to the claimant. OAuth 2.0 is the framework that OIDC rides on, and is another standard offering passwordless authentication with single sign-on (SSO) functionality across multiple applications [38].

a. OpenID Connect

OIDC is becoming a widely used authentication standard. When an application, such as Facebook or Google+, asks a claimant to authenticate utilizing an authenticator for a another application, the application is more than likely leveraging OIDC [39].

OIDC can be described as “a thin layer that sits on top of OAuth 2.0 that adds login and profile information about the person who is logged in” [37]. The OIDC flow mirrors that of OAuth 2.0, which is described in Chapter IV.2.b; however, OIDC has two differences in the standard’s flow. The first difference occurs during the initial request; as OIDC requests a specific scope, which refers to which explicit permissions the client requested. The second difference occurs during the final exchange, when the client takes possession of both the access and ID tokens, which contains login information about the claimant [37].

b. OAUTH 2.0

OAuth 2.0 is not an authentication standard. It is important to address in this research; however, because it is sometimes confused with being an authentication standard. We address the details of OAuth 2.0 because it is used in conjunction with OIDC, and is a framework used for authorization and allows other applications to gain access, although limited, to an http service [38]. Access can be granted “on behalf of a resource owner by orchestrating an approval interaction between the resource owner and http service, or by allowing the third-party application to obtain access on its own behalf” [38]. The application is given a key that gives it specific permissions (scope) to access particular information on behalf of the claimant [37]. As noted by Hardt [38], this framework secured pre-existing issues that existed in the old client-server authentication model, to include:

- Storing credentials, typically an authenticator, for future use, in the clear.
- The requirement for servers to support authenticator approval, regardless of the known vulnerabilities inherent in certain authenticators.
- Applications receiving more access than necessary, thus compromising the resource owners’ capacity to limit accesses to restricted resources.
- Compromise of a third-party authenticator resulting in the compromise of all resources and data protected by that authenticator. [38]

The flow described in RFC 6749 between the resource owner, the resource server, the client, and the authorization server is as follows:

- The client requests authorization from the resource owner. The authorization request can be made directly to the resource owner (as shown), or preferably indirectly via the authorization server as an intermediary.
- The client receives an authorization grant, which is a credential representing the resource owner's authorization, expressed using one of four grant types defined in this specification or using an extension grant type. The authorization grant type depends on the method used by the client to request authorization and the types supported by the authorization server.
- The client requests an access token by authenticating with the authorization server and presenting the authorization grant.
- The authorization server authenticates the client and validates the authorization grant, and if valid, issues an access token.
- The client requests the protected resource from the resource server and authenticates by presenting the access token.
- The resource server validates the access token, and if valid, serves the request. [38]

3. CAC

As discussed in Chapter III.A.3, the CAC/PKI authentication standard is the current PKI-based authentication standard for the U.S. Department of Defense. On December 7, 2018, the DOD released a memorandum titled "Modernizing the Common Access Card—Streamlining Identity and Improving Operational Interoperability" [12]. According to the "DOD Cybersecurity Discipline Implementation Plan" [12], the memo was in response to the DOD's acknowledgement that it lacked the common PKI standards used by the rest of the Federal Government. The then current practices had resulted in poor interoperability between DOD and other government agencies (OGAs). The memo directs the DOD to align its use of the CAC with the Federal PIV-Auth certificate [40]. The memo outlines the following methods to accomplish this process:

- Secure information exchange with DOD and OGAs by standardizing protocols and reducing inefficiencies.

- Use a standard PKI authenticator to improve cybersecurity and streamline configuration and change management.
- Reduce costs with maintaining legacy authentication infrastructure.
- Support commercial products that are HSPD-12 PIV/PKI compliant. [40]

Modernizing the CAC will decrease the number of certificates on a CAC from four to three. The current CAC PKI X.509 certificates are DOD identity, DOD PIV Authentication, DOD e-mail signing, and DOD e-mail encryption. As stated by "Modernizing the Common Access Card - Streamlining Identity and Improving Operational Interoperability" [41], following this conversion, the DOD "identity certificate will be removed and the e-mail signing certificate will no longer support client authentication," (e.g., secure logon to CAC-enabled services).

B. AUTHENTICATION PRODUCTS/VENDORS

From our research, we chose these four products because they had strong MFA standards: RSA, CyberArk, Yubico, and Okta.

1. RSA

RSA offers an MFA product called SecurID Access. This product is compatible with authentication for information technology (IT) devices in one's local (on premises) environment, as well as authentication among IT devices interacting with a cloud infrastructure environment. This product can support: "mobile push authentication, biometrics (fingerprint, eye print), short messaging service (SMS), voice, e-mail, risk-based, FIDO, proximity-based authentication and soft tokens, and, … hardware tokens" [42]. SecurID offers options for both hardware and software tokens and can be deployed locally, in the cloud, or part of a hybrid environment [42].

2. Cyber Ark

In March 2016, the CyberArk privileged account security solution became the only privileged account solution on the U.S. Department of Defense Information Network (DODIN) Unified Capabilities Approved Products List (UC APL) [43].

CyberArk advertises itself as a security provider that offers the industry's most comprehensive answer, "for protecting, controlling, and monitoring privileged access across on-premises, cloud, and hybrid infrastructure" [44]. CyberArk offers a multitude of products from privileged access solutions to cloud services, and application and endpoint management. Product experts from CyberArk will survey, employ, and provide management of programs to maximize what the overall security posture should be [45].

CyberArk's privileged access security solution, formerly known as "privileged account security solution," attempts to protect privileged accounts. According to a white paper "Privileged Account Security Solutions: A Competitive Review" [46], a review conducted by IDG Strategic Marketing Services and CyberArk, states that 80% of security breaches involved a compromised privileged account. The white paper uses the Office of Personnel Management (OPM) and Bangladesh Bank breaches as examples of how an administrator account was compromised, allowing hackers to obtain access to privileged accounts [46].

The CyberArk privileged access security solution is currently deployed to "multiple Department of Defense customers and 130+ installations across the U.S. federal government" [47]. The security solution is FIPS 140-2 validated and can support AES-256 and RSA-2048 encryption algorithms. It can accept many forms of authentication to include: password, RSA SecurID, PKI, and smart cards. It also can support a large number of technologies, to include, network devices, databases, security appliances, cloud environments, directories, and applications; among many others [44].

3. Yubico

Yubico is a company that develops physical MFA devices that can be implemented with several different authentication standards that were discussed in Section B of this chapter. This research focuses on the "YubiKey FIPS Series" devices because they are the only

security devices that are FIPS 140-2 validated with an overall rating of Level 2, and a physical security rating of Level 3. These devices meet AAL3 standards [48].

Though the series includes four versions of MFA devices, there is no operationally-relevant distinction beyond which USB type is used. The series of devices include two of which are USB-A and two of which are USB-C. All four of these devices have the same functionality with the following standards supported: "FIDO U2F, smart card (PIV), YUBICO OTP, OpenPGP, OATH-TOTP, OATH-HOTP, and Challenge-Response" [48]. The supported cryptographic algorithms are: "RSA 2048, ECC p256, ECC p384" [48]. YubiKeys use hardware to protect these cryptographic devices.

4. Okta

Okta offers "Workforce Identity" products to include "Adaptive MFA." Okta states the "Adaptive MFA" will secure applications and VPNs [49]. Figure 7 displays the supporting authenticators that Okta's "Adaptive MFA" can support. Adaptive MFA can also enable policies to mediate access based on location, device, and network context. Okta states that their infrastructure has achieved certifications that include FedRamp ATO (approval to operate) and FIPS 140-2 validation; and that they support PIV/CAC authentication [50]. FedRamp is a program run by the government which is intended to provide "a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services" [51].

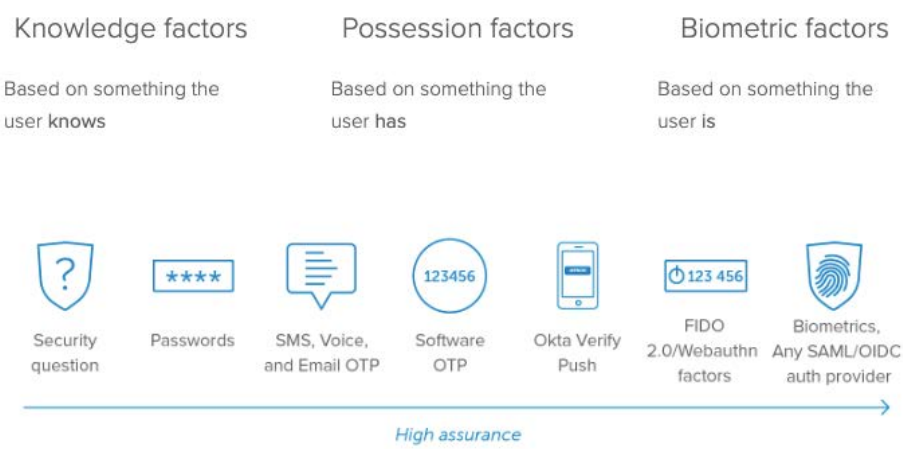

Figure 7. Okta Adaptive MFA Supported Standards. Source: [52].

C. AUTHENTICATION METHODS COMPARISON

Table 3 was created to compare the different methods discussed in Section A of this chapter by ranking them based on a list of weighted criteria. The table utilizes weighted technical and environmental attributes that are key considerations when dealing with the DoN authentication ecosystem. A Weighted Objectives Method [53], was used to determine which digital authentication method would be the best fit for the DoN to modernize its current authentication practices.

The attributes in Tables 3 and 4 were selected based on our research of the NIST 800-63 Series and FIPS 140-2; and these attributes were determined to be the most relevant for consideration by DoN decision-makers. Table 3 is used to determine the most secure authentication method, with no direct consideration given to likely DoN usability issues. Effectively then, this table ignores the denominator (investment) in the well-known return on investment relationship (ROI), and concerns itself only with security strength (return). Table 4 reproduces Table 3, but adds four usability considerations which are negatively weighted (-1) to "penalize" any method that does not satisfy the usability attribute listed. These usability columns provide a means to tabulate added/required infrastructure investments that may alter the scoring of our candidate authentication methods. We deemed this to be important as it informs security decision makers who are applying a risk management (cost vs. benefit) approach to such investments. We weighted our security

attributes with integer values ranging from 0 to 3. A weight of 0 was included for instances where a range of weights were possible for a given attribute, but for which a given method did not satisfy even the lowest (weight of 1) requirement for the attribute. A fixed weight of 1 was given to attributes that we determined are important for secure authentication, but are not required by the NIST 800-63 series. A fixed weight of 2 was given to attributes that are mentioned in the 800-63 series, but not required to achieve AAL3. Finally, a fixed weight of 3 was given to attributes that are required by the NIST 800-63 series to achieve AAL3. The following bullets list the attributes, show the weights, in parentheses, that were assigned, and include a brief rationale for the weight chosen for each:

- Passwordless (1): While this attribute is good to have due to the weaknesses inherent to passwords; it is not required by [3].

- Asymmetric Keys (3): This attribute is ascribed to methods that utilize public and private keys, "which are used to perform complementary operations such as encryption and decryption or signature verification and generation" [3].

- MFA (3)—To achieve AAL3, NIST 800-63B [6], requires MFA.

- FIPS 140-2 Verification (0-3)— To remain consistent with the NIST SP 800-63B we labeled this attribute FIPS 140-2 Verification. As we discussed in Chapter II.B, we believe it is "validation." This attribute was weighted 0-3. A weight of 0 indicates the authentication method does not have FIPS 140-2 validation. The authentication method was given a weight of 1 if it had the appropriate FIPS 140-2 validation to achieve AAL1. A weight of 2 was assigned if it had the appropriate FIPS 140-2 validation to achieve AAL2. Finally, a weight of 3 was given if the appropriate FIPS 140-2 validation to achieve AAL3.

- Physical Authenticator (3): AAL3 requires proof of possession of a key (secret) and a cryptographic protocol. At this level, a hardware-based (physical) authenticator must be used [6].

- Authenticator Recovery Notification to User (2): NIST 800-63B [6], references that poorly implemented authentication recovery is a weak point owing to its vulnerability to social engineering attacks. To thwart such attacks, a notification to the user of any attempt to recover an authenticator can inform the user of malicious activity.

- Provides an Attestation Certificate (2): NIST 800-63B [6], states that "attestation information MAY be used as part of a verifier's risk-based authentication decision."

- Phishing Resistant (2): An authentication method offering phishing resistance with, "approved cryptographic algorithms shall be used," when it is necessary [6]. The implementation will establish safeguards against RP impersonation, adding another level of security against malicious actors.

- Implements Traditional PKI (0-2): The PKI model has been used for years within the DoN and has been proven to be a safe and viable attribute for more secure authentication. Two key characteristics of the PKI model are that certification of subscribers' public keys is centralized to a certification authority (CA), and the subscribers have their true identities vetted during the enrollment phase of their digital certificates' life-cycle. A weight of 0 was given if neither of these 2 aspects were met. A weight of 1 was given if only 1 of these aspects was met. A weight of 2 was given if both of these aspects were met.

Although not specifically referenced in NIST 800-63B [6], we included four usability attributes in our analysis because this information helps to ground our DoN recommendations in Chapter V. We used the information provided in Chapter II.F from Table 2 to determine the attributes of usability that we consider the most important in a DoN infrastructure. The identified attributes were deemed important based on the research that we conducted to support and discuss Chapters I-IV, in addition to our experiences

working in many different DoN environments. The NIST SP800-63B states that the goal of authentication usability is “to minimize user burden and authentication friction (e.g., the number of times a user has to authenticate, the steps involved, and the amount of information he or she has to track” [6]. The usability attributes that were identified will support the NIST definition of authentication usability. The following bullets reference each usability attribute and include a brief description of why they are important to the current DoN infrastructure:

- Compatibility with Cloud Based Systems: As the DoN moves towards migrating to cloud-based applications, authentication methods need to meet compatibility requirements for successful implementation.

- Authenticator Availability: Authentication methods that require either a mobile device, NFC, Bluetooth, or physical key for authenticating a claimant were penalized considering there are many work environments wherein DoN employees will not be authorized to use these technologies.

- Location / Availability of Direct Computer Interface (e.g. USB port): Several authentication methods require a connection to a USB port. It is imperative that a claimant has the ability to utilize these ports for authentication.

- Interoperability with Legacy Systems: Due to the reliance and use of older legacy systems in the DoN, interoperability between legacy systems is of the utmost importance. Authentication methods need to be compatible for the security and operation of legacy systems.

Following the assignment of weighted attributes, a total was calculated for each method, with a maximum possible weighted total of 21 for both Table 3 and Table 4.

Table 3. Security Attributes of Methods

METHODS	SECURITY ATTRIBUTES									TOTAL WEIGHT
	ASYMMETRIC KEYS	MFA	PASSWORDLESS	FIPS 140 VERIFICATION	PHYSICAL AUTHENTICATOR	AUTHENTICATOR RECOVERY NOTIFICATION TO USER	PROVIDES ATTESTATION CERTIFICATE	PHISHING RESISTANCE	IMPLEMENTS TRADITIONAL PKI	
WEIGHT	**3**	**3**	**1**	**0-3**	**3**	**2**	**2**	**2**	**0-2**	**21**
CTAP1 (FIDO U2F)	●	●		3	●	*	●	●	0	**18**
FIDO2 (PSUEDONYMOUS)	●	●	●	3	●	*	●	●	0	**19**
FIDO2 (IDENTITY VERIFIED)	●	●	●	3	●	*	●	●	1	**20**
FIDO UAF	●	●	●	2	●	*	●	●	0	**15**
OPENID	●	●	●	3			●		1	**13**
CAC	●	●	●	3	●	●	●	●	2	**21**
2FA		●		0	●	*	●		0	**10**
PASSWORD				0		*			0	**2**

* If properly set up MFA prior to lost device; else these points should be subtracted from the total shown.

Table 4. Security Attributes of Methods with DoN Usability "Penalties" Considered

METHODS	SECURITY ATTRIBUTES									USABILITY W/ DON INFRASTRUCTURE				TOTAL WEIGHT
	ASYMMETRIC KEYS	MFA	PASSWORDLESS	FIPS 140 VERIFICATION	PHYSICAL AUTHENTICATOR	AUTHENTICATOR RECOVERY NOTIFICATION TO USER	PROVIDES ATTESTATION CERTIFICATE	PHISHING RESISTANCE	IMPLEMENTS TRADITIONAL PKI	COMPATIBILITY W/ CLOUD BASED SYS	AUTHENTICATOR AVAILABILITY	LOCATION/ AVAILABILITY OF DIRECT COMPUTER INTERFACE (e.g. USB Port)	COMPATIBILITY W/ LEGACY SYS	
WEIGHT	3	3	1	0-3	3	2	2	2	0-2	0 = meets requirement -1 = does not meet requirement				21
CTAP1 (FIDO U2F)	●	●		3	●	*	●	●	0	-1	0	0	-1	16
FIDO2 (PSUEDONYMOUS)	●	●	●	3	●	*	●	●	0	0	0	0	0	19
FIDO2 (IDENTITY VERIFIED)	●	●	●	3	●	*	●	●	1	0	0	0	0	20
FIDO UAF	●	●	●	2	●	*	●	●	0	-1	-1	-1	-1	11
OPENID	●	●	●	3			●		1	0	-1	0	0	12
CAC	●	●	●	3	●	●	●	●	2	-1	0	0	-1	19
2FA		●		0	●	*	●		0	0	0	0	0	10
PASSWORD				0		*			0	-1	0	0	0	1

* If properly set up MFA prior to lost device; else these points should be subtracted from the total shown.

V. IMPROVING U.S. NAVY DIGITAL AUTHENTICATION

Secure operations in an increasingly digitized and online environment is something that impacts virtually every aspect of the DoN's ability to accomplish its mission. Controlled access to digital resources lies at the heart of preventive security controls, and audited (user and program) system-level events lie at the heart of accountability (and related investigative) security controls. Given that authentication is a core enabler for both of these security control types, this chapter utilizes the analysis used to build Tables 3 and 4 in Chapter IV.C, to formulate recommendations for modernizing the DoN's current authentication methods.

A. CURRENT DON AUTHENTICATION ENVIRONMENT

As addressed in Chapter III.B, the adopted standard currently being utilized by the DoN is the CAC model. Also, Chapter III.B references the documents governing the employment and regulations for effective CAC integration. For perspective, this section will address current authentication processes used by the DoN (i.e., the status quo), in order to compare them to recommended improvements.

1. Distribution of CAC to DoN Personnel

CAC distribution occurs immediately upon either volunteering for active duty/ reserve military service, accepting employment as a DOD civilian, or for those fulfilling DOD eligible contracts. As stated in DOD Instruction 1000.13, "the CAC, a form of DOD ID card, shall serve as the PIV card for DOD implementation of HSPD—12" [54]. Effective CAC distribution will be accomplished by complying with the following criteria:

- Issued based on sound criteria for verifying an individual employee's identity
- Strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Issued only by providers whose reliability has been established by an official accreditation process. [2]

PKI certificates are issued onto CACs, allowing personnel to access DOD-specific websites and digitally sign and encrypt electronic correspondence. Per the DOD X.509 Certificate Policy, PKI certificates will be distributed to the following claimants who have a legitimate need:

- DOD uniformed and civilian personnel, and eligible contractors
- Executive department and agency personnel, and eligible contractors
- State governments
- Foreign government and foreign organization personnel, and eligible contractors. [14]

For those entities that do not have access to DOD approved credentials, there are External Certification Authority (ECA) PKI certificates [55]. These certificates will authorize commercial partners to establish secure means of communication with DOD agencies.

2. DON Instructions Governing Present Authentication Policies

The governing documents that guide the DoN with its governance of authentication policies and procedures are:

- SECNAV INSTRUCTION 3052.2: CYBER POLICY AND ADMINISTRATION WITHIN THE DON
- SECNAV INSTRUCTION 5239.3C: DON CYBERSECURITY POLICY
- OPNAV INSTRUCTION 5239.1D: USN CYBERSECURITY PROGRAM

These documents all refer to the overarching DOD instructions discussed in Chapter III.B. Those instructions inform DOD managers regarding how to obtain and maintain interoperability between each branch of the military and partnering agencies, as well as interoperability between legacy systems. The importance of maintaining a robust cybersecurity posture is expounded in each of these documents. The overarching emphasis in the documents is perhaps best expressed in the “US Navy Cybersecurity Program” [56] as the:

> prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wired communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. [56]

B. RECOMMENDATIONS FOR ENHANCED DON-WIDE AUTHENTICATION

The attributes of the different authentication methods from Table 3 and Table 4 were used to select the recommendations. These weighted tables represent the foundation of our overall recommendations to enhance the DoN authentication environment. The results gleaned from Table 4 enabled us to identify four Tiers of authentication methods and the products that are utilized to implement them. The identified Tiers and their corresponding methods are: 1) CAC, 2) FIDO2, 3) 2FA (password and device), and 4) password-only. According to Table 3, CAC received the highest point total, signifying it as the most secure authentication method. When adding usability attributes, as displayed in Table 4; however, FIDO2 took the lead position among the contending methods. The aforementioned Tiers were organized based on the order of the authentication security provided (i.e., 1 provides the most, 4 the least). Given that a risk management approach is prudent here, the four tiers enumerated provide DoN cybersecurity decision-makers with options that provide the necessary—risk vs cost—flexibility.

As discussed in Chapter II.B, when PII or personal information characterizes the information for which authentication is required, AAL2 should be used [6]. AAL2 requirements are met in Tiers 1 through 3. According to DODI 8520.03 [7], "information that could adversely affect DOD mission interests and would have a moderate or high impact on the efficacy of DOD missions if the information were compromised," would require, at a minimum, MFA (also provided by Tiers 1 through 3). Examples of this type of information are personnel information, logistics, or finance [7]. Furthermore, when critical information that could result in "severe mission capability degradation, major damage to DOD information based resources, or a risk of serious injury or death to personnel, but that has not been specifically authorized to be classified," at a minimum, PKI-based authentication (provided by Tiers 1 and 2) is required [7]. On DOD networks,

password-only authentication (Tier 4) is only approved when the "Sensitivity Level" of the information "would have a low or moderate adverse impact on the efficacy of DOD missions or the reputation of the DOD if the information were compromised" [7].

It should be noted here that our research was initially scoped to preclude the identity vetting aspect of the full authentication life-cycle (see Section I.A.1). This was decided owing to our interest in focusing more narrowly on the authentication processes that occur post-enrollment; that is, those processes directly related to a claimant proving possession of an already registered secret or biometric. It later became evident; however, that some degree of consideration was warranted in this regard, specifically as it pertained to authentication methods that were designed to offer anonymity as an option (e.g., FIDO2). This consideration of identity vetting is effectively captured in the Table 3 and Table 4 security attribute labeled: "Implements Traditional PKI." This attribute was described in Section III.C. Given that DoN's most risk averse environments are unlikely to support any degree of anonymity (barring under-cover work), this attribute was largely at the heart of the criteria used to discriminate our Tier 1 (most secure) and Tier 2 (second most secure but more widely supportable) recommendation choices.

Our recommendations stem from the results of the combined security and usability attributes listed in Table 4; all of which are detailed next.

1. Tier-1 (CAC)

CAC achieves AAL3. The CAC architecture is the current authentication method used by the DoN. For reference, Chapter III details how CAC is implemented.

a. Strengths

This Tier does not require the DoN to incur any additional developmental costs, given this architecture is currently implemented. Furthermore, the DoN will not have to provide any additional training to IT personnel. In contrast to other tiers, the CAC can be used in all work environments.

b. Challenges

Not every DoN employee is eligible for a CAC [57]. As a result, they will have to rely on less secure authentication methods when accessing a government system. To overcome this challenge, the DoN could consider changing this policy, thus allowing more employees to be eligible to receive CACs.

According to the FIDO Alliance [57], CAC is not easily integrated with legacy systems that do not have CAC infrastructure established. Furthermore, as the DoN moves to more cloud based applications, many of these applications do not support CAC/PKI [57]. These are the very usability factors that favor a 2nd Tier option that, even though not matching the security strength of the CAC method, still meets the AAL3 standard while also being more interoperable in more environments than the CAC.

2. Tier-2 (FIDO2)

FIDO2 standards achieve AAL3. Following our research and the results from Table 3, we observed that FIDO2 is not as secure as CAC authentication, but it makes PKI-based authentication more widely available. FIDO2 can leverage other secure authentication standards, such as the CAC, which may already be integrated within existing DoN infrastructure. Incorporating FIDO2 into the current DoN infrastructure would provide additional security in all operational instances that are currently using weaker methods (i.e., those less than AAL3, such as a password only method). According to the FIDO Alliance [57], "FIDO is not a replacement for PKI but rather complements it, enabling greater number of users and applications to be protected using asymmetric encryption."

a. Strengths

According to "NIST 800-63 Guidance and FIDO Authentication" [58], the FIDO2 authentication standards meet NIST AAL3. These standards protect claimants from having their authenticators re-used, owing to the fact that their authenticators never leave the device. Additionally, FIDO2 standards prevent phishing attacks because authenticators cannot be shared [58]. FIDO2 standards are also relatively easy to deploy, as they do not require middleware.

The General Services Administration's (GSA) website, *login.gov*, provides an excellent example of how FIDO2 is utilized in a government system [59]. Prior to GSA implementing FIDO2, GSA evaluated several different authentication standards to determine how these standards integrated with their priorities: security, cost, and compliance [59]. Ultimately, GSA chose FIDO2 because of its phishing resistance (security), its relatively low cost (a usability factor), and its compliance with NIST SP 800-63B (compliance) [59].

Using FIDO2, employees would be able to access government systems with a FIDO security key, or with their own devices, such as cell phones, if they are FIDO-compatible. According to Corum [60], PIV credentials "are not issued to all individuals accessing agency networks and services, so this could prove a cost effective, rapid approach to authenticating these individuals."

b. Challenges

These standards require a FIDO-compliant device, such as a mobile phone, or a FIDO security key. Many environments in the DoN do not permit mobile devices in workspaces. For those situations, a FIDO security key would be necessary. However, the Yubico FIPS keys, as discussed in Chapter IV.B.3, are relatively expensive to implement, ranging in price from $46 to $69 each [48].

Further, in order to implement FIDO2, the DoN will have to develop code that enables WebAuthn to function. According to FIDO Alliance [59], GSA was able to develop the code in two weeks with a team of three persons. The team was able to create the code quickly because the code is open-source on GitHub, which offers the developers a solid starting point. As a result, this challenge is deemed relatively easy to overcome.

3. Tier-3 (2FA (Password + Device))

Two Factor Authentication achieves AAL2.

a. Strengths

2FA is a less expensive option than is employing either of the methods enumerated for Tiers 1 and 2. This is related to the fact that DoN employees can likely utilize their own personal devices as the second factor in those less security stringent environments where personal devices are permitted.

b. Challenges

Similar to one of the challenges with FIDO2, many work environments do not authorize *personal* devices in the workplace. Therefore, 2FA would be hard to implement in these environments given that e-mail (a popular method of delivering the 2nd factor to claimants using their *work* devices), is not authorized as an out-of-band authentication method for 2FA [6].

2FA also has vulnerabilities that make it more susceptible to phishing and account recovery attacks. In some instances, account recovery bypasses the second authentication factor by resetting the password of an account, which can be exploited by attackers. Attackers have successfully used this method to gain access to accounts that had 2FA enabled [61]. For example, in 2011, a Chinese, state-sponsored hacking group successfully bypassed RSA's SecurID 2FA system [62]. RSA's Executive Chairman wrote,

> While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack [63].

4. Tier-4 (PW only)

Password only authentication achieves AAL1.

a. Strengths

Password-only authentication incurs no additional overhead costs, which is similar to our Tier 3 recommendation. This method of authentication also has widespread support throughout the authentication ecosystem.

b. Challenges

Where the DoN currently supports password-only authentication, it continues to subjugate itself to the list of vulnerabilities described in Chapter II.E. These inherent risks can be ameliorated somewhat with complex password policies.

C. SUMMARY

In the process of conducting research on the various digital authentication methods, highlighting security attributes, and examining usability attributes within the existing DoN infrastructure, this chapter focused on choosing the most suitable options. The recommended tiers were developed from the results gleaned from Table 3 and Table 4.

VI. SUMMARY AND FUTURE WORK

This thesis examined the current digital authentication standards currently employed by the DoN, analyzed the governing documents and instructions that provide direction and performed an in-depth examination into more modern options available for operational use. It also analyzed the methods and their usability within the DoN's authentication ecosystem.

A. SUMMARY

By analyzing a relatively large sample of modern digital authentication standards, this thesis offered recommendations to improve the overall security strength of the Navy's currently deployed digital authentication ecosystem. This effort revolved around four main areas of inquiry: 1) the clarification of terminology used in the subject of I&A, 2) an assessment of protocols and techniques (collectively "methods") available to conduct I&A, 3) the identification of security and usability attributes useful for comparing I&A methods, and 4) understanding the competing methods sufficiently so as to be capable of assigning appropriate weights to each with regard to how well they satisfy our chosen comparison attributes. The security and usability attributes are presented in tabular form in Table 3 and Table 4, respectively.

Given that security controls are largely driven by a risk management approach (i.e., the impact of a potential security control failure influences the security investment), we sought to present a tiered (range) of I&A methods to DoN managers. As such Tier 1 is considered the most secure, and thus most appropriate for high impact (or high risk) operations; and Tier 4 is considered the least secure (except for no I&A), and thus only appropriate for relatively low impact (or low risk) operations. In the final analysis, we articulated four Tiers as follows: Tier 1—CAC-based PKI method, Tier 2—FIDO2-based PKI method, Tier 3—2FA method, and Tier 4—password-only method.

1. Standardizing the Terminology

One of the many challenges of conducting research on this topic was the wide-ranging and not always standardized jargon that is used throughout the literature on this topic. This thesis required the delineation between, and explanation of, key terms used to describe different aspects of the modern authentication environment, so as to minimize possible confusion between key topics.

Key terms established in Chapter I.C of this thesis for uniformity include the following:

- Attribute—Specific information that correlates the claimant to a digital identity (e.g., name, agency name)
- Authenticator—represents whatever is being presented by the claimant to satisfy the authentication criteria utilized by the verifier (e.g., password)
- Authentication—the act of verifying a claimant's preferred identity
- Claimant—the entity that is claiming ownership of a registered persona, as (typically) represented by an identity (e.g., username)
- Credential—that which binds an authenticator to a claimant (e.g., a claimant's digital certificate containing the public key that corresponds with the authenticator private key)
- Registrant—an entity that is in the process of having its persona validated (usually via corroboration with extant forms of identification) by various authorized criteria or processes (also referred to as enrollment)
- Relying Party (RP)—the entity that has a security-related interest in the truthfulness of a claimant's declaration of a particular identity, usually for purposes of access control or non-repudiation
- Token—A digital object (e.g., a unique string of characters bound to a claimant for identity authentication, that will not be shared between

claimants) presented to a claimant that serves as proof verifiable by a 3rd party RP that the claimant has been authenticated by a verifier

- Verifier— the entity in possession of previously registered authenticators associated with registered claimants (e.g., biometric or secret), which performs the authentication process

- Identity— The claimant will be distinguished with the unique characterization provided by the CSP (e.g., john.doe3690)

2. Methods That Were Considered and Why

With the added complexity of navigating a dynamically and fluid environment in which identification and authentication are required, the research for choosing an authentication method was dictated by what would best fulfill the needs of the DoN's efforts to modernize information security.

Through review of the NIST 800-63-3 series, and online resources like the FIDO Alliance and W3C, authentication methods were selected on the basis of how secure they could be, and whether or not they could satisfy DOD security implementation standards. Other factors considered for inclusion were technological attributes that were interoperable with existing infrastructure, and the requirement for additional hardware or software prescribed by governing documents. The following authentication methods were identified and analyzed in Chapter IV.A to construct a sufficient recommendation for implementation:

- CTAP-1 (FIDO U2F)

- FIDO2 (CTAP-2/WEBAUTH)

- FIDO UAF

- OPENID

- CAC

- 2FA
- Password

The basis for the continued research and analysis of the methods was determined, and tabulated as attributes in Tables 3 and 4. Further, these attributes were weighted in terms of their relative security strength and usability within the DoN.

3. Primary Guidance for Evaluating the Contenders

The guidance for evaluating authentication methods was dictated by factors mandated by several over-arching documents that included implementation guidance and technical requirements. The publications and resources cited throughout this thesis provided a baseline for the research, and a wealth of knowledge for determining whether or not each recommended option's passwordless authentication ecosystem was viable.

a. NIST 800-63 SERIES

This series of instructions was written and disseminated to be the guiding principles to, "provide technical requirements for federal agencies implementing digital identity services" [3]. The following publications provide the guidance and requirements for what meets the DOD standard:

- NIST 800-63-3—Digital Identity Guidelines
- NIST 800-63A—Digital Identity Guidelines: Enrollment and Identity Proofing
- NIST 800-63B—Digital Identity Guidelines: Authentication and Life cycle Management
- NIST 800-63C—Digital Identity Guidelines: Federation and Assertions

b. FIPS 140-2

The FIPS 140-2 [9] was crucial to the research because it served as the guideline for the security requirements set forth by the NIST 800-63B. It articulates a standard that is required for use by Federal organizations when it is made evident that a "cryptographic-based security system," must be relied upon for the security for sensitive data [10].

Also, FIPS 140-2 security level requirements for cryptographic modules were discussed in Chapter II.B, with Level 1 specifying the least security required of cryptographic modules, and Level 4 specifying the most. These levels played a relatively decisive role when assigning weight values to each standard that was considered in Chapter IV and described in detail in Chapter II.B.

c. U.S. DOD X.509 Certificate Policy

The X.509 Certificate Policy was used to outline the guidelines that would need to be considered for the implementation of a reliable PKI infrastructure. Additionally, this publication sets the guidelines for which equipment is authorized, and which guidelines a certification authority (CA) must adhere to for establishment and operation [14].

d. FIDO Alliance

The FIDO Alliance is an open standard that aims at eliminating passwords, and providing MFA and 2FA environments [21]. Because the goal of the research was to improve and modernize the DoN's current authentication methods, third party methods like FIDO's CTAP-1 (FIDO U2F), CTAP-2 (FIDO2), and FIDO UAF became viable options when performing the analysis to formulate an impactful recommendation.

e. W3C

Similar to the FIDO Alliance, W3C is open platform that allows developers to share and make improvements to the overall health and growth of the web [64]. Information pertaining to standards like OIDC, OAuth 2.0, the WebAuthn authorization API, and other technologies associated with authentication can be easily researched here.

4. Metrics of Comparison

Two tables were established at the end of Chapter IV for the purpose of providing a high-level summary of the most applicable metrics (captured as attributes) useful for comparing each authentication method against the others. The security-related metrics chosen were: asymmetric keys, MFA, passwordless, FIPS 140 verification (MFA must meet Level 2 and single factor cryptographic devices must meet level 1), physical

authenticator, authenticator recovery notification to the user, phishing resistance, implements traditional PKI, and provides an attestation certificate. The usability metrics from the NIST 800-63B chosen were: authenticator availability, location availability of direct computer interface (e.g. USB port), compatibility with cloud-based systems, and interoperability with legacy systems [6].

Table 3 was used to tabulate methods with order based solely upon the desired security attributes of a digital authentication system. Issues related to DoN usability and the potential for additional costs related to upgrading infrastructure to support the methods were omitted. This was done to show the clear *security* winners when immediacy of implementation may be of lesser concern than security. This is useful for situations wherein DoN decision-makers may deem the risks associated with authentication failures to be so high, that budget increases are justified for mitigation. This follows well established risk management policy.

Table 4 was used to tabulate Table 3 with DoN usability/cost "penalties" subtracted to account for likely usability challenges and added costs associated with implementing each of the methods being compared. These usability "penalties" affected the ordering of the top methods from Table 3. FIDO2 superseded CAC since it has usability attributes that are more compatible within the DoN infrastructure (e.g., compatibility with legacy and cloud-based systems).

5. Ranking and Recommendations

The results from Table 3 and Table 4 constituted the foundation of our recommendations to enhance the DoN authentication environment. CAC (Tier 1) was the strongest authentication method in Table 3 (most secure), and FIDO2 was the strongest method in Table 4 (usability). If these methods are not an option, this thesis recommends that 2FA (Tier 3) be implemented. Finally, password-only authentication (Tier 4) is recommended only when the aforementioned authentication methods are not available or cannot be integrated.

According to DODI 8520.03 [7], Tiers 1, 2, or 3 would suffice if the information for which authentication is required "could adversely affect DOD mission interests and

would have a moderate or high impact on the efficacy of DOD missions if the information were compromised." Furthermore, only Tiers 1 or 2 would suffice if the information could result in "severe mission capability degradation, major damage to DOD information based resource, or a risk of serious injury or death to personnel" [7]. Finally, on DOD networks, Tier 4 is only approved when the information "would have a low or moderate adverse impact on the efficacy of DOD missions or the reputation of the DOD if the information were compromised" [7].

B. FUTURE WORK

This thesis based its recommendations on one aspect of the authentication life cycle: use of pre-established (via enrollment or registration) authenticators to prove the claimed identity. Future research is needed to determine if these recommendations are still the most secure options when implementing other aspects of authentication, such as the registration—also known as enrollment—or (authenticator) recovery/revocation processes.

1. Concern with the Novelty of FIDO2

Currently, the security concerns with FIDO2 are few and far between, but there is an issue if the authentication device associated with the claimant is lost. The possibility of exploitation of a lost authentication device by a cyber actor is cause for concern. According to Steven Soneff, a product manager at Google, "The recovery mechanism is often the weakest link and where attackers will find their way in" [65].

PIV smart card security keys that support FIDO standards are a cause for concern as well. In the past there was a vulnerability in the firmware during RSA key generation which reduced, "the strength of keys generated immediately after power-up by up to 10 bytes for affected RSA keys" [66]. In this case, the vulnerability was discovered and addressed with a firmware update to inhibit the issues from becoming more widespread. Although chances of an attacker getting access to this information is slim, the vulnerability still remains and could prove to be very damaging.

Another cause for concern is the rivalry between Android and IOS devices. The compatibility issues each platform has with the other could lead to the exclusion of large

numbers of mobile devices to be used as an authenticator. This is slowing down the public distribution of FIDO2 to the masses. Apple continues to implement proprietary security measures within their own environment instead of leveraging well-known technologies like FIDO authentication standards [65].

2. Further Research to Shore Up Vulnerabilities that May Exist

FIDO2 is in its infancy, but just as with other security standards, there will be a concerted effort to exploit or break the protocol for nefarious means. Because of the backwards combability between FIDO2 and CTAP-1 (FIDO U2F), the possibility exists that any of the prior (weaker) generation's vulnerabilities could be exploited by attackers seeking to compromise the newer generation.

Although time consuming, investigative reverse engineering could reveal security vulnerabilities not previously found in these new protocols and standards. Vulnerabilities could exist in components used in initial releases that were discovered during product teardown, revealing attack vectors not previously seen by product developers.

All of these factors must be accounted for when developers are engineering products used to provide reliable security for the safeguarding of services promoting identity and information management. The challenge of mitigating "all" vulnerabilities persisting in authentication methods and products, and anything requiring connectivity to the internet will remain an issue that will require security professionals to evolve and pivot when emerging threats present themselves.

LIST OF REFERENCES

[1] Joint Task Force Transformation Initiative, “Security and Privacy Controls for Federal Information Systems and Organizations,” National Institute of Standards and Technology, NIST SP 800-53r4, Apr. 2013. Available. https://doi.10.6028/NIST.SP.800-53r4

[2] G. Bush, *Policies for a Common Identification Standard for Federal Employees and Contractors*, Homeland Security Presidential Directive-12. 2008.

[3] P. A. Grassi, M. E. Garcia, and J. L. Fenton, “Digital Identity Guidelines: Revision 3,” National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST SP 800-63-3, Jun. 2017. Available. https://doi.10.6028/NIST.SP.800-63-3.

[4] P. A. Grassi, J. L. Fenton, N. B. Lefkovitz, J. M. Danker, Y. Y. Choong, K. K. Greene, M. F. Theofanos, “Digital Identity Guidelines: Enrollment and Identity Proofing,” National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST SP 800-63A, Jun. 2017. Available. https://doi.10.6028/NIST.SP.800-63a.

[5] J. Fulp, “E-Authentication,” presented at the CS3690, Naval Postgraduate School, Feb. 11, 2020.

[6] P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y. Y. Choong, K. K. Greene, M. F. Theofanos, “Digital Identity Guidelines: Authentication and Life cycle Management,” National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST SP 800-63B, Jun. 2017. Available. https://doi.10.6028/NIST.SP.800-63b.

[7] Department of Defense, *Identity Authentication for Information Systems*, DoDI 8520.03. Jul. 27, 2017. Washington, DC, USA: Department of Defense.

[8] Department of Defense. *Cybersecurity.* DODI No. 8500.01. Mar 14, 2014. [Online]. Available: https://fas.org/irp/doddir/dod/i8500_01.pdf.

[9] D. L. Evans, *Federal Information Processing Standards Publication - Security Requirements for Cryptographic Modules*, FIPS 140-2. 25May2001. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

[10] Computer Security Division, Information Technology Laboratory, “Personal Identity Verification (PIV) of Federal Employees and Contractors,” National Institute of Standards and Technology, NIST FIPS 201-2, Aug. 2013. NIST.FIPS.201-2.

[11] D. Todorov, *Mechanics of User Identification and Authentication*. Boca Raton, FL, USA: Auerbach Publications, 2007.

[12] Department of Defense, *DOD Cybersecurity Discipline Implementation Plan*. Washington, DC, USA, 20160201.

[13] U.S. Government, "Introduction - PIV Guides. Accessed Mar. 1, 2020. [Online]. Available: piv.idmanagement.gov

[14] Department of Defense, *United States Department of Defense X.509 Certificate Policy*. Washington, DC, USA: Department of Defense, 20180520.

[15] Department of Defense, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, DoDI 8520.02. Washington, DC, USA: Department of Defense, 20110524.

[16] Department of Defense, "CAC Security." Accessed Mar. 1, 2020. [Online]. Available: https://www.cac.mil/Common-Access-Card/CAC-Security/

[17] Department of Defense, "Common Access Card (CAC)." Accessed Mar. 1, 2020. [Online]. Available: https://www.cac.mil/Common-Access-Card/

[18] Double Octopus, "What is Smart Card Authentication? | Security Wiki." Accessed Mar, 26, 2020. [Online]. Available: https://doubleoctopus.com/security-wiki/authentication/smart-card-authentication/

[19] IPWITHEASE, "What is PKI - Public Key Infrastructure."Accessed Mar. 1, 2020. [Online]. Available: https://ipwithease.com/what-is-pki-public-key-infrastructure/

[20] D. R. Kuhn, V. Hu, W. T. Polk, and S.-J. H. Chang, "Introduction to Public Key Technology and the Federal PKI Infrastructure," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST SP 800-32, 2001. https://doi.10.6028/NIST.SP.800-32.

[21] FIDO Alliance, "What is FIDO?," Accessed Feb. 24, 2020. [Online]. Available: https://fidoalliance.org/what-is-fido/

[22] A. Shikiar, "Authentication in the Age of GDPR," *Infosecurity Magazine*, Jul. 19, 2019. [Online]. Available: https://www.infosecurity-magazine.com:443/opinions/authentication-gdpr/

[23] FIDO Alliance, "FIDO Alliance Overview - Changing the Nature of Authentication," Accessed Feb. 24, 2020. [Online]. Available: https://fidoalliance.org/overview/

[24] FIDO Alliance, “Universal 2nd Factor (U2F) Overview.” [Online]. Available: https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.pdf.

[25] FIDO Alliance, “How FIDO Works - Standard Public Key Cryptography & User Privacy,” [Online]. Available: https://fidoalliance.org/how-fido-works/ (accessed Apr. 01, 2020).

[26] FIDO Alliance, “FIDO2: Web Authentication (WebAuthn),” [Online]. Available: https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/ (accessed Mar. 26, 2020).

[27] F. Reimair, C. Kollmann, and A. Marsalek, “Emulating U2F Authenticator Devices,” in *2016 IEEE Conference on Communications and Network Security (CNS)*, Oct. 2016, pp. 543-551, https://doi.10.1109/CNS.2016.7860546.

[28] FIDO Alliance, “Specifications Overview,” *FIDO Alliance*. [Online]. Available: https://fidoalliance.org/specifications/ (accessed Mar. 26, 2020).

[29] CardLogix, “Yubico Launches FIPS 140-2 Validated YubiKey Series | CardLogix,” *CardLogix Corporation*, Jun. 25, 2018. [Online]. Available: https://www.cardlogix.com/industry-news/yubico-launches-fips-140-2-validated-yubikey-smart-card-piv-dfars/.

[30] FIDO Alliance, “FIDO2: Moving the World Beyond Passwords using WebAuthn & CTAP,” [Online]. Available: https://fidoalliance.org/fido2/ (accessed Mar. 26, 2020).

[31] FIDO Alliance, “FIDO 2.0: Key Attestation Format.” Accessed: Mar. 27, 2020. [Online]. Available: https://fidoalliance.org/specs/fido-v2.0-ps-20150904/fido-key-attestation-v2.0-ps-20150904.html.

[32] W3C, “W3C and FIDO Alliance Finalize Web Standard for Secure, Passwordless Logins.” [Online]. Available: https://www.w3.org/2019/03/pressrelease-webauthn-rec.html.en (accessed Mar. 26, 2020).

[33] W3C, “World Wide Web Consortium (W3C).” [Online]. Available: https://www.w3.org/ (accessed Mar. 26, 2020).

[34] C. Brand and E. Kitamura, “Enabling Strong Authentication with WebAuthn,” Google Developers, 2019. [Online]. Available: https://developers.google.com/web/updates/2018/05/webauthn.

[35] Duo, “Web Authentication: What It Is and What It Means for Passwords,” [Online]. Available: https://duo.com/blog/web-authentication-what-it-is-and-what-it-means-for-passwords (accessed Apr. 09, 2020).

[36] FIDO Alliance, “FIDO UAF Architectural Overview.” Accessed: Mar. 26, 2020. [Online]. Available: https://fidoalliance.org/specs/fido-uaf-v1.1-ps-20170202/fido-uaf-overview-v1.1-ps-20170202.html.

[37] D. Neal, “An Illustrated Guide to OAuth and OpenID Connect,” Okta Developer. [Online]. Available: https://developer.okta.com/blog/2019/10/21/illustrated-guide-to-oauth-and-oidc (accessed Mar. 26, 2020).

[38] D. Hardt, “The OAuth 2.0 Authorization Framework.” [Online]. Available: https://tools.ietf.org/html/rfc6749 (accessed Mar. 26, 2020).

[39] OneLogin, “OpenID Connect Tutorial - OpenID Connect Flow & Specs - OIDC Examples - OIDC Server,” [Online]. Available: https://developers.onelogin.com/openid-connect (accessed Apr. 29, 2020).

[40] Office of the Secretary of Defense, *Modernizing the Common Access Card - Streamlining Identity and Improving Operational Interoperability*. Washington, DC, USA: Department of Defense, 2019.

[41] MARADMIN, “Modernizing the Common Access Card (CAC) - Streamlining Identity and Improving Operational Interoperability.” [Online]. Available: https://www.marines.mil/News/Messages/MARADMINS/Article/1729875/modernizing-the-common-access-card-cac-streamlining-identity-and-improving-oper/ (accessed Mar. 26, 2020).

[42] RSA, “50 Reasons RSA SecurID® Access is the Best Choice for Modern Authentication.” [Online]. Available: https://www.rsa.com/content/dam/en/white-paper/50-reasons-rsa-securid-access-is-the-best-choice-for-modern-authentication.pdf.

[43] CyberArk, “CyberArk Earns U.S. Department of Defense UC APL Certification,” [Online]. Available: https://www.cyberark.com/press/cyberark-earns-u-s-department-of-defense-uc-apl-certification/ (accessed Mar. 26, 2020).

[44] CyberArk, “Core Privileged Access Security.” [Online]. Available: https://lp.cyberark.com/rs/316-CZP-275/images/Core-Privileged-Access-Security-ds.pdf.

[45] CyberArk, “CyberArk Enterprise Security Services and Support Plans,” [Online]. Available: https://www.cyberark.com/services-support/professional-services/ (accessed Mar. 26, 2020).

[46] IDG Strategic Marketing Services and CyberArk, “Privileged Account Security Solutions: A Competitive Review.” IDG Strategic Marketing Services, CyberArk, Nov. 2017, [Online]. Available: https://www.cyberark.com/resource/privileged-account-security-solutions-competitive-review/.

[47] CyberArk, “The Cyberark Privileged Access Security Solution for U.S. Federal Government Agencies.” .

[48] Yubico, “YubiKey FIPS Series | FIPS 140-2 Validated Keys,” [Online]. Available: https://www.yubico.com/products/yubikey-fips/ (accessed Mar. 26, 2020).

[49] Y. Abousselham, “Okta Security Technical Whitepaper.” Okta, Apr. 02, 2018, [Online]. Available: https://www.okta.com/resources/whitepaper/okta-security-technical-white-paper/.

[50] Okta, “Okta for Government.” [Online]. Available: https://www.okta.com/resources/datasheet-okta-for-government/.

[51] FedRAMP, “About Us.” [Online]. Available: https://fedramp.gov/about/ (accessed Mar. 26, 2020).

[52] Okta, “Adaptive Multi-Factor Authentication - New Q2 FY19,” May 08, 2018. [Online]. Available: https://www.okta.com/products/adaptive-multi-factor-authentication/.

[53] Wikid. “Weighted Objectives .” Accessed Jun 12, 2020. [Online]. Available: http://wikid.io.tudelft.nl/WikID/index.php/Weighted_objectives_method (accessed Jun. 12, 2020).

[54] Department of Defense, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*. Washington, DC, USA: Department of Defense, 2017.

[55] Department of Defense, “About - DOD Cyber Exchange.” Accessed Apr. 25, 2020. [Online]. Available: https://public.cyber.mil/pki-pke/about/

[56] Office of the Chief of Naval Operations, *U.S. Navy Cybersecurity Program*, OPNAVINST 5239.1D. Washington, DC, USA, 2018.

[57] FIDO Alliance, “FIDO Alliance White Paper: Leveraging FIDO Standards to Extend the PKI Security Model in United States Government Agencies,” 2017. https://1nmqmp2u9dgf3jo9centu6rq-wpengine.netdna-ssl.com/wp-content/uploads/White-Paper-Leveraging-FIDO-Standards-to-Extend-the-PKI-Security-Model-in-US-Govt-Agencies.pdf

[58] FIDO Alliance, “NIST 800-63 Guidance & FIDO Authentication,” *FIDO Alliance*, Sep. 21, 2017. [Online]. Available: https://fidoalliance.org/nist-800-63-guidance-fido-authentication-2/

[59] FIDO Alliance, “U.S. General Services Administration’s Rollout of FIDO2 on login.gov.” Accessed Apr. 25, 2020. [Online]. Available: https://1nmqmp2u9dgf3jo9centu6rq-wpengine.netdna-ssl.com/wp-content/uploads/2020/03/Fido-US-GSA-2020-1.pdf

[60] C. Corum, “Merging FIDO and PIV Could Help Feds Achieve Strong Authentication Goals,” SecureIDNews, Mar. 17, 2017. [Online]. Available: https://www.secureidnews.com/news-item/merging-fido-and-piv-could-help-feds-achieve-strong-authentication-goals/

[61] S. Rosenblatt, “Two-Factor Authentication: What You Need to Know (FAQ),” CNET. Accessed Apr. 22, 2020. [Online]. Available: https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq

[62] B. Schneier, “Chinese Hackers Bypassing Two-Factor Authentication,” Schneier on Security. Accessed Apr. 22, 2020. [Online]. Available: https://www.schneier.com/blog/archives/2019/12/chinese_hackers_1.html

[63] E. Mills, “RSA: Cyberattack Could Put Customers at Risk.” Accessed Apr. 22, 2020. [Online]. Available: https://www.cnet.com/news/rsa-cyberattack-could-put-customers-at-risk/

[64] W3C, “W3C Mission.” Accessed May 5, 2020. [Online]. Available: https://www.w3.org/Consortium/mission

[65] J. Porter, “When Can We Finally Get Rid of Passwords?,” *The Verge*, Apr. 24, 2019. [Online]. Available: https://www.theverge.com/2019/4/24/18514225/passwords-fido2-authentication-webauthn-security-key-cybersecurity-online-browser-web

[66] Yubico, “Security Advisory 2019-06-13 - Reduced Initial Randomness on FIPS Keys,” *Yubico*, Jun. 13, 2019. [Online]. Available: https://www.yubico.com/support/security-advisories/ysa-2019-02/

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California