NIST SPECIAL PUBLICATION 1800-17B

Multifactor Authentication for E-Commerce

Risk-Based, FIDO Universal Second Factor Implementations for Purchasers

Volume B:
Approach, Architecture, and Security Characteristics

William Newhouse
Information Technology Laboratory
National Institute of Standards and Technology

Brian Johnson
Sarah Kinling
Jason Kuruvilla
Blaine Mulugeta
Kenneth Sandlin
The MITRE Corporation
McLean, Virginia

July 2019

This publication is available free of charge from https://doi.org/10.6028/NIST.SP.1800-17

The first draft of this publication is available free of charge from
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/cr-mfa-nist-sp1800-17.pdf

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

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-17B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-17B, 52 pages, (July 2019), CODEN: NSPUE2

FEEDBACK

As a public-private partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at consumer-nccoe@nist.gov.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

As retailers in the United States have adopted chip-and-signature and chip-and-PIN (personal identification number) point-of-sale (POS) security measures, there have been increases in fraudulent online card-not-present electronic commerce (e-commerce) transactions. The risk of increased fraudulent online shopping became more widely known following the adoption of chip-and-PIN technology that increased security at the POS in Europe.

The NCCoE at NIST built a laboratory environment to explore methods to implement multifactor authentication (MFA) for online retail environments for the consumer and the e-commerce platform administrator. The NCCoE also implemented logging and reporting to display authentication-related system activity.

This NIST Cybersecurity Practice Guide demonstrates to online retailers that it is possible to implement open standards-based technologies to enable Universal Second Factor (U2F) authentication at the time of purchase when risk thresholds are exceeded.

The example implementations outlined in this guide encourage online retailers to adopt effective MFA implementations by using standard components and custom applications that are composed of open-source and commercially available components.

KEYWORDS

electronic commerce (e-commerce) security; internet shopping security; multifactor authentication (MFA)

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Greg Dicovitsky	RSA
Leonardo Andrade	RSA
Adam Cohn	Splunk
Arshad Noor	StrongKey
Kamil Kreiser	TokenOne
Derek Hanson	Yubico
David Coley	Dominion Tea
Brian Abe	The MITRE Corporation
Lorrayne Auld	The MITRE Corporation
Lura Danley	The MITRE Corporation

Name	Organization
Sallie Edwards	The MITRE Corporation
Charles Jones, Jr.	The MITRE Corporation
Joshua Klosterman	The MITRE Corporation
Jay Vora	The MITRE Corporation
Mary Yang	The MITRE Corporation

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build these example implementations. We worked with:

Technology Partner/Collaborator	Build Involvement
RSA	RSA Adaptive Authentication (Cloud) Version 13.1
Splunk	• Splunk Enterprise Version 6.6.1 • Splunk DB Connect Version 3.1.2 • Splunk Universal Forwarder Version 7.0.1
StrongKey	• StrongKey CryptoEngine Version 2.0 Open Source Fast IDentity Online (FIDO) U2F server • MagentoFIDO (magfido) 1st Edition Module
TokenOne	TokenOne cloud-based Authentication Version 2.8.5
Yubico	Yubico YubiKey NEO Security Key

Contents

List of Figures

List of Tables

1 Summary

Smart chip credit cards and terminals work together to protect in-store payments. The in-store security advances were introduced in 2015 [1], and those have pushed malicious actors who possess stolen credit card data to perform payment card fraud online. This guide describes implementing stronger user-authentication techniques to reduce the risk of electronic commerce (e-commerce) fraud. The guide documents a system in which risk determines when to trigger multifactor authentication (MFA) challenges to existing customers.

1.1 Challenge

Volume A of this publication described why the National Cybersecurity Center of Excellence (NCCoE) took on a retail cybersecurity challenge as a project. Here in Volume B, we shift to the challenge of building two example implementations that show online retailers some options to deploy strong authentication solutions that use open and scalable standards offering enhanced authentication security. Such modern authentication systems support the following security characteristics [2]:

- a foundation built on public key cryptography
- protection from authentication replay attacks
- options for determining when MFA should be requested
- auditing and system activity logging and display

To build the example implementations, the project collaborators reached consensus on architectures that demonstrate standards-based authentication solutions. We chose to enable the use of MFA by adding a distinct second authentication factor, recognizing that doing so can help lower the online retailer's exposure to fraudulent purchases by increasing the likelihood that the purchaser who is offering the second authentication factor is a legitimate returning customer. Continuing the focus on enhanced authentication provided an incentive for the architecture to address how system owners and administrators could use MFA when performing e-commerce platform administration activities. Additionally, situational awareness dashboards were created to visually demonstrate e-commerce authentication activity.

1.2 Implementations

The modern authentication security characteristic goals and the capabilities of the collaborators matched the open and scalable standards of the Fast IDentity Online (FIDO) Alliance [3], [4]. This project demonstrates how to prompt online purchasers to provide a second authentication factor—something they have—when risk thresholds are exceeded during an online shopping session.

The returning purchaser in our example implementations is an online shopper who has established login account credentials and has registered for MFA with a retailer. The example implementations describe and document architectures to enable a returning purchaser to complete a purchase when risk thresholds are exceeded during the transaction. The second authentication factor for returning purchasers in these example implementations is a FIDO Universal Second Factor (U2F) authenticator [3], [4]. The purchaser's U2F authenticator is unique, known to the retailer, and possessed only by the returning purchaser. The U2F used in the example implementations is a FIDO Certified product, compliant with the FIDO U2F specifications [5].

In the NCCoE example implementations, U2F authentication challenges are triggered when the total cost of the shopping-cart transaction exceeds predefined retailer thresholds. The two example implementations are referred to as the *cost threshold* and *risk engine* example implementations.

The *cost threshold* example implementation requests additional authentication when a dollar amount is exceeded. Because fraudulent activity may still occur in purchases below this threshold, the *risk engine* example implementation can examine many system and external elements related to a shopping session. In this example implementation, a shopping-cart-amount threshold input trigger was chosen to demonstrate that the *risk engine* can communicate the need for a second authentication factor. Additionally, returning-purchaser account-lockout techniques are demonstrated that can limit credential stuffing and takeovers of customer accounts.

In both the *cost threshold* and *risk engine* example implementations, MFA of the retailer's e-commerce platform system administrator is also included with onetime pad authentication principles. This increases the security of the overall system by prompting the system administrators to use their non-short message service, smartphone-based MFA capability before making changes to the e-commerce platform.

Both the returning purchaser and system administrator MFA capabilities require action to be taken by the user to prove the user's possession of an authentication factor that only the legitimate user should possess. The returning purchaser is asked to confirm their presence by pressing a contact on a registered U2F device, and the administrator is prompted to enter a code provided from a unique mobile-device application as part of the authentication process.

The example implementations also describe and document situational awareness within the overall system that tracks the important processes, including logging system functions such as authentication activity, and providing dashboard displays of this information [6] for system owners.

1.2.1 Standards and Guidance

In developing our example implementations, we were influenced by standards and guidance from the following sources, which can also provide an organization with relevant standards and best practices:

- FIDO U2F authentication specification [3], [4]

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2013, *Information Technology—Security Techniques—Information Security Management Systems—Requirements* [7]
- National Institute of Standards and Technology (NIST) Cybersecurity Framework [8]
- NIST Special Publication (SP) 800-30 Revision 1, *Guide for Conducting Risk Assessments* [9]
- NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* [10]
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* [11]
- NIST SP 800-63-3, *Digital Identity Guidelines* [12]
- NIST SP 800-63A, *Digital Identity Guidelines, Enrollment and Identity Proofing* [13]
- NIST SP 800-63B, *Digital Identity Guidelines, Authentication and Lifecycle Management* [14]
- NIST SP 800-63C, *Digital Identity Guidelines, Federation and Assertions* [15]
- NIST SP 800-73-4, *Interfaces for Personal Identity Verification* (3 Parts) [16]
- NIST SP 800-160 Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [17]
- NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [18]
- Payment Card Industry (PCI) Data Security Standard, *Requirements and Security Assessment Procedures*, Version 3.2, April 2016, PCI Security Standards Council [19]
- Identity Ecosystem Steering Group (IDESG) [20]

1.3 Benefits

The NCCoE's practice guide for *Multifactor Authentication for E-Commerce* can help your organization:

- increase the level of security and assurance for card-not-present (CNP) e-commerce transactions
- reduce the risk of account takeovers and fraudulent CNP e-commerce transactions
- reduce the risk of system-administrator-account security breaches
- understand and implement several different MFA-related capabilities
- automate processes to mitigate risks
- recognize potential fraud identifiers, and visually display them on dashboards to identify trends
- implement industry-standard security controls
- increase consumer confidence

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates two standards-based reference designs and provides users with the information they need to replicate the MFA for e-commerce example implementations. These reference designs are modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-17A: *Executive Summary*
- NIST SP 1800-17B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-17C: *How-To Guides* – instructions for building the example implementations

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-17A*, which describes the following topics:

- challenges that enterprises face in implementing MFA to reduce online fraud
- example implementations built at the NCCoE
- benefits of adopting the example implementations

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-17B,* which describes what we did and why. The following sections will be of interest:

- Section 3.4, Risk Assessment, provides a description of the risk analysis we performed
- Section 3.4.4, Security Control Map, maps the security characteristics of these example implementations to cybersecurity standards and best practices

You might share the *Executive Summary, NIST SP 1800-17A*, with your leadership team members to help them understand the importance of adopting standards-based solutions when implementing MFA, increasing the assurance about who is using the purchaser's credit card and account information.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-17C*, to replicate all or parts of the builds created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for installing and configuring the example implementations. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create these example implementations.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt these example implementations or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of these e-commerce security enhancing capabilities. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.5, Technologies, lists the products we used and maps them to the cybersecurity controls provided by these reference implementations. For additional information regarding cybersecurity control mappings, see Appendix A for the Cybersecurity Framework Components Mapping table (Table A-1).

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For detailed definitions of terms, see the *NCCoE Glossary.*
Bold	names of menus, options, command buttons, and fields	Choose **File > Edit.**
`Monospace`	command-line input, onscreen computer output, sample code examples, status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

3 Approach

This practice guide highlights the approach used to develop the NCCoE example implementations. Our approach includes risk assessment and analysis; logical design; example build development, test, and evaluation; and security control mapping. This guide is intended to provide practical guidance to retailers interested in implementing an MFA solution to reduce e-commerce fraud.

In developing the example implementations, the NCCoE:

- worked with retail organizations and other e-commerce payment stakeholders, including the Retail and Hospitality Information Sharing and Analysis Center [21], to identify the potential need and benefits of MFA for e-commerce. The need came from recognizing that malicious actors are increasingly targeting CNP online retail transactions in response to the adoption of chip credit cards in the U.S.
- participated in workshops to identify key issues that affect MFA for e-commerce. The conversations and the insight derived from those workshops have informed the direction of this project and this practice guide
- regularly interacted with members of the NCCoE Retail Community of Interest (COI) to discuss current cybersecurity trends and online retail needs
- received input from the participating technology vendors referenced in this guide who contributed to developing the architecture and reference design. They provided technologies to address the project's requirements and assisted in installing and configuring those technologies in an architecture design that reflected their customer's online retail environments

3.1 Audience

This guide is intended for individuals responsible for implementing IT security solutions and for individuals involved in reducing fraudulent purchases on retail shopping websites. The platforms demonstrated by this project, and the implementation information provided in this practice guide, permit the integration of products to implement MFA for an e-commerce system. While the example implementations' primary audience is those who support online e-commerce retailers, the capabilities may appeal to the broader audience of administrators, IT managers, IT security managers, risk-mitigation personnel, and others involved in the security of managing registered users for an organization's internet resources.

3.2 Scope

The project focuses on the need for MFA during e-commerce transactions with increased risk, and during system administration activities. The NCCoE drafted desired security solution characteristics that would be used by an online retailer. After an open call in the Federal Register for vendors to help develop a solution, we scoped the project to create the following high-level architectural elements and desired outcomes:

- provide consumers with an open standards-based MFA capability based upon FIDO
- provide a solution leveraging Universal Serial Bus (USB) Type A hardware multifactor devices used with desktop/laptop personal-computer form factors for returning purchasers
- demonstrate a system where MFA is required by e-commerce platform administration personnel before they perform system administration activities. Implementing MFA for administrative accounts can help limit the risk of compromising the information system that hosts the e-commerce solution
- demonstrate MFA device registration
- show protections to help mitigate password-guessing account takeover and credential stuffing scenarios by using account lockout protections after a certain number of incorrect logins are attempted
- enable system-activity situational awareness by providing dashboards that display account lockout and authentication activity

To maintain the project's focus on e-commerce MFA, the following areas are **out of scope** for these example implementations:

- purchasers who check out as guests, returning purchasers who do not possess U2F authenticators, and purchasers leveraging a mobile application to shop online
- MFA device registration security and lost token replacement that would help secure the device registration workflow (recommendations are provided in Section 5.3 regarding registration workflows that organizations may use)
- customer interaction and help-desk-related functions, such as the distribution and procurement of U2F authenticators, identity proofing, or account creation of the customer identification (ID), as well as recovery processes if the account becomes locked out

While the areas noted above can be important to implementing an MFA system, they were not included in the example implementations' design decisions. Additional system architectural elements, such as the separation of functionality and components, high availability, network or application firewalls, and intrusion detection/prevention capabilities, were out of scope for our builds.

3.3 Assumptions

Organizations should review the assumptions underlying the example builds before implementing the capabilities described in this practice guide. Before implementing these capabilities, organizations should consider whether the same assumptions apply to their environment. Appendix B provides implementation guidance for the following assumptions:

- availability of skills
- uniqueness of lab environment
- MFA decreases account takeover opportunities
- web browser (not mobile application) and returning purchaser accounts
- support of MFA devices
- customer-support mechanisms for lost tokens

Additionally, the scenarios associated with the example implementations assume that the returning purchaser has already completed these actions:

- registered their multifactor authenticator
- logged into the retailer e-commerce platform's website
- shopped and filled their shopping cart

3.4 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*—material that is available to the public. The Risk Management Framework (RMF) guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

3.4.1 Threats

A threat is "an event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss" [17]. The following subsections describe the authentication-based threats to e-commerce retail environments that were considered when developing this practice guide.

3.4.1.1 Credential Stuffing

Credential stuffing is a type of brute-force attack [22]. In credential stuffing, large-scale account username and password theft is used against online retailers. Common scenarios include stealing accounts from a different website, and then a credential stuffing capability tests the logins to find accounts that have identical customer IDs and passwords on both the website from which the account credentials were stolen and the website that is being targeted for theft.

An outcome or result of credential stuffing can be account takeover. A 2017 study reported that credential stuffing attacks accounted for “more than 90% of login traffic on many of the world’s largest websites and mobile applications” [23]. The accounts that have been compromised in credential stuffing attacks are then used in account takeover scenarios like those described below.

3.4.1.2 Account Takeover

In account takeover scenarios, where account theft and reuse occur, compromised or captured e-commerce customer accounts can be used for fraudulent purchases, gift card purchase and redemption, or customer loyalty program misappropriation.

Account takeover of e-commerce platform system administrator accounts can lead to the information system, and the data contained in it, being compromised.

3.4.2 Vulnerabilities

A vulnerability is a “weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat” [17]. Authentication-based vulnerabilities for e-commerce retail environments include the characteristics listed below.

Systems with these characteristics are especially susceptible to credential stuffing:

- allow multiple incorrect logins without account lockouts
- purchasers have reused the same password on multiple systems

Systems with these characteristics are especially susceptible to account takeover:

- accept weak passwords
- allow multiple incorrect logins without account lockouts
- account password-reset options are easily circumvented

3.4.3 Risk

Risks include the fraudulent use of account customer IDs and passwords to perform e-commerce fraud. This fraud impacts the e-commerce ecosystem by decreasing purchaser confidence in the security of their payment and account information and by increasing costs to offset the e-commerce fraud.

Additionally, through the potential compromise of administrative accounts, risk exists to the data contained within the e-commerce information-system infrastructure. Implementing MFA for these accounts can limit risk exposure in this area.

3.4.4 Security Control Map

The NIST Cybersecurity Framework security Functions and Subcategories that the reference designs support were identified through a risk analysis process. Additionally, work roles in the NICE Cybersecurity Workforce Framework [18] that perform the tasks necessary to implement those cybersecurity Functions and Subcategories were identified. See Appendix A for the Cybersecurity Framework Components Mapping table (Table A-1).

3.5 Technologies

Table 3-1 lists all of the technologies used in this project and provides a mapping among the generic product component term, the specific product used, the function of the product, and the NIST Cybersecurity Framework Subcategory outcomes that the product provides for the example implementations. Refer to Table A-1 for an explanation of the NIST Cybersecurity Framework Subcategory codes, a mapping to ISO/IEC 27001:2013 [7], NIST SP 800-53 Revision 4 controls [11], and NIST SP 800-181 [18] work roles. Many of the products have additional capabilities that were not used for the purposes of the example implementation builds.

Table 3-1 Products and Technologies

Component	Specific Product	Function	Cybersecurity Framework Subcategories
Retailer E-Commerce Platform	Magento Open Source Version 2.1.8 [24]	The landing point for the returning purchaser as they shop in the online store. The retailer e-commerce platform serves as the interaction point for the returning purchaser's e-commerce transaction. The retailer e-commerce platform also serves as the communication point between the returning purchaser and the back-office services that the website interacts with to obtain authentication, inventory information, etc.	**PR.AC-1, PR.AC-7, RS.AN-1**

Component	Specific Product	Function	Cybersecurity Framework Subcategories
U2F/Risk Assessment Module	magfido risk assessment policy rules and process module [25]	Provides purchaser account U2F registration and authentication capabilities, assesses information about the purchase and the returning purchaser's profile, and determines if MFA is required from the purchaser to complete shopping-cart checkout. These policies and processes are accomplished by Magento and StrongKey CryptoEngine (SKCE) Version 2.0 Open Source FIDO U2F server interaction [26].	**ID.RA-4, ID.RA-5**
Risk Engine	RSA Adaptive Authentication (Cloud) Version 13.1 [27]	Uses data science to provide transaction analysis and response, prompting the returning purchaser to use U2F when the organization's risk threshold is exceeded during a transaction, providing a low-friction experience for the consumer to reduce fraud while minimizing the interruptions and denials that a consumer may encounter.	**ID.RA-4, ID.RA-5**
MFA Mechanism	SKCE Version 2.0 Open Source FIDO U2F server [26] and TokenOne cloud-based Authentication Version 2.8.5 [28]	Provides a server-based enhanced-authentication capability as required by the risk assessment module (magfido) or for the e-commerce platform administrator (TokenOne).	**PR.AC-1, PR.AC-7**

Component	Specific Product	Function	Cybersecurity Framework Subcategories
Multifactor Authenticator	Yubico YubiKey NEO Security Key USB Type A ports and near-field communication device [29]; TokenOne smartphone application authenticator [28]	MFA device that the purchaser possesses and presents when requested (Yubico) or that the e-commerce administrator uses (TokenOne).	**PR.AC-1, PR.AC-7**
Logging/Reporting Dashboard	Splunk Enterprise Version 6.6.1 [6]	Provides logging and reporting data for use by MFA for e-commerce system owners.	**DE.CM-1**

3.6 NIST SP 800-63-3 Alignment

NIST SP 800-63-3, *Digital Identity Guidelines* [12], identifies three components of digital identity:

- Identity Assurance Level (IAL), which discusses the identity proofing process
- Authenticator Assurance Level (AAL), which discusses the authentication process
- Federation Assurance Level (FAL), which discusses the strength of an assertion in a federated environment

The example implementations presented in this guide align with NIST SP 800-63-3 assurance concepts in the following ways:

- IAL: demonstrates a returning purchaser's self-asserted identity. For the e-commerce platform administrator's use of MFA, the identity levels will depend upon organizational requirements and processes (reference Section 2.2 in NIST SP 800-63A, *Digital Identity Guidelines*, *Enrollment and Identity Proofing* [13]).
- AAL: demonstrates a single-factor cryptographic device used by the returning purchaser in conjunction with memorized secret (reference Sections 4.2.1, 5.1.1, and 5.1.7 in NIST SP 800-63B, *Digital Identity Guidelines*, *Authentication and Lifecycle Management* [14])
- FAL: Federated identity is not part of the example implementations. However, federation concepts can be further explored in NIST SP 800-63C, *Digital Identity Guidelines*, *Federation and Assertions* [15].

4 Architecture

The NCCoE worked with project collaborators to develop two open, standards-based, commercially available example implementations demonstrating the following capabilities:

- MFA for e-commerce returning purchasers who use FIDO U2F
- MFA for administrators of the e-commerce system who use onetime pad principles
- *cost threshold*- or *risk engine*-initiated MFA request
- authentication log aggregation and display

While these capabilities are implemented as integrated example implementations in this guide, subsets of these capabilities could be deployed as organizational requirements may dictate. The modular design of the two example implementations is made to support such use cases.

The two example implementations include online e-commerce platform capabilities, risk assessment and MFA, and logging and display capabilities. The high-level reference architectures shown in Figure 4-1 and Figure 4-2 illustrate the two example implementations that are also known as the *cost threshold* and *risk engine* example implementations, respectively.

The example implementations were constructed on the NCCoE's VMware vSphere virtualization operating environment. Internet access was used to connect to remote cloud-based components, while software components were installed as virtual servers within the vSphere environment.

4.1 Architecture Description

The architecture that was used to create the example implementations is described in this section. The example implementations were designed and built in the NCCoE lab environment. The lab network is not connected to the NIST enterprise network. Table 3-1 lists the MFA software and hardware components used, as well as the specific function of each component. Hardware components, such as the U2F, were used with laptops.

4.1.1 MFA for E-Commerce Returning Purchasers Who Use FIDO U2F

The example implementations demonstrated MFA by using FIDO protocols for the returning purchasers. The retailer e-commerce platform was built on Magento. StrongKey, a technology collaborator in this project, created a Magento module, magfido, to support the FIDO U2F protocol to enable strong authentication.

FIDO protocols have been designed to provide strong authentication by using a challenge-response-based protocol with strong cryptographic keys and algorithms. FIDO U2F authenticators in the example implementations are hardware-based devices on which cryptographic keys are generated and used. FIDO protocols include a test-of-human-presence requirement to confirm that a real human is in possession of the U2F. The U2F was used in the USB Type A port of a laptop that used a current version of a graphical user interface operating system that did not require additional software drivers to be installed.

4.1.2 Cost Threshold- or Risk Engine-Initiated MFA Request

In both example implementations, the FIDO capability is supported by StrongKey's SKCE FIDO Server, which is integrated with the Magento e-commerce platform and Yubico's YubiKey NEO Security Key. Magento allows extension of its base code through modules. In the first example implementation, also known as the *cost threshold* example implementation, the magfido risk assessment module is used to override Magento's default checkout process to require FIDO-based strong authentication on purchases that exceed $25—the dollar threshold used to simulate a riskier transaction.

In the second example implementation, also known as the *risk engine* example implementation, the RSA Adaptive Authentication product provides risk engine analysis capabilities that can interact with the example implementation's Magento web server and that leverage the magfido module to require FIDO-based authentication from the returning purchaser.

4.1.3 MFA for E-Commerce System Administrators Using Onetime Pad Principles

TokenOne's authentication capability authenticates the Magento e-commerce platform administrator before any administrative modifications are made to the e-commerce platform. It is based upon TokenOne's cloud-based authentication infrastructure and a smartphone application on either an Android or iPhone device. This helps secure the e-commerce organization's overall infrastructure.

4.1.4 Authentication Log Aggregation and Display

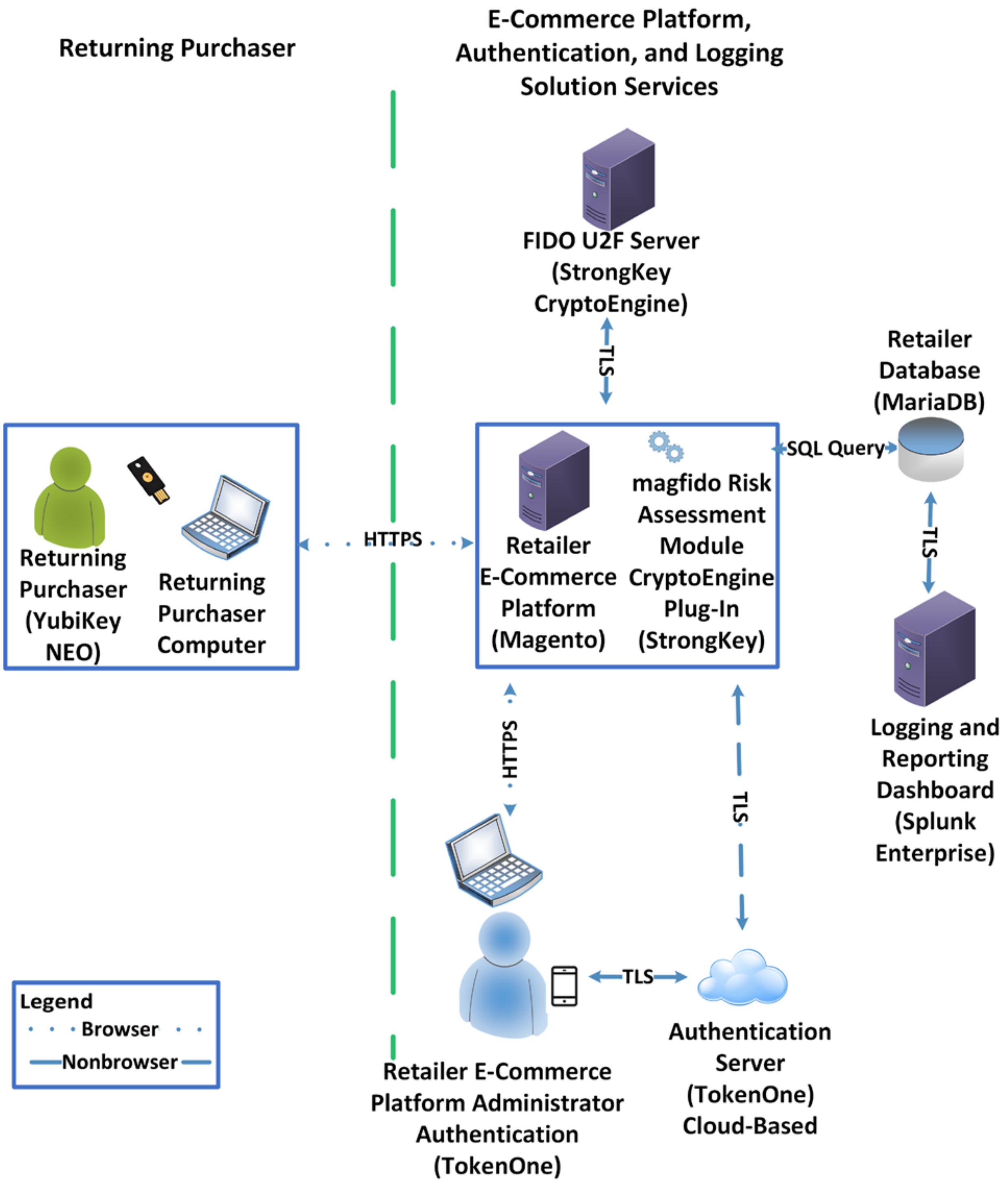
Splunk Enterprise provides authentication-related logging and dashboard capabilities.

4.2 Cost Threshold Architecture Details

The *cost threshold* example implementation is described in this section, and the *risk engine* example implementation is described in Section 4.3. The *cost threshold* architecture depicted in Figure 4-1 includes the following elements:

- returning purchaser
- retailer e-commerce platform
- magfido risk assessment module
- FIDO U2F server
- e-commerce platform administrator authentication
- logging and reporting dashboard

Figure 4-1 High-Level Cost Threshold Reference Architecture


Returning Purchaser
E-Commerce Platform, Authentication, and Logging Solution Services
FIDO U2F Server (StrongKey CryptoEngine)
TLS
Retailer Database (MariaDB)
SQL Query
Returning Purchaser (YubiKey NEO)
Returning Purchaser Computer
HTTPS
Retailer E-Commerce Platform (Magento)
magfido Risk Assessment Module CryptoEngine Plug-In (StrongKey)
TLS
Logging and Reporting Dashboard (Splunk Enterprise)
HTTPS
TLS
TLS
Legend
Browser
Nonbrowser
Retailer E-Commerce Platform Administrator Authentication (TokenOne)
Authentication Server (TokenOne) Cloud-Based

The high-level *cost threshold* architecture components are described in the following subsections.

4.2.1 Returning Purchaser

The returning purchaser initiates an e-commerce purchase from their returning-purchaser computer, logging in with their customer ID and password to complete the purchase. The returning purchaser can present their U2F authenticator, if requested by the e-commerce retailer, when the risk threshold has been exceeded. The user's U2F authenticator leveraged in the example implementations is the Yubico YubiKey NEO Security Key [29].

4.2.2 Retailer E-Commerce Platform

The returning purchaser uses a FIDO-supported web browser for accessing the retailer e-commerce platform. The retailer e-commerce platform allows the returning purchaser to browse the retailer's products and services. The e-commerce platform provides the returning purchaser with the ability to select items for eventual purchase and to check out to complete the purchase. The checkout process includes authentication requests presented to the purchaser. The information conveyed to the returning purchaser is provided by or through the retailer e-commerce platform's website.

The retailer e-commerce platform serves as a conduit with the back-office components of the e-commerce retailer's information systems, such as product inventory, shopping-cart information, customer identity management, authentication information, as well as the retailer database.

The specific product that we leveraged in our example implementations for the retailer e-commerce platform is an open-source version of Magento [24] that integrates with third-party modules like the magfido module developed for the example implementations and described in this guide.

4.2.3 magfido Risk Assessment Module

The magfido risk assessment module identifies when a risk threshold has been exceeded and then requires the purchaser to provide their U2F authenticator to complete a purchase. It also allows a returning purchaser to register the U2F authenticator needed when the risk threshold has been exceeded. The magfido risk assessment module was developed by StrongKey and is publicly available [25]. The magfido module is explained in greater detail in Section 2.3 of Volume C of this guide.

4.2.4 FIDO U2F Server

The FIDO U2F server provides server-based enhanced authentication capabilities. SKCE Version 2.0 performs cryptographic functions through web services and, among other capabilities, includes a FIDO engine to support FIDO U2F authenticator registration and authentication [30].

4.2.5 Retailer E-Commerce Platform Administrator Authentication

In our example implementations, MFA is required to perform management functions on the retailer e-commerce platform. This MFA capability is provided by TokenOne's cloud-based and smartphone-based application [28]. Implementing this feature is consistent with PCI Data Security Standards 3.2, Requirement 8.3 [31].

4.2.6 Logging and Reporting Dashboard Server

The logging and reporting dashboard aggregates log data from the different components in the e-commerce system. It then provides the system operator with a visual display of the authentication events. The product leveraged for the example implementations is Splunk Enterprise [6].

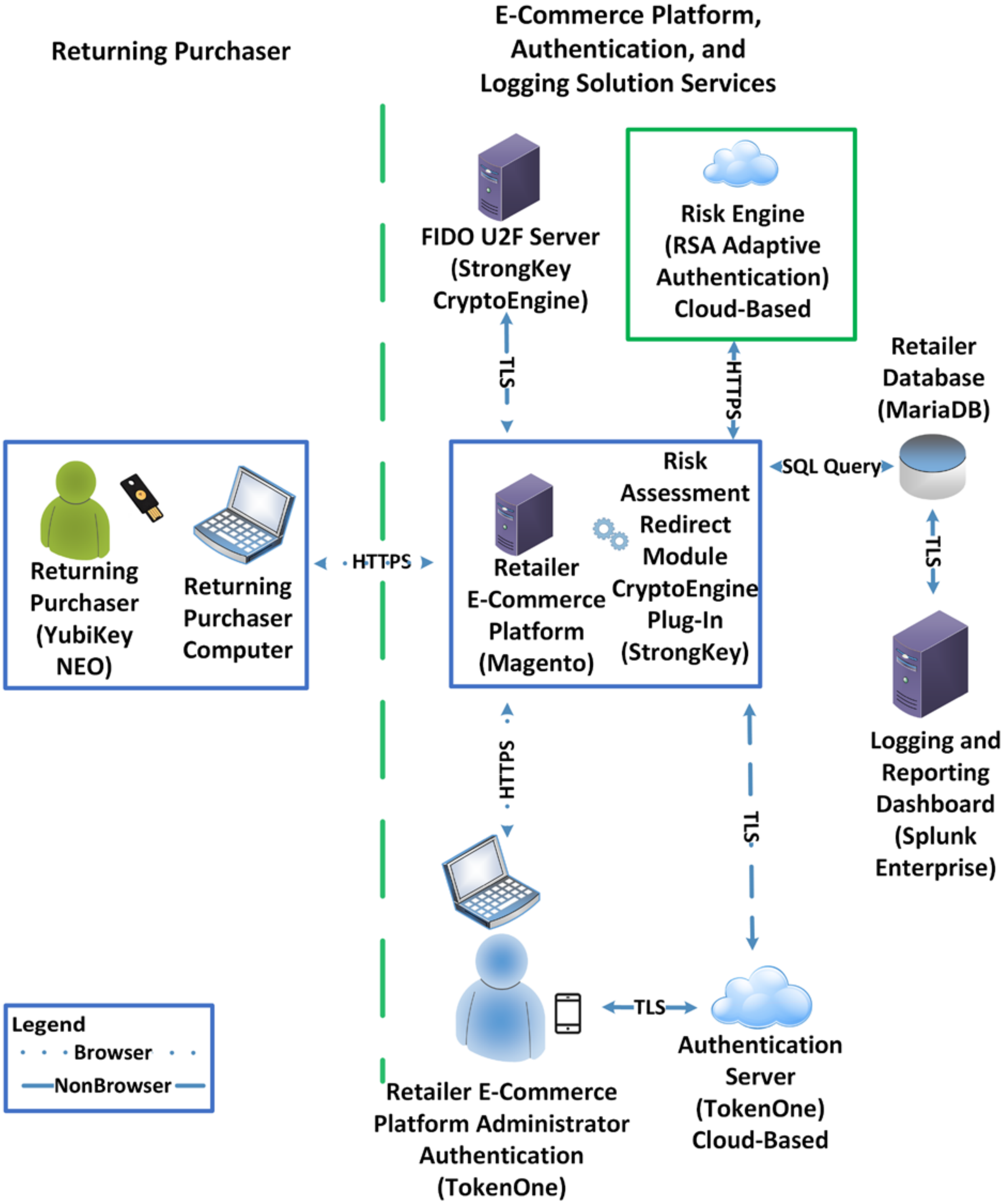
4.3 Risk Engine Architecture Details

The *risk engine* architecture depicted in Figure 4-2 includes the following elements:

- returning purchaser
- retailer e-commerce platform
- risk assessment redirect module
- adaptive authentication capability
- FIDO U2F server
- e-commerce platform administrator authentication
- logging and reporting dashboard

The *risk engine* architecture depicted in Figure 4-2 leverages the magfido module, replacing the *cost threshold* capability with the RSA Adaptive Authentication Risk Engine displayed in the figure's green box. This example implementation build focuses on risk engine-based MFA capabilities. This uses an analytic engine to leverage additional capabilities for detecting increased risks. The RSA Adaptive Authentication Risk Engine examines details of the transaction and requires the returning purchaser to use MFA only when the transaction is deemed to be higher risk.

Figure 4-2 High-Level Risk Engine Reference Architecture


Returning Purchaser
E-Commerce Platform, Authentication, and Logging Solution Services
FIDO U2F Server (StrongKey CryptoEngine)
Risk Engine (RSA Adaptive Authentication) Cloud-Based
TLS
HTTPS
Retailer Database (MariaDB)
SQL Query
TLS
Returning Purchaser (YubiKey NEO)
Returning Purchaser Computer
HTTPS
Retailer E-Commerce Platform (Magento)
Risk Assessment Redirect Module CryptoEngine Plug-In (StrongKey)
Logging and Reporting Dashboard (Splunk Enterprise)
HTTPS
TLS
TLS
Authentication Server (TokenOne) Cloud-Based
Retailer E-Commerce Platform Administrator Authentication (TokenOne)
Legend
Browser
NonBrowser

4.3.1 Risk Engine

In addition to the components described in Section 4.2, the *risk engine* example implementation modifies the magfido module to add an additional capability by using the RSA Adaptive Authentication Risk Engine highlighted in the green box in Figure 4-2 [27]. The risk engine leverages machine learning and risk-based authentication, and the example implementation will prompt users for FIDO-based authentication only when the risk engine deems the transaction to be higher risk.

For this purpose, we refer to the updated magfido module as the risk assessment redirect module.

In our example implementation, the risk engine suspends the transactions when it identifies the transaction as exceeding risk thresholds. Leveraging machine learning, the risk engine computes a score that focuses on each consumer's normal activity, the activity of the merchant's population, and global fraudulent device metrics (an outside service contributes the latter). In an online retail setting, the system would prompt the consumer to contact customer service for assistance in completing the transaction, a possible scenario where the risk engine would intercede.

4.3.2 Risk Assessment Redirect Module

The risk assessment redirect module is hosted by the Magento server and provides risk and authentication analysis information related to the returning purchaser's shopping-transaction activities to the risk engine. Risk engine decisions are then communicated back to the Magento server through the risk assessment redirect module.

Based upon an analysis performed by the risk engine, the risk assessment redirect module then directs the Magento server to allow the returning purchaser to use their customer ID and password for lower-risk transactions, and then requires the returning purchaser to also successfully present their FIDO U2F authenticator to complete their shopping transaction.

Optionally at the retailer's discretion, and with additional programming of the risk assessment redirect module, the transaction can be suspended when the risk engine identifies the transaction as exceeding particular risk thresholds.

4.4 Process Flows

The following process flows show the sequence of events taking place as a returning purchaser completes an online purchase by using the *cost threshold* or *risk engine* example implementation.

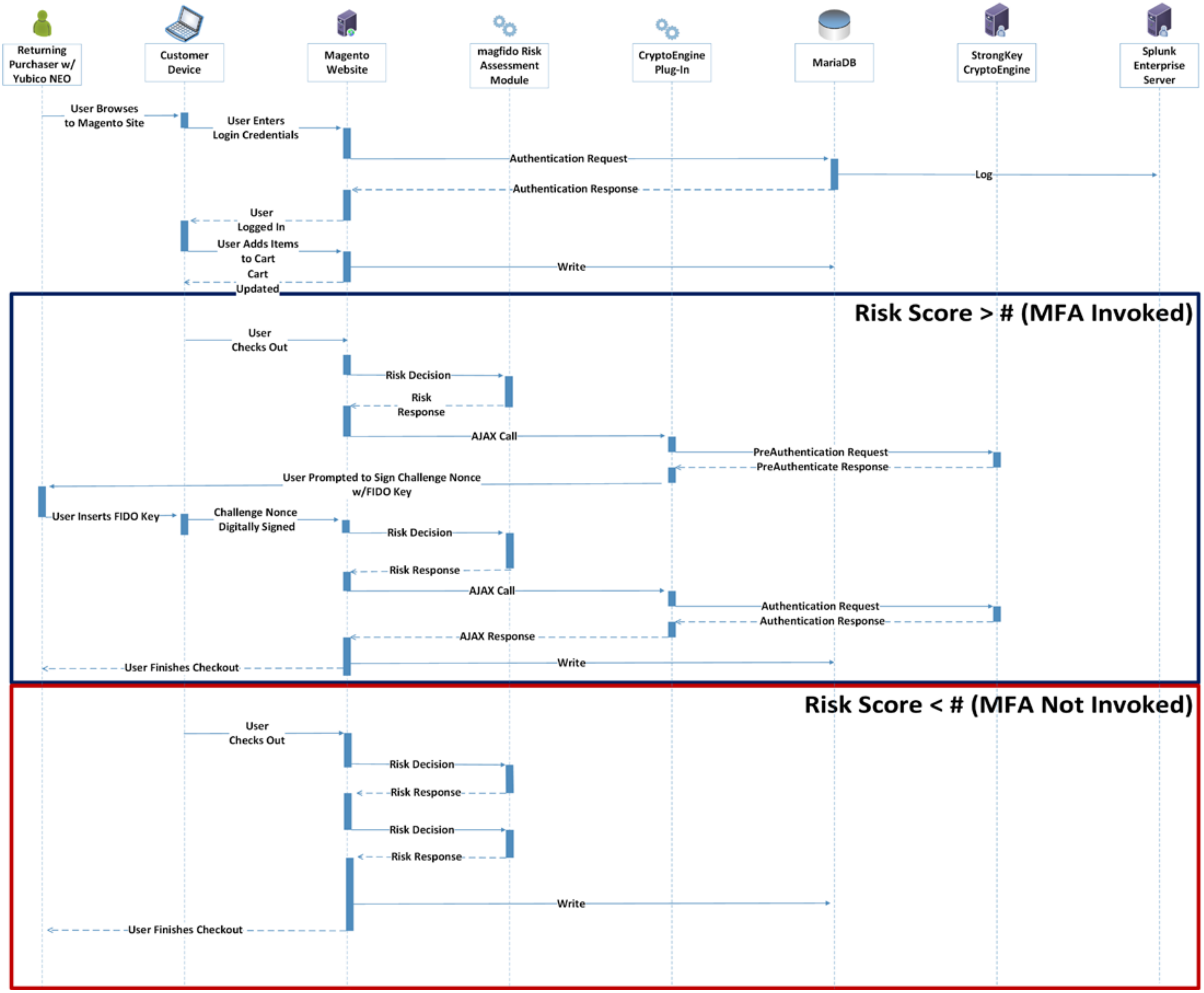
4.4.1 Cost Threshold Process Flow

Figure 4-3 shows the process flow as a returning purchaser browses to the shopping site and enters their customer ID and password, and as, upon checkout, the risk assessment module makes a decision to either require (box surrounded in blue) or not require (box surrounded in red) use of the U2F authenticator. If the returning purchaser's U2F authenticator is requested, then the shopping transaction will complete only upon successful use of the U2F.

The process flow of Figure 4-3 is described below.

- The returning purchaser uses their laptop (customer device) to shop on the Magento e-commerce platform website.
- The returning purchaser authenticates to the Magento e-commerce platform's MariaDB with their customer ID and password.
- As the checkout process begins, the risk assessment module makes a risk decision and then either allows the transaction to complete with no further authentication requirements (as shown within the red box) or, in the case of a transaction with increased risk, transmits its risk assessment need to use MFA to the SKCE Plug-In (as shown within the blue box).
- The returning purchaser then inserts their FIDO key into their customer device, and their authentication is approved or denied based upon the validity of their security key.

Figure 4-3 Cost Threshold Process Flow



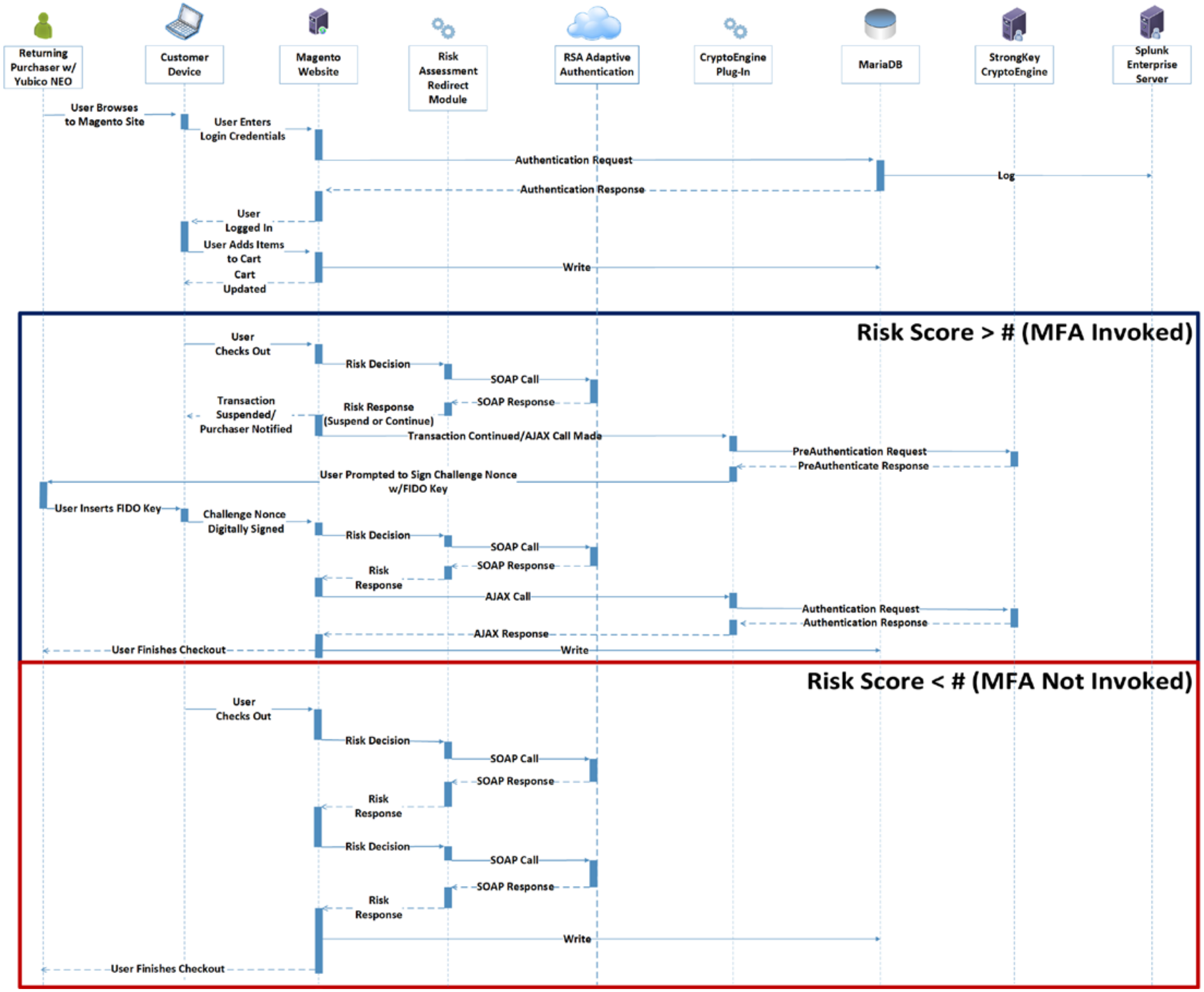
4.4.2 Risk Engine Process Flow

Figure 4-4 shows the process flow as a returning purchaser browses to the shopping site and enters their customer ID and password, and as, upon checkout, the risk engine makes a decision to either require (box surrounded in blue) or not require (box surrounded in red) use of the U2F authenticator. If the returning purchaser's U2F authenticator is requested, then the shopping transaction will complete only upon successful use of the U2F.

The process flow of Figure 4-4 is described below.

- The returning purchaser uses their laptop (customer device) to shop on the Magento e-commerce platform's website.
- The returning purchaser authenticates to the Magento e-commerce platform's MariaDB with their customer ID and password.
- As the checkout process begins, the risk engine makes a risk decision and then allows the transaction to complete with no further authentication requirements (as shown within the red box) or, in the case of a transaction with increased risk, allows the transaction to continue with the use of MFA or suspends the transaction if it exceeds organizational risk tolerances (as shown within the blue box).
- The returning purchaser then inserts their FIDO key into their customer device, and their authentication is approved or denied based upon the validity of their security key.

Figure 4-4 Risk Engine Process Flow



5 Solution Scoping for the Example Implementations

This section provides information about the scope and the use cases that apply to the example implementations, as well as customization options for the *cost threshold* example implementation.

5.1 Scoping Context of the Returning Purchaser Processes

Real-world extension modules to Magento could include additional criteria to identify risk. While there is also a multishipping workflow in Magento, this architecture modifies only the default single-address checkout process flow. In environments using the multishipping workflow to enable shipping a single order to multiple addresses, appropriate changes within that workflow will be needed to incorporate FIDO as described within this practice guide.

5.1.1 Securing the FIDO Security Key Registration Process

The FIDO registration workflow's level of security should be considered. The example implementations prompt the returning purchaser to use a registered U2F only when the shopping session exceeds a predetermined level of risk—in this case, the dollar amount. With this example, strong authentication is used only when a transaction exceeds the predetermined level of risk, and not for all purchaser-related activities. This implies that if an attacker compromised a legitimate purchaser's password, then the attacker could register a new FIDO Security Key under that account.

Once registered, the attacker could use their registered key to authorize any checkout that requires FIDO-based strong authentication. Reference Section 8 for information regarding how to help mitigate this threat.

5.1.2 Lost U2F or Registration of a New U2F

The following areas are outside this project's scope and were identified as options that could help mitigate risks related to lost or new U2F Security Key registration risks:

- The purchaser is required to register a key when an account is created. When any subsequent FIDO keys are registered, a previously existing FIDO key is required for authentication before registering those subsequent FIDO keys.
- Configure Magento to always require FIDO-based strong authentication for any changes to an account's U2F Security Key registration settings, once a FIDO Security Key is registered. This will help inhibit a malicious actor from registering a second FIDO key into the account and from using that FIDO key to perform cart checkout activities and to circumvent the security measures of the checkout process.
- As detailed in Section 8, workflow that enables existing purchasers to confirm their identity by other means (e.g., by confirming receipt of an email sent to their account, by entering a

personal identification number (PIN) before being able to register their FIDO key, or via other contact methods) could also be employed in cases where existing purchasers will be registering a new FIDO key.

5.2 Example Implementation Use Cases

The example implementations were designed and built to support the following e-commerce use cases that were developed with input from the NCCoE Retail COI. The first use case involved the U2F not being requested, and the second use case shows the U2F being requested when the returning purchaser attempts to make an online purchase. A third use case applies to both the *cost threshold* and *risk engine* example implementations when a system administrator is managing the e-commerce platform.

5.2.1 Use Case 1: Risk Threshold Not Exceeded—MFA Not Requested

In use case 1, a returning purchaser shops for items and places them into their shopping cart, and then, upon checkout, either a predetermined purchase amount is not exceeded (in the *cost threshold* example implementation) or the risk engine determines that the transaction is lower risk (in the *risk engine* example implementation). The purchaser continues through their checkout activities and completes the shopping experience without invoking the U2F.

5.2.2 Use Case 2: Risk Threshold Exceeded—MFA Requested

In use case 2, a returning purchaser shops for items and places them into their shopping cart, and then, upon checkout, either a predetermined purchase amount is exceeded *(cost threshold)* or the risk engine determines that the transaction is higher risk *(risk engine).* The returning purchaser is prompted to use U2F confirmation and, upon doing so, completes the shopping experience after successfully using their U2F.

The Adaptive Authentication Risk Engine leverages machine learning for device identification, assessment of the consumer’s purchase activity, the merchant population’s purchase activity, and global fraud indicators to determine if a transaction appears risky enough to warrant an MFA challenge.

In scenarios where the U2F is not successfully used, the purchase is declined. This could take place if the returning purchaser did not successfully use their U2F or if the purchaser’s customer ID and password are being used by someone who does not possess the U2F.

5.2.3 Use Case 3: System Administrator Prompted for MFA

In use case 3, MFA is required by e-commerce platform administration personnel before they perform system administration activities. Implementing MFA for administrative accounts can help limit the risk of compromising the information system that hosts the e-commerce solution. This applies to both example implementations *(cost threshold* and *risk engine).* This helps limit the risk of the e-commerce platform administrator's authentication credentials being compromised and provides assurance that they are being used by an authorized person.

5.3 Cost Threshold Example Implementation Customization Options

Leveraging the concepts from this practice guide's example implementations, retail organizations can customize their risk mitigation scenarios beyond those described above. For example, if the MFA login was not successfully used, then customized risk mitigation scenarios could include these actions:

- Identify the transaction for follow-up and review by the retailer fraud-detection team. Direct the person attempting to complete the transaction to the online retailer's customer service department, where review of the shopping transaction could take place.
- Notify the returning purchaser via email if a purchase is declined because their MFA device is not used successfully (potentially by another person not authorized to shop on their account).

In addition to the above scenarios, the retailer can review their organizational risk thresholds and explore additional risk-based decision options beyond the shopping-cart purchase exceeding a predetermined dollar amount. These options could include requesting MFA from the purchaser when the following situations take place:

- The purchaser provides a new or updated ship-to address.
- The purchaser's billing and ship-to address do not match.
- The machine internet protocol (IP) address differs from those previously used or is from a certain IP address range.
- The purchaser uses a new credit card.
- The purchaser purchases specific items or categories that are often included in fraudulent purchases.
- The purchaser purchases items from a new location.
- a combination of any of the above risk factors, for example, an order with a high transaction amount that is shipping to a new or updated ship-to address or transactions where billing and ship-to addresses do not match and a prespecified transaction amount is exceeded
- other scenarios whose logic could be predetermined, such as additional combinations from the list above or other risk-based decision options could also be used

6 Security Characteristic Analysis

The purpose of the security characteristic analysis is to understand the extent to which the project meets its objective of demonstrating the use of MFA in an e-commerce environment. In addition, it seeks to understand the security benefits and drawbacks of the example solutions.

6.1 Assumptions and Limitations

The security characteristic analysis has the following limitations:

- It is neither a comprehensive test of all security components nor a red-team exercise.
- It cannot identify all weaknesses.
- It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting these reference architectures.

As a best-practice recommendation to help keep the organization's Magento product current, visit the Resources section of the Magento website to sign up for updates on the most recent security patches and best practices [32].

6.2 Build Testing

The purpose of the security characteristic analysis is to understand the extent to which the project meets its objective of demonstrating the use of MFA in an e-commerce environment. In addition, it seeks to understand the security benefits and drawbacks of the reference designs. Also, Appendix C provides information regarding research into the products used for architecture components.

6.3 Scenarios and Findings

One aspect of our security evaluation involved assessing how well the reference designs address the security characteristics that they were intended to support. The Cybersecurity Framework Subcategories were used to provide structure to the security assessment by consulting the specific sections of each standard that are cited in reference to that Subcategory. The cited sections provide validation points that the example implementations would be expected to exhibit. Using the Cybersecurity Framework Subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference designs support the intended security characteristics.

6.4 Analysis of the Reference Designs' Support for Cybersecurity Framework Subcategories

This section analyzes the example implementations in terms of the specific Subcategories of the Cybersecurity Framework that they support. This enables an understanding of how the example implementations achieved the goals of the design when compared against a standardized framework. This section identifies the security benefits provided by each component of the example implementations and how those components support specific cybersecurity activities, as specified in terms of Cybersecurity Framework Subcategories.

The Cybersecurity Framework includes Functions, Categories, and Subcategories that define the capabilities and processes needed to implement a cybersecurity program. In Table A-1, the NCCoE has identified the Subcategories that are desirable to implement when deploying the example implementations. This section discusses how the example implementations support each of the Subcategories listed in Table A-1. Using the Subcategories as a basis for organizing our analysis allowed us to systematically consider how well the example implementations support specific security activities and provides structure to our security analysis.

6.4.1 DE.CM-1: The Network Is Monitored to Detect Potential Cybersecurity Events

The reference designs support monitoring network activity, with a focus on monitoring authentication attempts. Event log information is correlated with the reference designs' network architectures to make the following determinations:

- total authentication attempts
- successful login attempts
- unsuccessful login attempts

6.4.2 ID.RA-4: Potential Business Impacts and Likelihoods Are Identified

The example implementations track the transaction dollar-purchase amount to determine whether U2F authentication is needed. If the purchase amount meets or exceeds the threshold dollar amount, then U2F authentication is activated.

The risk assessment function of the example implementations enables the online retailer to identify shopping experience attributes that are likely to create business impact. These attributes include the cost of items in the shopping cart and could also use the attributes and potential workflow discussed in Section 5.3 or the capabilities that the risk engine provides.

The information gained from the shopping cart's dollar-amount attribute is used to determine when an organization would elect to employ a U2F authentication device request for a shopping session.

6.4.3 ID.RA-5: Threats, Vulnerabilities, Likelihoods, and Impacts Are Used to Determine Risk

The impact to the implementing organization of a potentially fraudulent transaction is used to determine risk. In the example implementations, the risk engine or the total cost of the items in the shopping cart could be used to help determine the financial risk to which the implementing e-commerce retailer might be subject. Section 5.3 describes additional attributes that could be used to help determine and mitigate the online shopping session's risk.

6.4.4 PR.AC-1: Identities and Credentials Are Issued, Managed, Verified, Revoked, and Audited for Authorized Devices, Users, and Processes

The example implementations use U2F authentication to authorize purchasers and their devices. Specifically, the Yubico YubiKey NEO Security Key was used as the purchaser's second factor authentication mechanism. The Yubico YubiKey NEO Security Key is a hardware FIDO Ready U2F authenticator. It uses public key cryptography, which includes a private key that never leaves the NEO. When a purchaser registers an account on the e-commerce platform, the Yubico YubiKey NEO Security Key uses the private key to generate another cryptographic key that is unique for the e-commerce platform.

In the example implementations, the unique key is used to develop a public key that is sent and stored on the StrongKey FIDO server. After the registration process is completed, logging into the e-commerce platform's website continues to use the unique generated cryptographic key and the public key stored on the StrongKey FIDO server to authenticate the purchaser. The StrongKey FIDO server provides the U2F registration, authentication, and storage of purchaser registration data. The TokenOne cloud-based infrastructure provides an administration interface and services for authentication credential life-cycle management.

6.4.5 PR.AC-7: Users, Devices, and Other Assets Are Authenticated (e.g., Single Factor, Multifactor), Commensurate with the Risk of the Transaction (e.g., Individuals' Security and Privacy Risks and Other Organizational Risks)

Authentication that is commensurate with the risk of the transaction is an intrinsic part of the example implementations. Users are authenticated based upon the shopping transaction's level of risk. For transactions deemed to be lower risk, customer ID and password are used. For transactions with increased risk, U2F MFA is used.

For the *cost threshold* example implementation, acceptable shopping cart dollar-amount risk levels are made by the implementing organization. For the *risk engine* example implementation, risk engine analysis determines when additional authentication will be prompted. In both example implementations, when the risk threshold is exceeded, an MFA request is then activated and communicated to the returning purchaser.

In both example implementations, MFA is required by e-commerce administration personnel before they perform system administration activities. Implementing MFA for administrative accounts can help limit the risk of compromise of the information system that hosts the e-commerce solution.

6.4.6 RS.AN-1: Notifications from Detection Systems Are Investigated

The example implementations leverage Splunk Enterprise displays to provide logging information in a dashboard format that can be investigated by system operators.

6.5 Systems Engineering

Some organizations use a systems-engineering-based approach to plan and implement their IT projects. Organizations wishing to implement IT systems should conduct robust requirements development, considering the operational needs of each system stakeholder. Standards, such as ISO/IEC 15288:2015 [33] and NIST SP 800-160 [17], provide guidance for applying security in systems development. With each of these standards, organizations can choose to adopt only those sections of the standard that are relevant to their development approach, environment, and business context. NIST SP 800-160 recommends thoroughly analyzing alternative solution classes accounting for security objectives, considerations, concerns, limitations, and constraints. This advice applies to both new system developments and integration of components into existing systems, which would be required to deploy the example implementations described in this practice guide.

6.5.1 Example Implementation Code Analysis

In support of systems engineering best practices, code developed to support the example implementations was analyzed by using manual and automated code analysis methods. As part of an overall systems engineering process, organizations can use systematic procedures and code-checking tools that will help find vulnerabilities or weaknesses that can be improved upon.

7 Functional Evaluation

Functional evaluations of the MFA example implementations, as constructed in our lab, were conducted to verify that they meet their objective of enabling a returning purchaser to use enhanced authentication capabilities for e-commerce transactions.

Section 7.1 describes the format and components of the functional test cases. Each functional test case was designed to assess the capability of the example implementations.

7.1 MFA Functional Tests

This section includes the test cases necessary to conduct the functional evaluation of the MFA example implementations. Refer to Section 4 for descriptions of the tested example implementations.

Each test case consists of multiple fields that collectively identify the goal of the test, the specifics required to implement the test, and how to assess the results of the test. Table 7-1 describes each field in the test case.

Table 7-1 Test Case Fields

Test Case Field	Description
Parent Requirement	Identifies the top-level requirement, or the series of top-level requirements, leading to the testable requirement.
Testable Requirement	Guides the definition of the remainder of the test case fields. Specifies the capability to be evaluated.
Description	Describes the objective of the test case.
Associated Test Cases	In some instances, a test case may be based on the outcome of (an)other test case(s). For example, analysis-based test cases produce a result that is verifiable through various means (e.g., log entries, reports, alerts).
Associated Cybersecurity Framework Subcategories	Lists the Cybersecurity Framework Subcategories addressed by the test case.
Preconditions	The starting state of the test case. Preconditions indicate various starting state items, such as a specific capability configuration required or specific protocol and content.
Procedure	The step-by-step actions required to implement the test case. A procedure may consist of a single sequence of steps or multiple sequences of steps (with delineation) to indicate variations in the test procedure.
Expected Results	the expected results for each variation in the test procedure

Test Case Field	Description
Actual Results	the observed results
Overall Results	The overall result of the test as pass/fail. In some test case instances, determination of the overall result may be more involved, such as determining pass/fail based on a percentage of errors identified.

7.1.1 MFA Use Case Requirements

Table 7-2 identifies the MFA functional analysis requirements that are addressed in the associated requirements and test cases.

Table 7-2 Functional Analysis Requirements

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
CR 1	The MFA example implementations shall determine if a purchase does not require U2F authentication for the *cost threshold* and *risk engine* example lab builds.			MFA-1
CR 1.a		RSA, StrongKey, and Magento, with the authenticator contained in CR 1.a.1		MFA-1
CR 1.a.1			Customer ID and password	MFA-1
CR 2	The MFA example implementations shall determine if a purchase requires U2F authentication for			MFA-2

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
	the *cost threshold* and *risk engine* example lab builds.			
CR 2.a		RSA, StrongKey, and Magento, with the authenticator contained in CR 2.a.1		MFA-2
CR 2.a.1			Yubico	MFA-2
CR 3	The MFA example implementations shall detect failed login attempts by a purchaser's account for the *cost threshold* and *risk engine* example lab builds.			MFA-3
CR 3.a		Splunk Enterprise and Magento, with the authenticator contained in CR 3.a.1		MFA-3
CR 3.a.1			Customer ID and password	MFA-3
CR 4	The MFA example implementations shall lock a purchaser's account upon detection of that account exceeding a predetermined number of failed login attempts for the *cost threshold* and *risk engine* example lab builds.			MFA-4

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
CR 4.a		Magento, with the authenticator contained in CR 4.a.1		MFA-4
CR 4.a.1			Customer ID and password	MFA-4
CR 5	The MFA example implementations shall strongly authenticate retailer e-commerce platform administrators before the administrators perform administration activities.			MFA-5
CR 5.a		Magento and TokenOne, with the authenticator contained in CR 5.a.1		MFA-5
CR 5.a.1			TokenOne Authenticator	MFA-5

7.1.2 Test Case MFA-1 (MFA Not Required)

Table 7-3 contains test case requirements, associated test cases, and descriptions of the test scenarios for the MFA capabilities of the example implementations.

Table 7-3 Test Case MFA-1 (MFA Not Required)

Test Case Field	Description
Parent Requirement	(CR 1) The MFA example implementations shall determine if a purchase does not require a U2F mechanism for the *cost threshold* and *risk engine* example lab builds.

Test Case Field	Description
Testable Requirement	(CR 1.a) RSA, StrongKey, and Magento (CR 1.a.1) Using customer ID and password
Description	Show that the MFA example implementation can determine that a purchase is lower risk and therefore does not require additional U2F authentication.
Associated Test Cases	CR 1
Associated Cybersecurity Framework Subcategories	ID.RA-4, ID.RA-5, PR.AC-7
Preconditions	(CR 1.a) RSA, StrongKey, and Magento capabilities are implemented and operational in the lab environment. Yubico FIDO U2F authenticator is registered to a purchaser account on the e-commerce platform. The purchase dollar-amount threshold has been set to determine when U2F authentication is activated.
Procedure	The returning purchaser logs into the e-commerce platform's website with their customer ID and password and initiates and completes a lower-risk purchase that does not require U2F use by the returning purchaser.
Expected Results	(CR 1) The MFA example implementation determines that U2F authentication is not needed. (CR 1.a) U2F authentication with Yubico (CR 1.a.1) is not activated because the purchase dollar-amount is below the set threshold.
Actual Results	The returning purchaser logged into their account by using their customer ID and password, placed items totaling $25 or less (for the *cost threshold* build) or $50 or less (for the *risk engine* build) into the shopping cart, and then completed their shopping purchase.

Test Case Field	Description
Overall Results	The returning purchaser was able to complete their lower-risk purchase with only their customer ID and password.

7.1.3 Test Case MFA-2 (MFA Required)

Table 7-4 contains test case requirements, associated test cases, and descriptions of the test scenarios for the MFA capabilities of the example implementations.

Table 7-4 Test Case MFA-2 (MFA Required)

Test Case Field	Description
Parent Requirement	(CR 2) The MFA example implementations shall determine if a purchase requires U2F authentication for the *cost threshold* and *risk engine* example lab builds.
Testable Requirement	(CR 2.a) RSA, StrongKey, and Magento (CR 2.a.1) Yubico
Description	Show that the MFA example implementation can determine that a shopping session exceeds organizational risk tolerance, and therefore the transaction requires the successful use of U2F authentication for the shopping transaction to be completed.
Associated Test Cases	CR 2
Associated Cybersecurity Framework Subcategories	ID.RA-4, ID.RA-5, PR.AC-7
Preconditions	(CR 2.a) Reuse RSA, StrongKey, and Magento capabilities in the state after MFA-1 is completed
Procedure	The returning purchaser logs onto the website and initiates and completes an increased-risk purchase that would require the returning purchaser to use U2F.

Test Case Field	Description
Expected Results	(CR 2) The MFA example implementation determines that U2F authentication is needed. (CR 2.a) U2F authentication with Yubico (CR 2.a.1) is activated because the purchase dollar-amount is above the thresholds that trigger an MFA response. The online shopping transaction does not proceed to completion without the returning purchaser's successful use of the U2F authenticator.
Actual Results	The returning purchaser logged into their account with their customer ID and password, placed items greater than $25 (for the *cost threshold* build) or greater than $50 (for the *risk engine* build) into the shopping cart, and then completed the shopping purchase by using the U2F authenticator when prompted. The shopping session would not continue without the U2F authenticator being successfully activated.
Overall Results	The returning purchaser was able to complete their increased-risk purchase with U2F.

7.1.4 Test Case MFA-3 (Failed Login Attempts Detected)

Table 7-5 contains test case requirements, associated test cases, and descriptions of the test scenarios for the failed-login-attempt detection capabilities of the example implementations.

Table 7-5 Test Case MFA-3 (Failed Login Attempts Detected)

Test Case Field	Description
Parent Requirement	(CR 3) The MFA example implementation shall detect failed login attempts by a purchaser's account for the *cost threshold* and *risk engine* example lab builds.
Testable Requirement	(CR 3.a) Splunk Enterprise and Magento
Description	Show that the MFA example implementation can detect and demonstrate in a dashboard the customer ID and password's failed login attempts.

Test Case Field	Description
Associated Test Cases	CR 2
Associated Cybersecurity Framework Subcategories	DE.CM-1, PR.AC-1, PR.AC-7, RS.AN-1
Preconditions	Reuse MFA example implementation in the state after MFA-2 is completed.
Procedure	An automated logging and reporting dashboard capability is built. It identifies and displays failed purchaser-authentication attempts.
Expected Results	(CR 3, CR 3.a) The logging and reporting dashboard capability identifies and displays failed purchaser-account-authentication attempts. (CR 3.a.1) The account is identified by the customer ID and password.
Actual Results	The automated logging and reporting dashboard displayed failed purchaser-authentication attempts.
Overall Results	The automated logging and reporting dashboard displayed a historical display of failed purchaser-authentication attempts.

7.1.5 Test Case MFA-4 (Accounts Automatically Locked After Failed Login Attempts)

Table 7-6 contains test case requirements, associated test cases, and descriptions of the test scenarios for the automatic account lockout capabilities of the example implementations.

Table 7-6 Test Case MFA-4 (Accounts Automatically Locked After Failed Login Attempts)

Test Case Field	Description
Parent Requirement	(CR 4) The MFA example implementation shall lock a purchaser's account upon detection of that account exceeding a predetermined number of failed login attempts for the *cost threshold* and *risk engine* example lab builds.

Test Case Field	Description
Testable Requirement	(CR 4.a) Magento
Description	Show that the MFA example implementation can lock a purchaser account if the allowed number of customer ID and password-authentication attempts is exceeded.
Associated Test Cases	CR 3
Associated Cybersecurity Framework Subcategories	DE.CM-1, PR.AC-1
Preconditions	Reuse MFA example implementation in the state after MFA-3 is completed.
Procedure	After the failed authentication limit has been met, the purchaser account is locked out.
Expected Results	(CR 4, CR 4.a, CR 4.a.1) The returning purchaser account is locked, and the purchaser is unable to log into the account after the threshold limit for failed authentications is met for an amount of time determined by the organization.
Actual Results	The failed authentication attempts were made until the previously identified threshold was met, at which time the account was locked for a previously identified amount of time (in this case, 20 minutes).
Overall Results	The returning purchaser's account was locked out for a previously determined amount of time before the account could be used again.

7.1.6 Test Case MFA-5 (System Administrator MFA)

Table 7-7 contains test case requirements, associated test cases, and descriptions of the test scenarios for the e-commerce platform system administrator MFA capabilities of the example implementations.

Table 7-7 Test Case MFA-5 (System Administrator MFA)

Test Case Field	Description
Parent Requirement	(CR 5) The MFA example implementations shall strongly authenticate e-commerce platform administrators before the administrators perform administration activities.
Testable Requirement	(CR 5.a) Magento and TokenOne
Description	Show that the MFA example implementation requires the e-commerce platform administrator to authenticate with TokenOne before logging in and performing administration.
Associated Test Cases	None applicable
Associated Cybersecurity Framework Subcategories	ID.RA-4, PR.AC-7
Preconditions	Reuse MFA example implementation in the state after MFA-1 is completed.
Procedure	Attach to the Magento e-commerce platform and attempt to log in. Provide account and authentication information as prompted.
Expected Results	(CR 5, CR 5.a, CR 5.a.1) The e-commerce platform administrator must authenticate by using their TokenOne authenticator before administering the platform.
Actual Results	The e-commerce platform administrator was prompted for their TokenOne multifactor authenticator before being able to manage the platform.
Overall Results	When the e-commerce platform administrator used their TokenOne authenticator, they were able to manage the Magento e-commerce platform. When the e-commerce administrator did not provide their TokenOne credentials, their account was denied access to the Magento e-commerce platform.

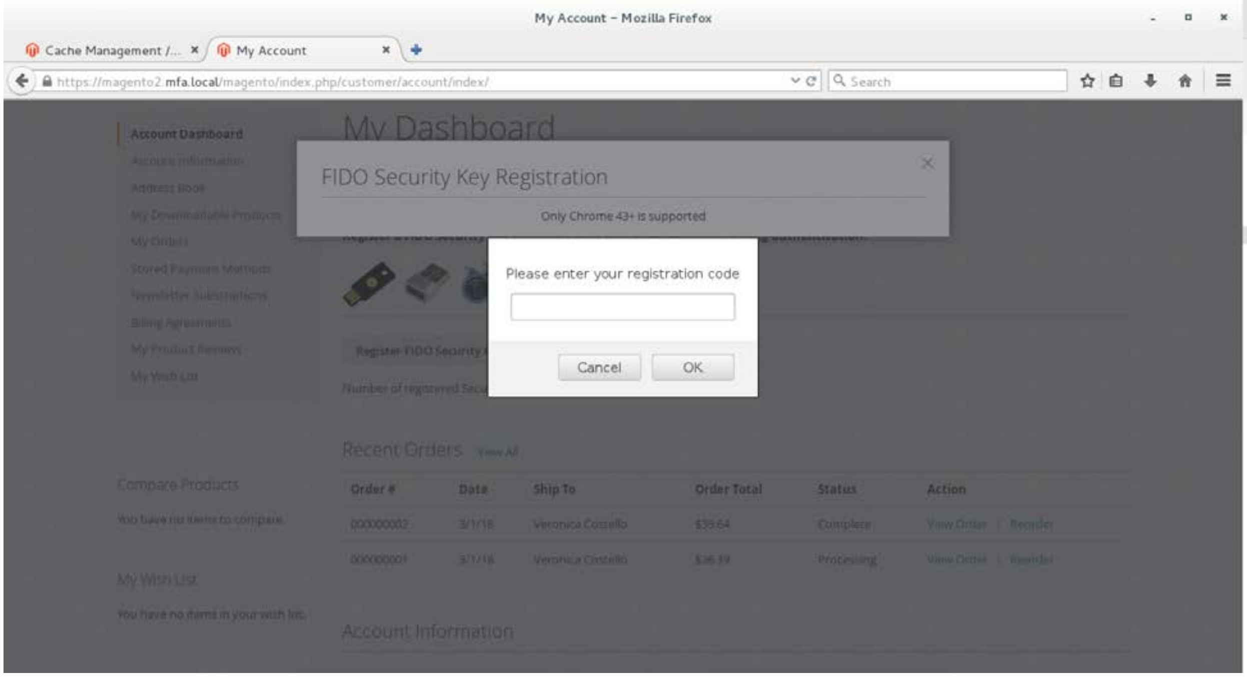
8 Future Build Considerations

Authentication technologies, such as MFA, are continuously evolving. Additional future build considerations may include the topics described in this section.

8.1 FIDO Key Registration Enhancements

Additional future build considerations include securing the FIDO key registration process with a PIN. The PIN would be sent to the customer's registered email account. The customer would then enter the registration-code PIN received in the email, as displayed on the screen shown in Figure 8-1, before being allowed to register a FIDO authenticator.

Figure 8-1 FIDO Authenticator Registration Confirmation PIN



FIDO Security Key Registration

Only Chrome 43+ is supported

Please enter your registration code

You have no items to compare.

You have no items in your wish list.

Recent Orders View All

Order #	Date	Ship To	Order Total	Status	Action
000000002	3/1/18	Veronica Costello	$39.64	Complete	View Order | Reorder
000000001	3/1/18	Veronica Costello	$36.39	Processing	View Order | Reorder

8.2 IP Address as a Risk Factor

Another future build consideration would be to add the IP address as a factor that is analyzed to trigger the need for MFA in the *cost threshold* example implementation. Currently, the *cost threshold* example implementation examines the dollar amount in the shopping cart when determining whether MFA is needed. An e-commerce transaction's originating IP address can be an indicator of increased risk [34]. Adding the IP address as a factor that is analyzed during an e-commerce transaction might appeal to those who are considering the *cost threshold* example implementation and who require more risk factors to be addressed.

Appendix A Mapping to Cybersecurity Framework

Table A-1 maps National Institute of Standards and Technology (NIST) and consensus security references to the NIST Cybersecurity Framework Subcategories and International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 27001:2013 mappings that are addressed in this practice guide. Additionally, from NIST Special Publication (SP) 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [18], work roles are identified so that organizations may understand the work roles that are typically used by those implementing the capabilities contained in this practice guide.

Table A-1 Multifactor Authentication for E-Commerce Cybersecurity Framework Components Mapping

Cybersecurity Framework v1.1			Standards and Best Practices Alignment		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Rev. 4 Security and Privacy Controls**	**ISO/IEC 27001:2013**	**NIST SP 800-181, NICE Framework Work Roles**
IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-4: Potential business impacts and likelihoods are identified.	RA-2: Security Categorization RA-3: Risk Assessment PM-9: Risk Management Strategy PM-11: Mission/Business Process Definition SA-14: Criticality Analysis	ISO/IEC N/A	AN-TWA-001 Threat/Warning Analyst OM-ANA-001 Systems Security Analyst PR-CDA-001 Cyber Defense Analyst OV-MGT-001 Information Systems Security Manager
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	RA-2: Security Categorization RA-3: Risk Assessment PM-16: Threat Awareness Program	A.12.6.1	AN-TWA-001 Threat/Warning Analyst PR-CDA-001 Cyber Defense Analyst OV-MGT-001 Information Systems Security Manager

Cybersecurity Framework v1.1			Standards and Best Practices Alignment		
Function	Category	Subcategory	NIST SP 800-53 Rev. 4 Security and Privacy Controls	ISO/IEC 27001:2013	NIST SP 800-181, NICE Framework Work Roles
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AC)	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	AC-1: Access Control Policy and Procedures AC-2: Account Management IA-1: Identification and Authentication Policy and Procedures IA-2: Identification and Authentication (Organizational Users) IA-3: Device Identification and Authentication IA-4: Identifier Management IA-5: Authenticator Management IA-6: Authenticator Feedback IA-7: Cryptographic Module Authentication IA-8: Identification and Authentication (Nonorganizational Users) IA-9: Service Identification and Authentication IA-10: Adaptive Identification and Authentication	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3	OM-ANA-001 Systems Security Analyst PR-CDA-001 Cyber Defense Analyst OM-ADM-001 System Administrator OV-PMA-003 Product Support Manager SP-DEV-001 Software Developer

Cybersecurity Framework v1.1			Standards and Best Practices Alignment		
Function	Category	Subcategory	NIST SP 800-53 Rev. 4 Security and Privacy Controls	ISO/IEC 27001:2013	NIST SP 800-181, NICE Framework Work Roles
			IA-11: Reauthentication		
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	AC-7: Unsuccessful Logon Attempts AC-8: System Use Notification AC-9: Previous Logon (Access) Notification AC-11: Session Lock AC-12: Session Termination AC-14: Permitted Actions Without Identification or Authentication IA-1: Identification and Authentication Policy and Procedures IA-2: Identification and Authentication (Organizational Users) IA-3: Device Identification and Authentication IA-4: Identifier Management IA-5: Authenticator Management IA-8: Identification and Authentication	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4	OM-ANA-001 Systems Security Analyst PR-CDA-001 Cyber Defense Analyst OM-ADM-001 System Administrator OV-PMA-003 Product Support Manager SP-DEV-001 Software Developer

Cybersecurity Framework v1.1			Standards and Best Practices Alignment		
Function	Category	Subcategory	NIST SP 800-53 Rev. 4 Security and Privacy Controls	ISO/IEC 27001:2013	NIST SP 800-181, NICE Framework Work Roles
			(Nonorganizational Users) IA-9: Service Identification and Authentication IA-10: Adaptive Identification and Authentication IA-11: Reauthentication		
DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-1: The network is monitored to detect potential cybersecurity events.	AC-2: Account Management AU-12: Audit Generation CA-7: Continuous Monitoring CM-3: Configuration Change Control SC-5: Denial of Service Protection SC-7: Boundary Protection SI-4: Information System Monitoring	ISO/IEC N/A	PR-CDA-001 Cyber Defense Analyst

Cybersecurity Framework v1.1			Standards and Best Practices Alignment		
Function	Category	Subcategory	NIST SP 800-53 Rev. 4 Security and Privacy Controls	ISO/IEC 27001:2013	NIST SP 800-181, NICE Framework Work Roles
RESPOND (RS)	Analysis (RS.AN)	RS.AN-1: Notifications from detection systems are investigated.	AU-6: Audit Review, Analysis, and Reporting CA-7: Continuous Monitoring IR-4: Incident Handling IR-5: Incident Reporting PE-6: Monitoring Physical Access SI-4: Information System Monitoring	A.12.4.1, A.12.4.3, A.16.1.5	PR-CDA-001 Cyber Defense Analyst PR-CIR-001 Cyber Defense Incident Responder IN-FOR-002 Cyber Defense Forensics Analyst

Appendix B Assumptions

This project is guided by the assumptions described in the following subsections. Implementers are advised to consider whether the same assumptions can be made based on current policy, process, and information-technology infrastructure. Where applicable, appropriate guidance is provided to assist implementation.

B.1 Availability of Skills

An organization has a workforce able to implement the multifactor authentication (MFA) capabilities described in this practice guide. Work roles in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [18] are identified in Appendix A to assist organizations to see which work roles perform the tasks necessary to implement the capabilities contained in this practice guide. A NICE Framework work role is composed of specific knowledge, skills, and abilities required to perform tasks in that work role.

B.2 Uniqueness of Lab Environment

The example implementations were developed in a lab environment. They do not reflect the complexity of a production environment, and production deployment processes were not used. Before production deployment, it should be confirmed that the example implementation capabilities meet the organization’s architecture, reliability, and scalability requirements.

B.3 MFA Decreases Account Takeover Opportunities

Using customer identification (ID) and password alone for authentication provides increased opportunities for account takeover, compared with the additional use of MFA.

B.4 Web Browser and Returning Purchaser Accounts

A web browser, not a mobile application, was used to make the purchase from the electronic commerce (e-commerce) platform’s website. A returning purchaser had an account with the online retailer.

B.5 Support of MFA Devices

The purchaser expects the retailer to be committed to the continued use and support of Universal Second Factor (U2F) because the returning purchaser has invested time and/or expense in obtaining the authenticator device.

B.6 Customer Support Mechanisms for Lost Tokens

The retailer has established customer support mechanisms for lost U2F authenticators. This could include the ability to determine that the person calling their customer assistance line is the actual returning purchaser.

Appendix C Common Vulnerabilities and Exposures

To understand and mitigate security issues associated with architecture components, the Common Vulnerabilities and Exposures (CVE) database [35] was searched for security issues associated with the example build components.

A search of the collaborating vendors' products used in the example implementations was performed on March 15, 2018, which led to discovery of a single CVE vulnerability that applied to the example implementations. As reported in the online CVE database, the product has since been patched in an update. The example implementations froze version numbers in the example lab builds before the product patch was released.

Automated alerts can be subscribed to via the United States Computer Emergency Readiness Team to keep up-to-date on current security issues and vulnerabilities [36].

Appendix D List of Acronyms

AAL	Authenticator Assurance Level
CNP	Card Not Present
COI	Community of Interest
CR	Capability Requirement
CVE	Common Vulnerabilities and Exposures
e-commerce	Electronic Commerce
FAL	Federation Assurance Level
FIDO	Fast IDentity Online
IAL	Identity Assurance Level
ID	Identification
IDESG	Identity Ecosystem Steering Group
IP	Internet Protocol
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information Technology
MFA	Multifactor Authentication
NCCoE	National Cybersecurity Center of Excellence
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
PCI	Payment Card Industry
PIN	Personal Identification Number
SKCE	StrongKey CryptoEngine
SP	Special Publication
U.S.	United States
U2F	Universal Second Factor

USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team

Appendix E Glossary

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources [12]

Authentication Factor

The three types of authentication factors are *something you know*, *something you have*, and *something you are*. Every authenticator has one or more authentication factors [12].

Authenticator

Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity [12]

Authenticator Assurance Level (AAL)

A category describing the strength of the authentication process [12]

Credential

An object or data structure that authoritatively binds an identity—via an identifier or identifiers–and (optionally) additional attributes to at least one authenticator possessed and controlled by a subscriber

While common usage often assumes that the subscriber maintains the credential, these guidelines also use the term to refer to electronic records maintained by the Credential Service Providers that establish binding between the subscriber's authenticator(s) and identity [12].

Federation Assurance Level (FAL)

A category describing the assertion protocol used by the federation to communicate authentication and attribute information (if applicable) to a relying party [12]

Identity

An attribute or set of attributes that uniquely describe a subject within a given context [12]

Identity Assurance Level (IAL)

A category that conveys the degree of confidence that the applicant's claimed identity is their real identity [12]

Identity Fraud and Identity Theft

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain [37]

Multifactor A characteristic of an authentication system or an authenticator that requires more than one distinct authentication factor for successful authentication. MFA can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are [12].

Multifactor Authentication (MFA) An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are [12].

Multifactor Authenticator An authenticator that provides more than one distinct authentication factor, such as a cryptographic authentication device with an integrated biometric sensor that is required to activate the device [12]

Personal Identification Number (PIN) A memorized secret typically consisting of only decimal digits [12]

Phishing An attack in which the subscriber is lured (usually through an email) to interact with a counterfeit verifier or relying party and tricked into revealing information that can be used to masquerade as that subscriber to the real verifier or relying party [12]

Private Key The secret part of an asymmetric key pair that is used to digitally sign or decrypt data [12]

Public Key The public part of an asymmetric key pair that is used to verify signatures or encrypt data [12]

Public Key Certificate A digital document issued and digitally signed by the private key of a certificate authority that binds an identifier to a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. See also Request for Comment 5280 [12].

Relying Party An entity that relies upon the subscriber’s authenticator(s) and credentials or a verifier’s assertion of a claimant’s identity, typically to process a transaction or grant access to information or a system [12]

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence [9]

Session

A persistent interaction between a subscriber and an end point, either a relying party or a Credential Service Provider. A session begins with an authentication event and ends with a session termination event. A session is bound by use of a session secret that the subscriber's software (a browser, application, or operating system) can present to the relying party or the Credential Service Provider in lieu of the subscriber's authentication credentials [12].

Single Factor

A characteristic of an authentication system or an authenticator that requires only one authentication factor (something you know, something you have, or something you are) for successful authentication [12]

Subscriber

A party who has received a credential or authenticator from a Credential Service Provider [12]

Threat

An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss [17]

Token

See Authenticator [12]

Transaction

A discrete event between a user and a system that supports a business or programmatic purpose. A government digital system may have multiple categories or types of transactions, which may require separate analysis within the overall digital identity risk assessment [12].

Verifier

An entity that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status [12].

Vulnerability

Weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat [17]

Appendix F References

[1] U.S. Department of Treasury, Bureau of the Fiscal Service. Europay, Mastercard & Visa (EMV) [Online]. Available: https://fiscal.treasury.gov/cas/europay-mastercard-and-visa.html.

[2] FIDO Alliance. (n.d.). *What is FIDO?* [Online]. Available: https://fidoalliance.org/about/what-is-fido/.

[3] FIDO Alliance. (n.d.). *Specifications Overview* [Online]. Available: https://fidoalliance.org/specifications/overview/.

[4] FIDO Alliance. (n.d.). [Online]. Available: https://fidoalliance.org/.

[5] FIDO Alliance. (n.d.). *FIDO® Certified* [Online]. Available: https://fidoalliance.org/certification/fido-certified-products/.

[6] Splunk Inc. (n.d.). [Online]. Available: https://www.splunk.com/.

[7] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). (Oct. 2013). *ISO/IEC 27001:2013: Information technology–Security techniques–Information security management systems–Requirements* [Online]. Available: https://www.iso.org/standard/54534.html.

[8] National Institute of Standards and Technology (NIST). (Apr. 16, 2018). *NIST Cybersecurity Framework, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* [Online]. Available: https://www.nist.gov/cyberframework.

[9] NIST Special Publication (SP) 800-30 Rev. 1, *Guide for Conducting Risk Assessments.* (Sept. 2012). [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[10] NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach.* (June 5, 2014). [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final.

[11] NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* (Apr. 2013). [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[12] NIST SP 800-63-3, *Digital Identity Guidelines.* (June 2017). [Online]. Available: https://pages.nist.gov/800-63-3/.

[13] NIST SP 800-63A, *Digital Identity Guidelines, Enrollment and Identity Proofing.* (June 2017). [Online]. Available: https://pages.nist.gov/800-63-3/.

[14] NIST SP 800-63B, *Digital Identity Guidelines, Authentication and Lifecycle Management.* (June 2017). [Online]. Available: https://pages.nist.gov/800-63-3/.

[15] NIST SP 800-63C, *Digital Identity Guidelines, Federation and Assertions.* (June 2017). [Online]. Available: https://pages.nist.gov/800-63-3/.

[16] NIST SP 800-73-4, *Interfaces for Personal Identity Verification–Part 1: PIV Card Application Namespace, Data Model and Representation.* (May 2015). [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-73-4.pdf.

[17] NIST SP 800-160 Vol. 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.* (Mar. 21, 2018). [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final.

[18] NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* (Aug. 2017). [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-education-nice/nice-cybersecurity.

[19] PCI Security Standards Council, LLC. (n.d.). Document Library [Online]. Available: https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss.

[20] Identity Ecosystem Steering Group, Inc. (n.d.). The Identity Ecosystem Steering Group (IDESG) [Online]. Available: https://www.idesg.org/.

[21] Retail and Hospitality Information Sharing and Analysis Center (RH-ISAC). (n.d.). *RH-ISAC* [Online]. Available: https://rhisac.org/.

[22] Open Web Application Security Project. (Feb. 23, 2015). *Credential stuffing* [Online]. Available: https://www.owasp.org/index.php/Credential_stuffing.

[23] Shape Security, Inc. (Jan. 2017). *2017 Credential Spill Report* [Online]. Available: http://info.shapesecurity.com/2017-Credential-Spill-Report.html.

[24] Magento, Inc. (n.d.). *eCommerce Platform|Best eCommerce Software for Selling Online* [Online]. Available: https://magento.com/.

[25] A. Noor and A. de Leon. SourceForge. (Feb. 20, 2018). *FIDO U2F Integration for Magento 2* [Online]. Available: https://sourceforge.net/projects/magfido/?source=navbar.

[26] StrongKey. (n.d.). Home–StrongKey [Online]. Available: https://www.strongkey.com/.

[27] RSA Security LLC. (n.d.). *Adaptive Authentication|Fraud Detection–RSA* [Online]. Available: https://www.rsa.com/en-us/products/fraud-prevention/secure-consumer-access.

[28] TokenOne. (n.d.). *TokenOne|Secure Authentication|Sydney* [Online]. Available: https://www.tokenone.com.

[29] Yubico. (n.d.). *Yubico|YubiKey Strong Two Factor Authentication for Business and Individual Use* [Online]. Available: https://www.yubico.com/.

[30] A. Noor et al. (July 3, 2018). SourceForge. *FIDO strong authentication, encryption, digital signature engine* [Online]. Available: https://sourceforge.net/projects/skce/.

[31] PCI Security Standards Council, LLC. (May 2015). *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2* [Online]. Available: https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss.

[32] Magento, Inc. (n.d.). Security Center [Online]. Available: https://magento.com/security.

[33] ISO/IEC/Institute of Electrical and Electronics Engineers (IEEE). (May 2015). *ISO/IEC/IEEE 15288:2015: Systems and software engineering–System life cycle processes* [Online]. Available: https://www.iso.org/standard/63711.html.

[34] M. Tatham. (Apr. 13, 2018). Experian. *Russian Hackers Aren't the Only Ones to Worry About: Online Shopping Fraud Report* [Online]. Available: https://www.experian.com/blogs/ask-experian/the-state-of-online-shopping-fraud/.

[35] The MITRE Corporation. (n.d.). *CVE–Common Vulnerabilities and Exposures (CVE)* [Online]. Available: https://cve.mitre.org/.

[36] United States Computer Emergency Readiness Team (US-CERT). (n.d.). *Alerts* [Online]. Available: https://www.us-cert.gov/ncas/alerts.

[37] United States Department of Justice. (Feb. 7, 2017). *Identity Theft* [Online]. Available: https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.