National Cybersecurity Center of Excellence (NCCoE)

Consumer/Retail Sector Community of Interest Call

Multifactor Authentication for e-Commerce

Project Lead: Bill Newhouse
Guest Speaker: Paul A. Grassi
September 20, 2016

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

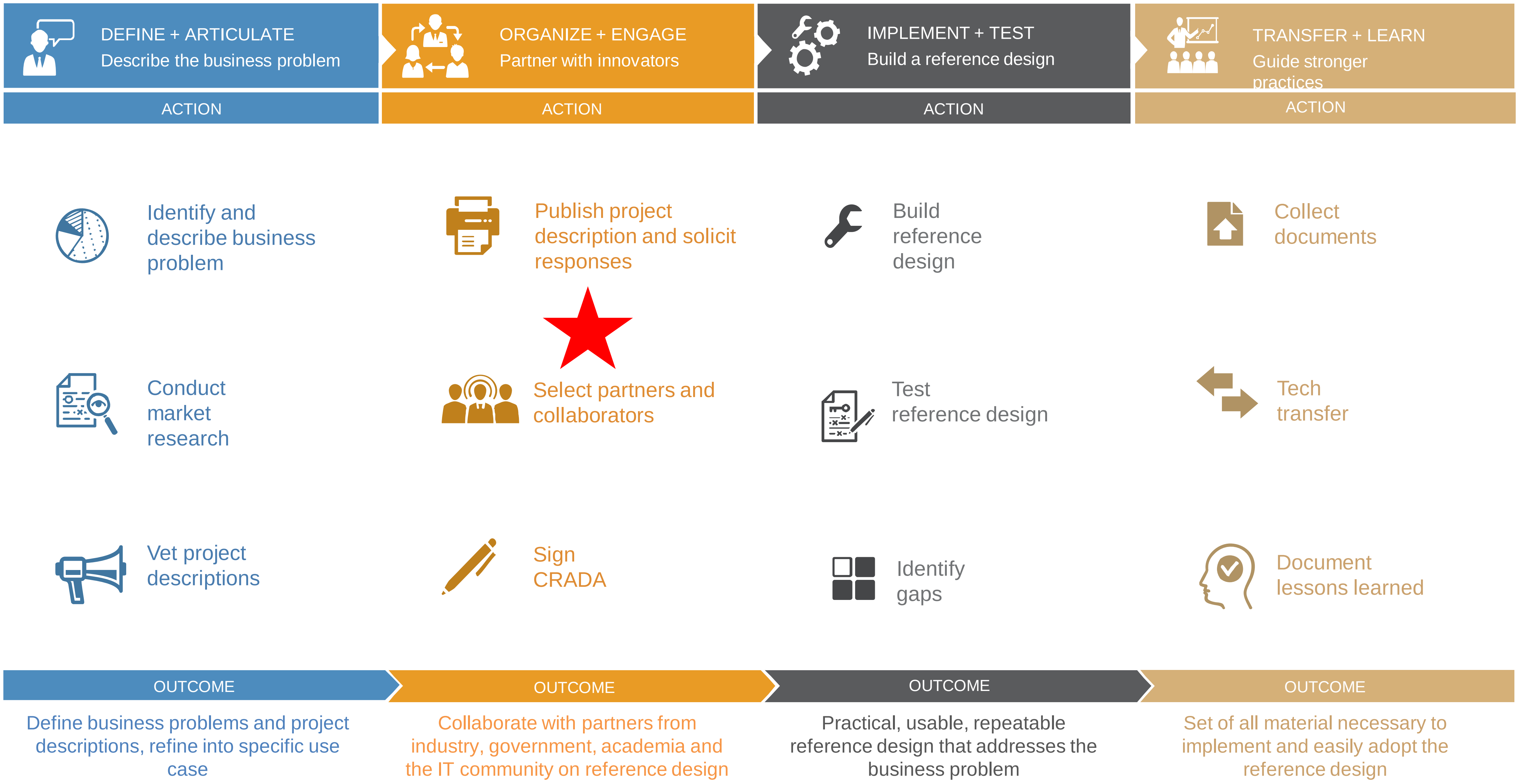
AGENDA

12:00 PM	Introductions & Overview of NCCoE Retail Sector project: *Multifactor Authentication for e-Commerce*	10 min
12:10 PM	Introduction of Paul Grassi	5 min
12:15 PM	Deep dive by Paul Grassi into NIST Special Publication 800-63-3 Draft	35 min
12:50 PM	MFA architecture overview and where to find additional information	5 min
12:55 PM	Open Q&A/Next Steps	5 min

MULTIFACTOR AUTHENTICATION FOR E-COMMERCE TRANSACTIONS

- Retailers note that EMV implementation will shift fraud to card-not-present (CNP) transactions
- Retailers have noted that secure CNP transactions will become more critical but hard for them to solve challenges due to competing business priorities
- Reference design to take into account need for frictionless consumer purchasing while ensuring strong authentication
- Scope may include the implementation of run-time risk calculation, web analytics, and multifactor authentication mechanisms during e-commerce transactions for a known consumer of a laboratory simulated retailer website.

ENGAGEMENT & BUSINESS MODEL



DEFINE + ARTICULATE
Describe the business problem

ACTION

- Identify and describe business problem
- Conduct market research
- Vet project descriptions

OUTCOME

Define business problems and project descriptions, refine into specific use case

ORGANIZE + ENGAGE
Partner with innovators

ACTION

- Publish project description and solicit responses
- Select partners and collaborators
- Sign CRADA

OUTCOME

Collaborate with partners from industry, government, academia and the IT community on reference design

IMPLEMENT + TEST
Build a reference design

ACTION

- Build reference design
- Test reference design
- Identify gaps

OUTCOME

Practical, usable, repeatable reference design that addresses the business problem

TRANSFER + LEARN
Guide stronger practices

ACTION

- Collect documents
- Tech transfer
- Document lessons learned

OUTCOME

Set of all material necessary to implement and easily adopt the reference design

800-63-3 DIGITAL AUTHENTICATION GUIDELINE

- **Paul A. Grassi:** Senior Standards and Technology Advisor, National Institute of Standards and Technology (NIST)

- NIST Special Publication 800-63-3 Digital Authentication Guideline: https://pages.nist.gov/800-63-3/

- From 800-63-3's Executive Summary:
  - *The suite of SP 800-63-3 documents provides technical guidelines to agencies to allow an individual to authenticate his or her identity to a Federal digital service. This document may inform but does not restrict or constrain the development or use of standards for application outside of the Federal government, such as e-commerce transactions. These guidelines address only traditional, widely implemented methods for digital authentication, based on secrets. With these methods, the individual to be authenticated proves that he or she knows or possesses a valid authenticator or combination of authenticators.*

- Submit 800-63-3 comments at: https://github.com/usnistgov/800-63-3/issues/

Draft Special Publication 800-63-3

Digital Authentication Guideline

(formerly known as Electronic Authentication Guideline)

SP 800-63-3
Digital Authentication Guideline

SP 800-63A
Identity Proofing & Enrollment

SP 800-63B
Authentication & Lifecycle Management

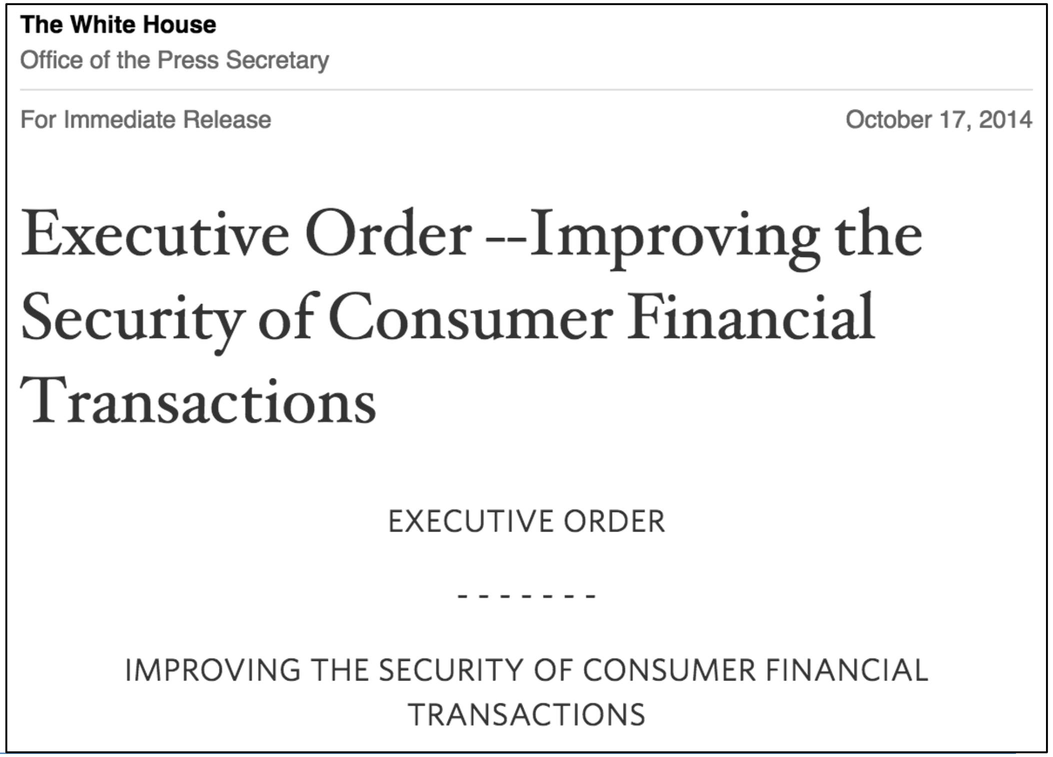
SP 800-63C
Federation & Assertions

https://pages.nist.gov/800-63-3

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

Why the update?

- Implement Executive Order 13681: *Improving the Security of Consumer Financial Transactions*
- Align with market and promote (adapt to) innovation
- Simplify and provide clearer guidance
- International alignment



The White House

Office of the Press Secretary

For Immediate Release October 17, 2014

Executive Order --Improving the Security of Consumer Financial Transactions

EXECUTIVE ORDER

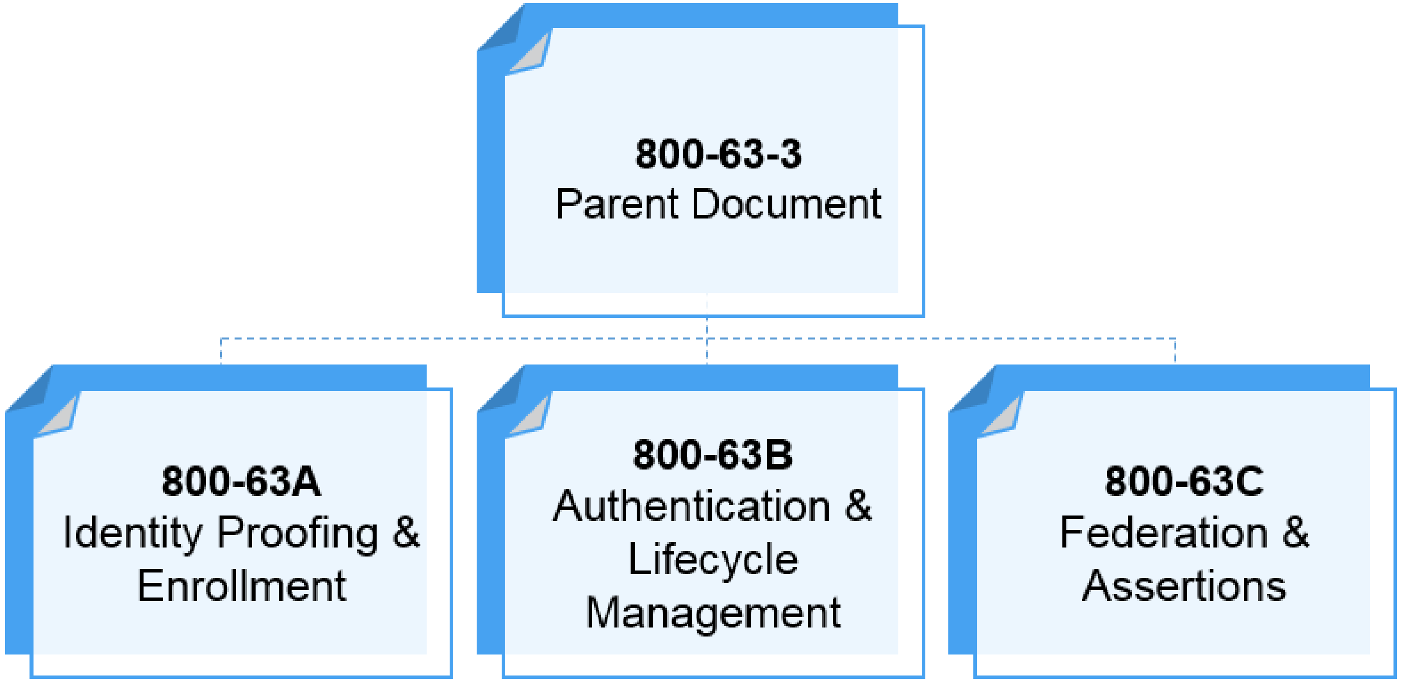
- - - - - - -

IMPROVING THE SECURITY OF CONSUMER FINANCIAL TRANSACTIONS

SP 800-63-3

Digital Authentication Guideline

Making 800-63 More Accessible



800-63-3
Parent Document

800-63A
Identity Proofing & Enrollment

800-63B
Authentication & Lifecycle Management

800-63C
Federation & Assertions

User Experience Considerations

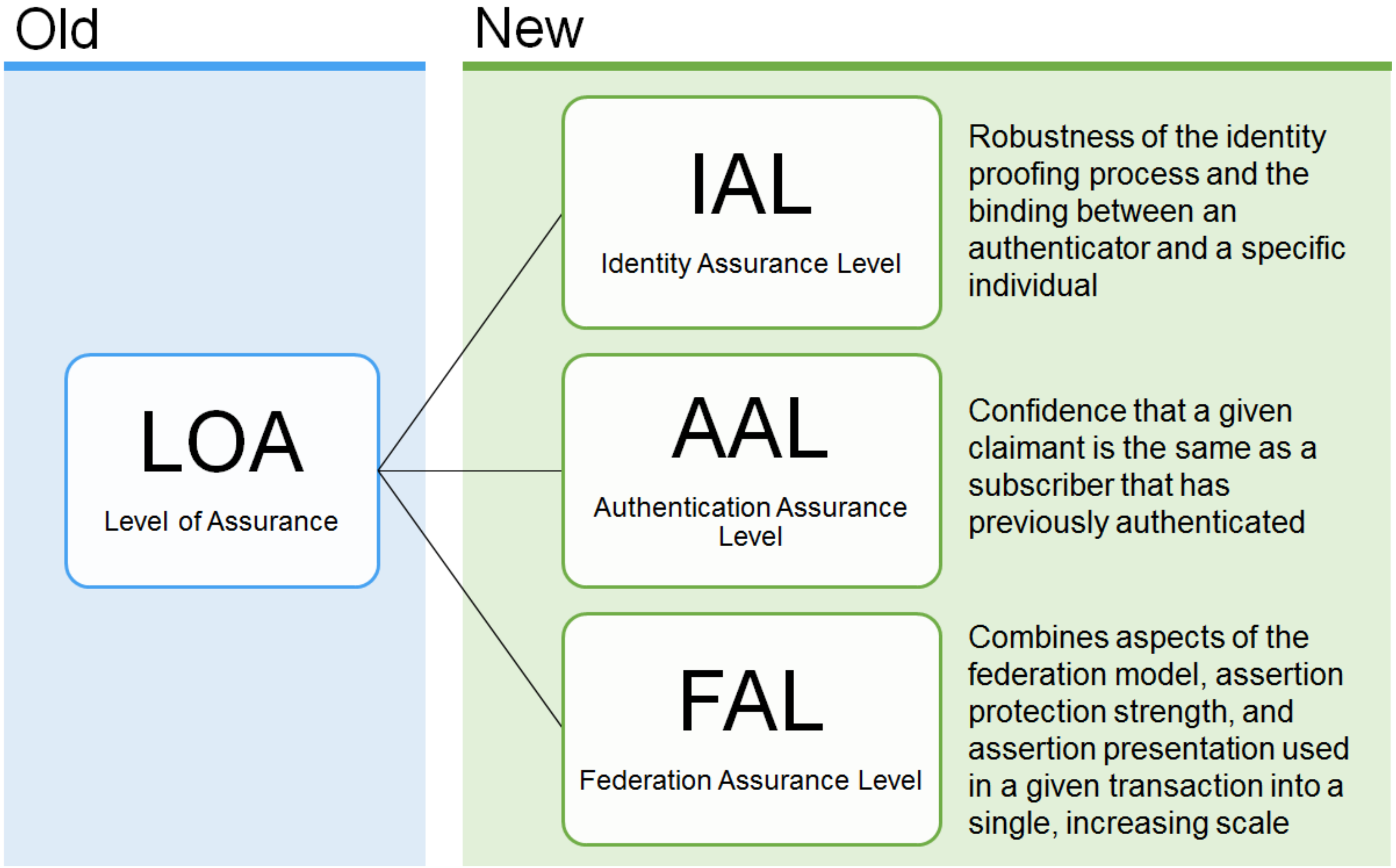
Privacy Requirements & Considerations

Streamlined Content & Normative Language

Reference to Previous Versions of 800-63

800-63-2	New
Sections 1 – 4	800-63-3
Section 5	800-63A
Sections 6 – 8	800-63B
Section 9	800-63C

New Model



Robustness of the identity proofing process and the binding between an authenticator and a specific individual

Confidence that a given claimant is the same as a subscriber that has previously authenticated

Combines aspects of the federation model, assertion protection strength, and assertion presentation used in a given transaction into a single, increasing scale

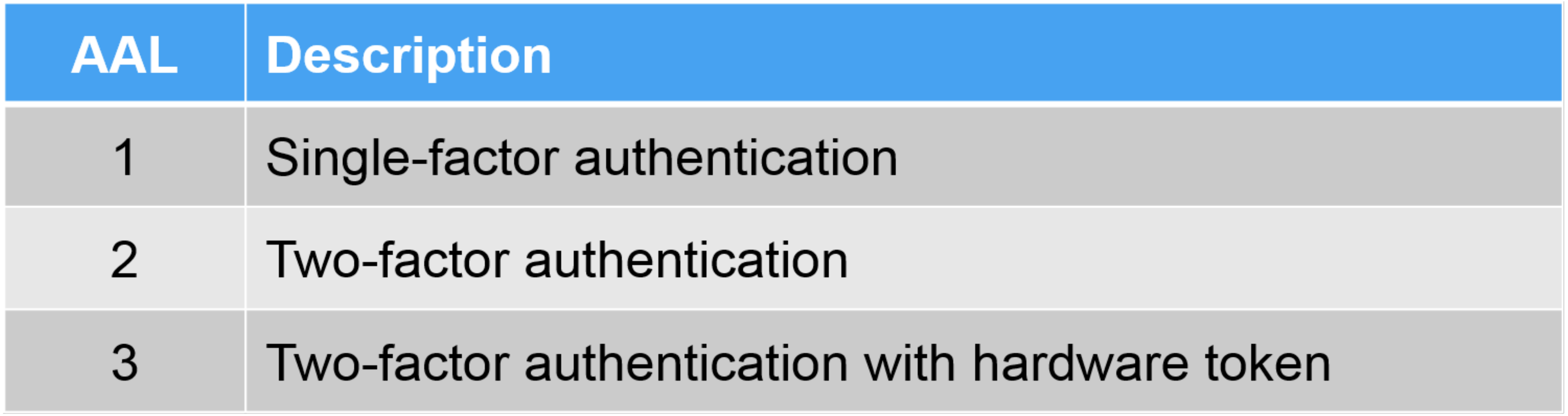
Identity Assurance Levels (IALs)

Refers to the robustness of the identity proofing process and the binding between an authenticator and a specific individual

IAL	Description
1	Self-asserted attribute(s) – 0 to n attributes
2	Remotely identity proofed
3	In-person identity proofed

Authenticator Assurance Levels (AALs)

Describes the robustness of confidence that a given claimant is the same as a subscriber that has previously authenticated



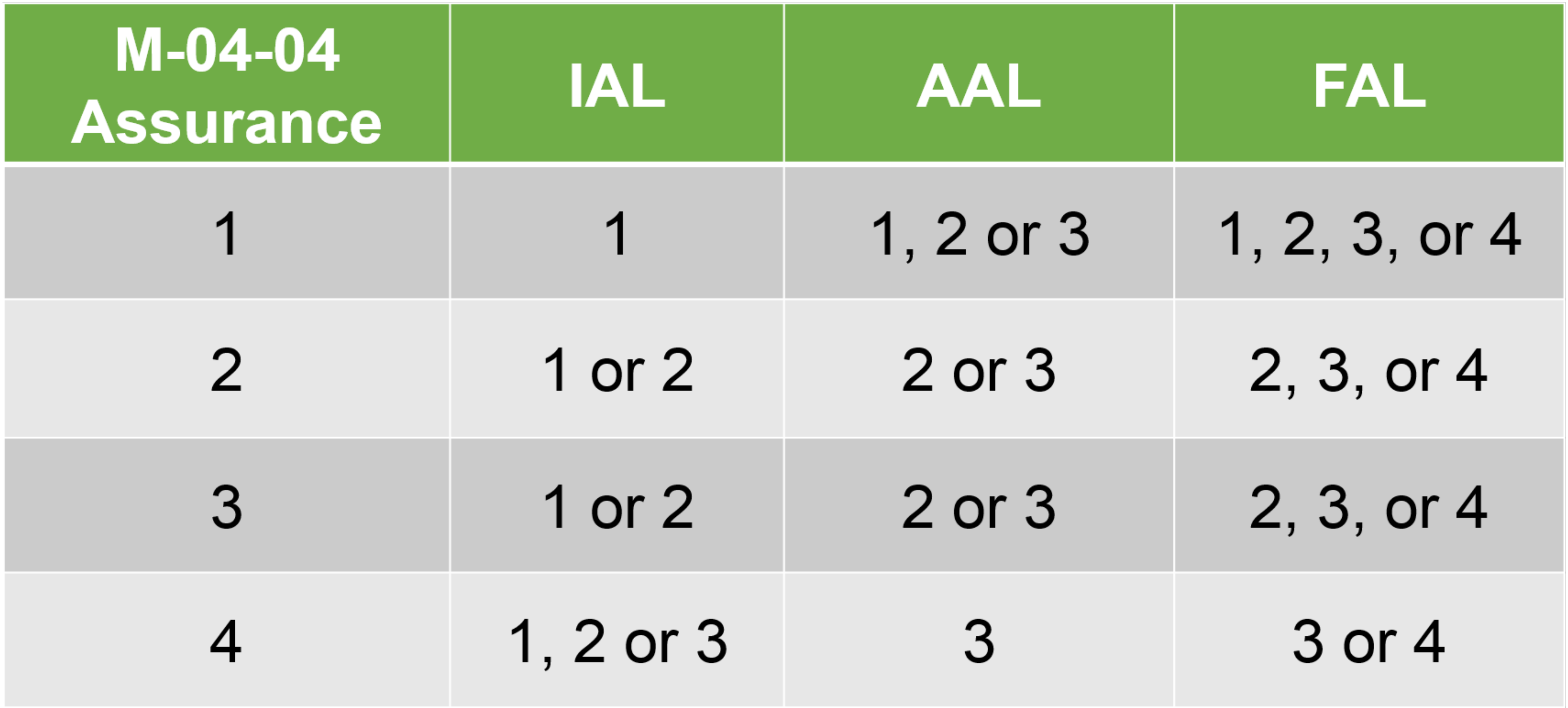
AAL	Description
1	Single-factor authentication
2	Two-factor authentication
3	Two-factor authentication with hardware token

Federation Assurance Levels (FALs)

Combines aspects of the federation model, assertion protection strength, and assertion presentation used in a given transaction into a single, increasing scale

FAL	Direct Presentation Requirement	Indirect Presentation Requirement
1	Bearer assertion, asymmetrically signed by CSP	Bearer assertion, asymmetrically signed by CSP
2	Bearer assertion, asymmetrically signed by CSP	Bearer assertion, asymmetrically signed by CSP and encrypted to RP
3	Bearer assertion, asymmetrically signed by CSP and encrypted to RP	Bearer assertion, asymmetrically signed by CSP and encrypted to RP
4	Holder of key assertion, asymmetrically signed by CSP and encrypted to RP	Holder of key assertion, asymmetrically signed by CSP and encrypted to RP

Digital Services Today



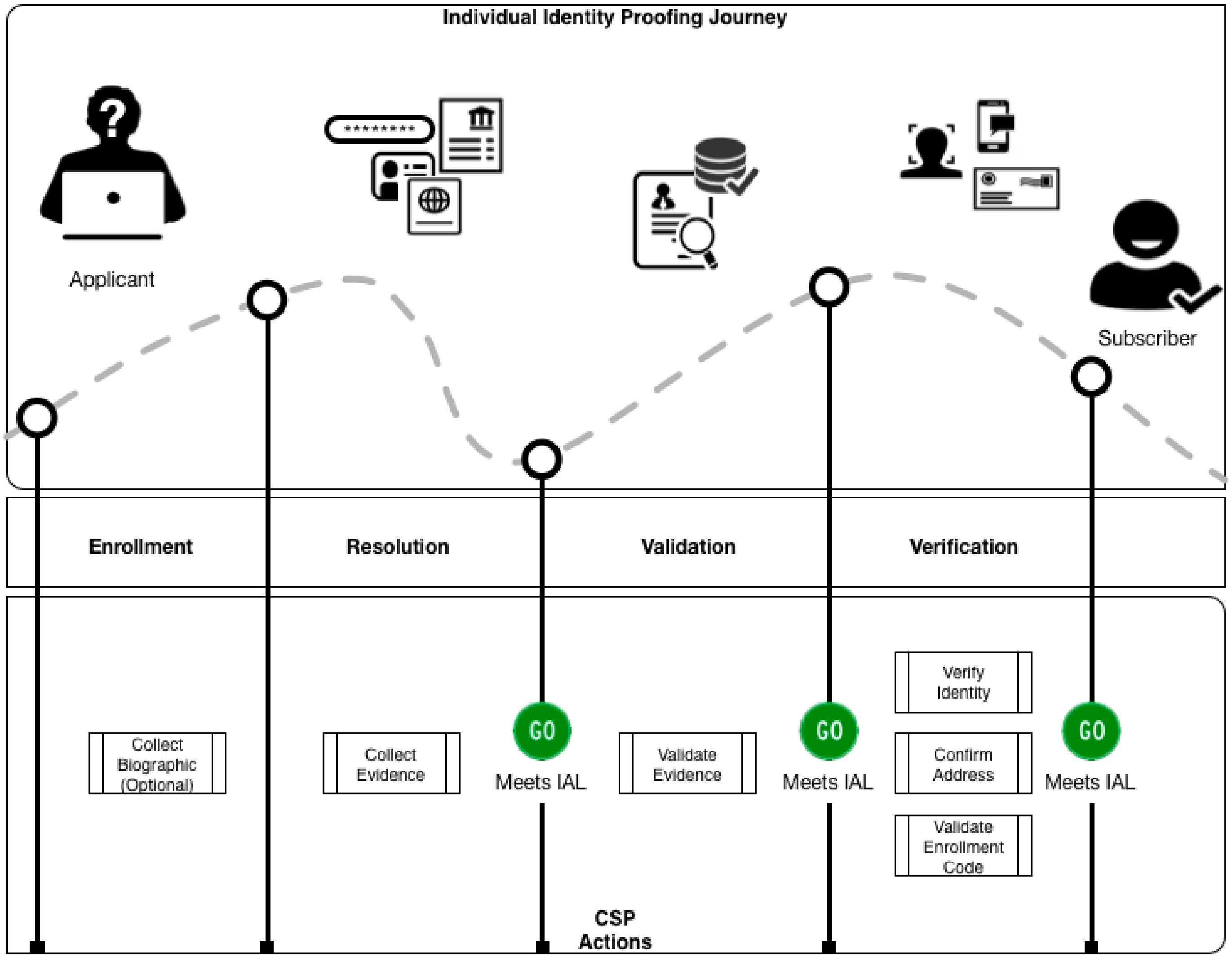
M-04-04 Assurance	IAL	AAL	FAL
1	1	1, 2 or 3	1, 2, 3, or 4
2	1 or 2	2 or 3	2, 3, or 4
3	1 or 2	2 or 3	2, 3, or 4
4	1, 2 or 3	3	3 or 4

Choose Your Own 'xAL' Adventure

SP 800-63A

Identity Proofing & Enrollment

A Stronger Identity Proofing Process



Components of Stronger ID Proofing

- Clarifies methods for resolving an ID to a single person
- Evaluating and determining the strength of presented evidence
  - Unacceptable, Weak, Adequate, Strong, Superior
- Moves away from a static list of acceptable documents and increases options for combining evidence to achieve the desired assurance level
- Visual inspection no longer satisfactory at higher IAL
- TFS-related requirements are gone
- Reduced document requirements in some instances
- Clearer rules on address confirmation

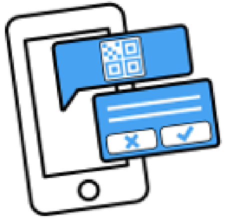
SP 800-63B

Authentication & Lifecycle Management

Authenticators

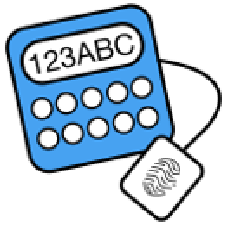
Memorized Secrets

Look-up Secrets



Out-of-Band Devices

Single Factor OTP Device



Multi-Factor OTP Devices

Single Factor Cryptographic Devices

Multi-Factor Cryptographic Software

Multi-Factor Cryptographic Devices

Password Guidance Changes

- Same requirements regardless of AAL
- SHALL be minimum of 8 characters.
- SHOULD (with heavy leaning to SHALL) be:
  - Any allowable unicode character
  - 64 characters or more
  - No composition rules
  - Won’t expire
  - Dictionary rules
- SHALL - Storage guidance to deter offline attack (salt, hash, HMAC)

AUTHENTICATOR GUIDANCE CHANGES

“Token” is out
“Authenticator” is in ✓

Server side biometric matching is in ✓

OTP via SMS is deprecated ⇥

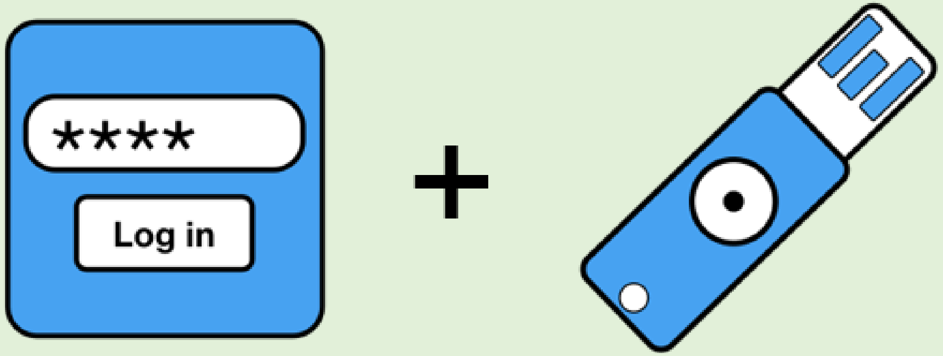
OTP via email is out ✗

Pre-registered knowledge tokens are out ✗

New Authenticator at AAL3

Single Factor Cryptographic Device
+ Memorized Secret Token

Example



SP 800-63C

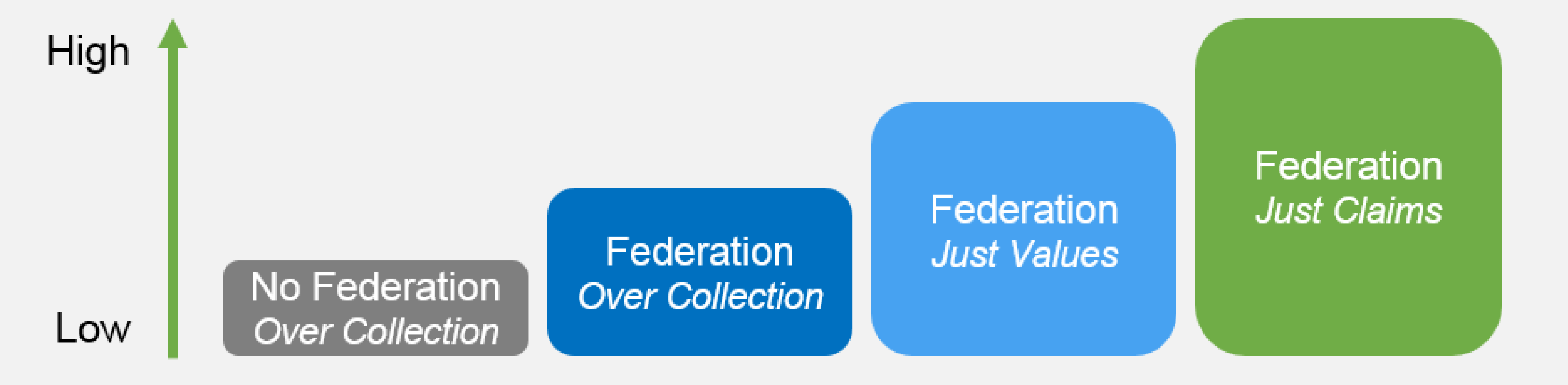
Federation & Assertions

800-63-C
Federation & Assertions

1. Discusses multiple models & privacy impacts & requirements
2. Many SHOULDs – document needs to be agnostic
3. Modernized to include OpenID Connect
4. Clarifies Holder of Key (HOK) for the new AAL 3
5. Attribute requirements

Attribute Claims vs. Values

Maturity Model



High

Low

No Federation *Over Collection*

Federation *Over Collection*

Federation *Just Values*

Federation *Just Claims*

Old

Give me date of birth. →

Give me full address. →

New

I just need to know if they are older than 18.

I just need to know if they are in congressional district X.

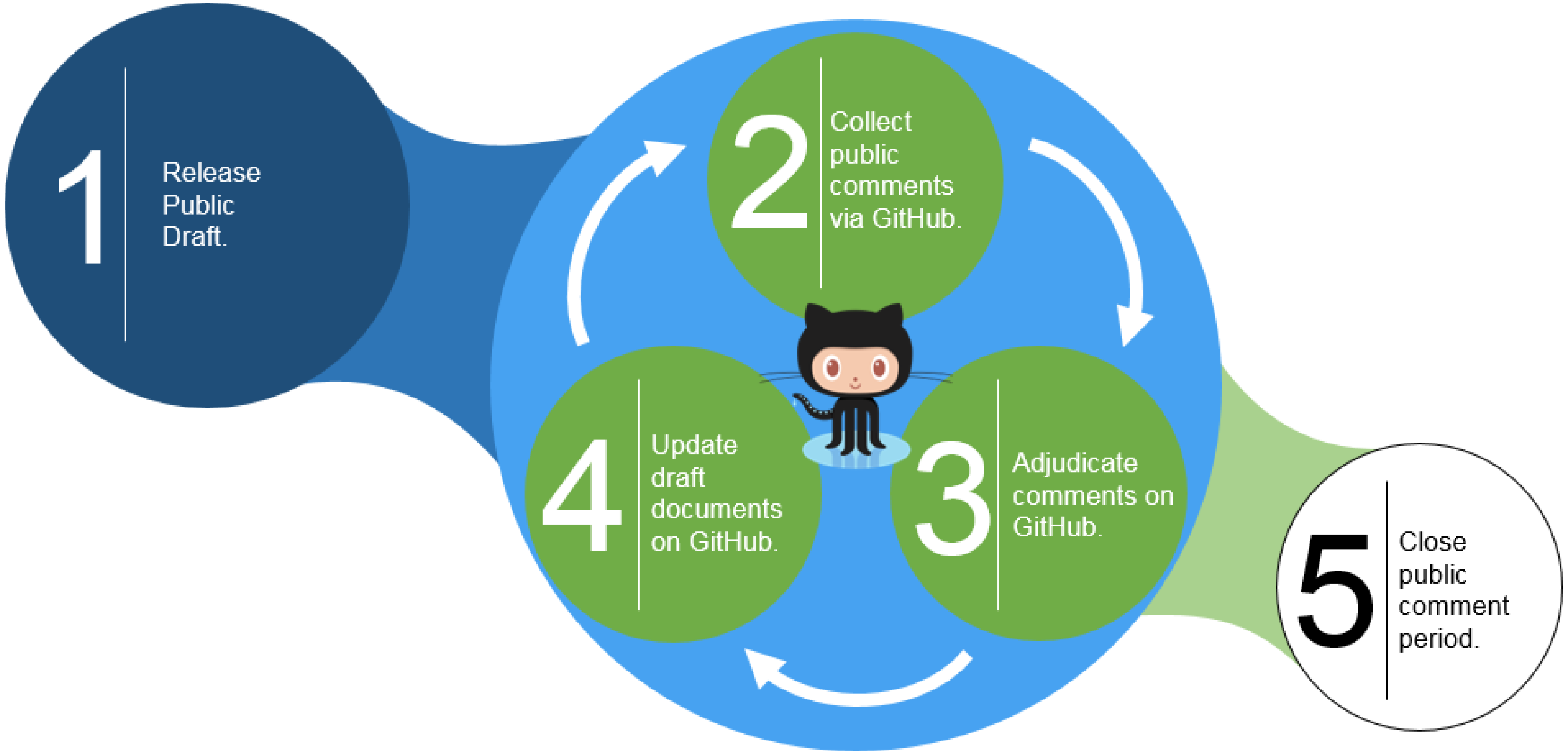
New Requirements

CSP SHALL support claims and value API

RP SHOULD request claims

Retaining the New Development Approach

Iterative – publish, comment, and update in a series of drafting sprints



1 Release Public Draft.

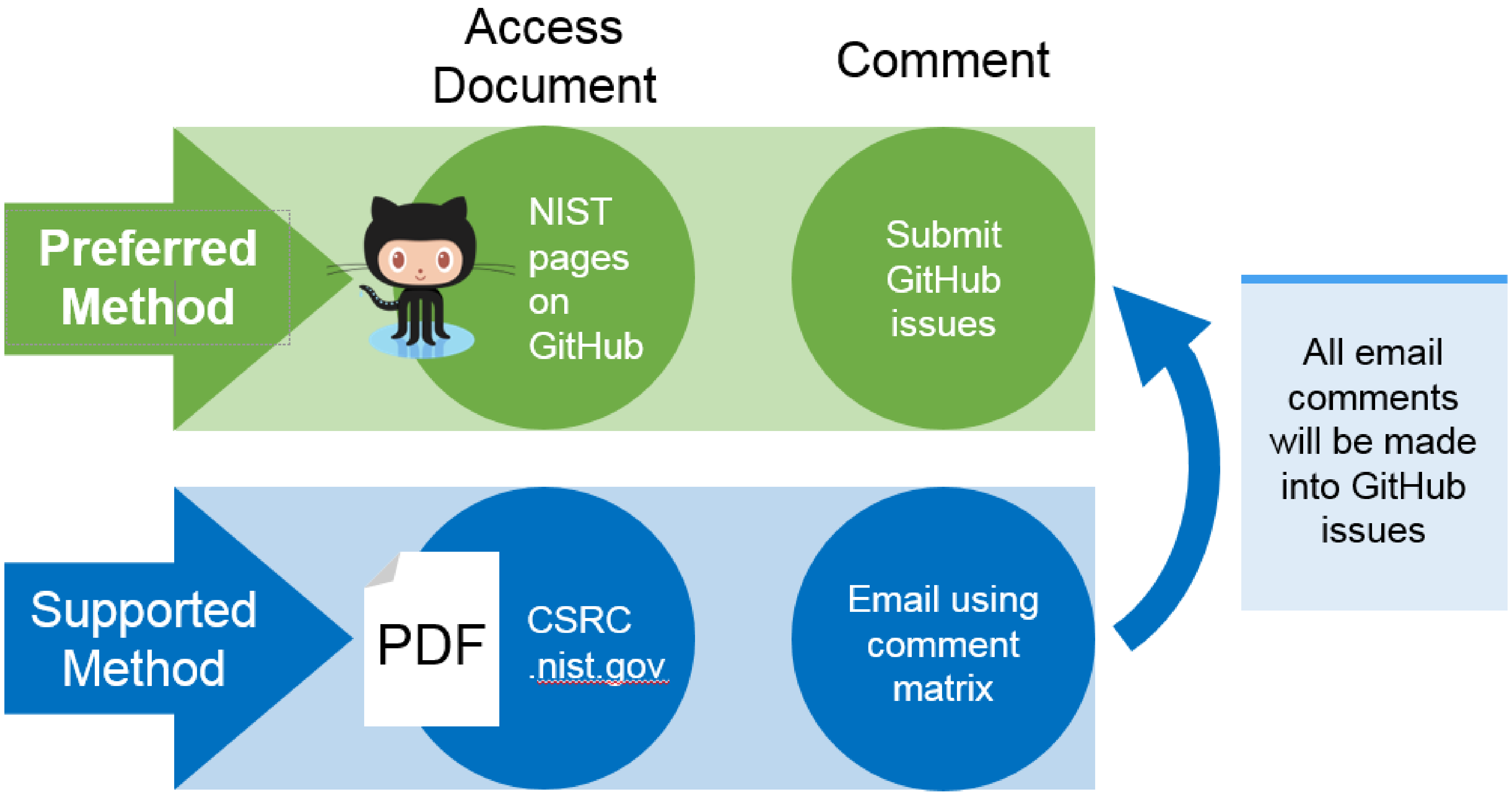
2 Collect public comments via GitHub.

3 Adjudicate comments on GitHub.

4 Update draft documents on GitHub.

5 Close public comment period.

Contributing During Public Comment



Access Document

Comment

Preferred Method

NIST pages on GitHub

Submit GitHub issues

Supported Method

PDF

CSRC .nist.gov

Email using comment matrix

All email comments will be made into GitHub issues

What's Next

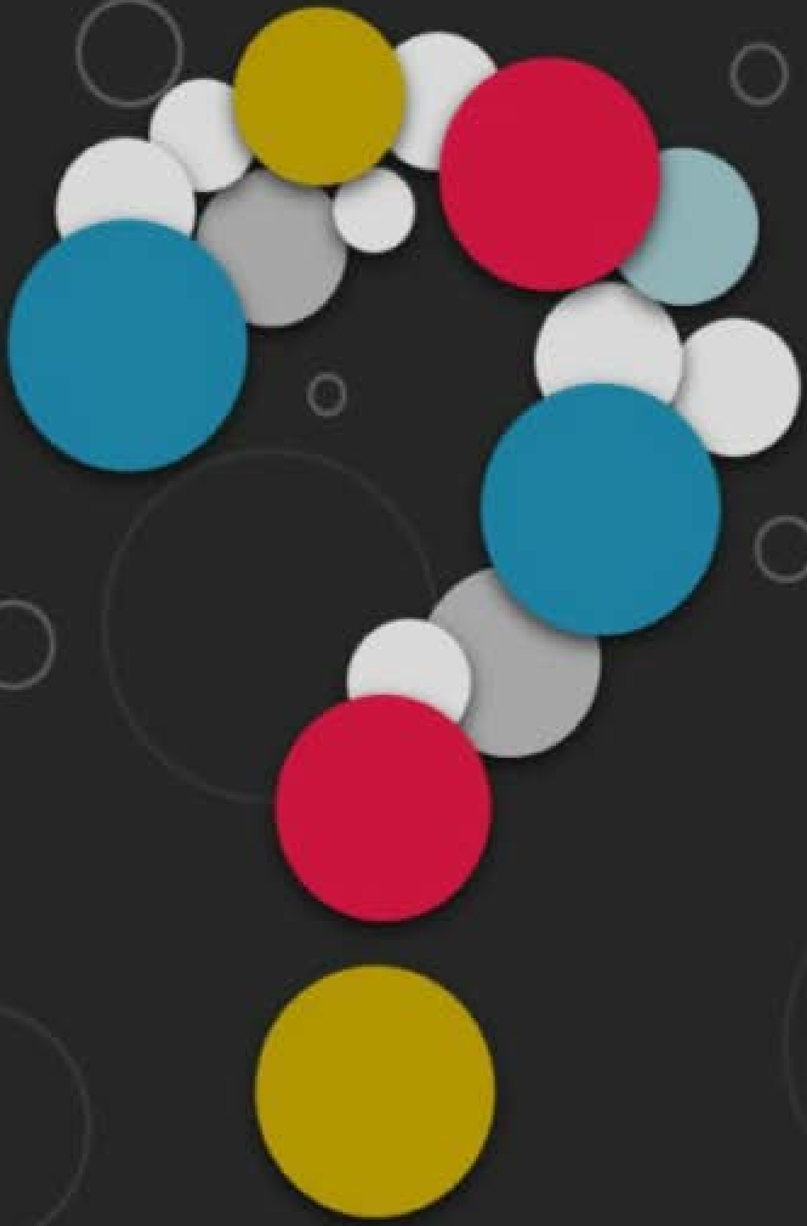
Public Draft Comment Period

opens ~**October 13, 2016**
closes **+60 days**

Final Document

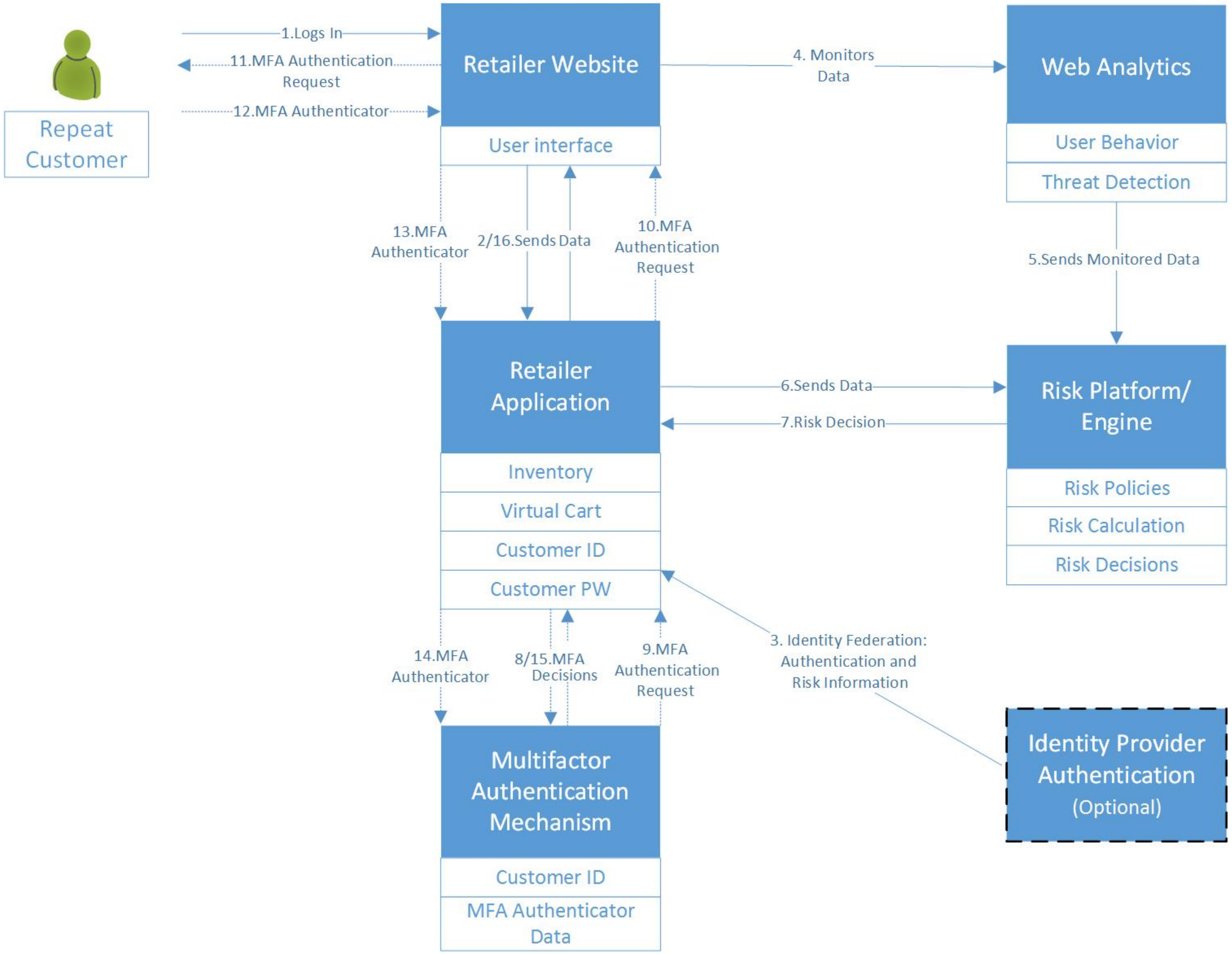
expected **Q2 FY17**

Questions



Multifactor Authentication

MULTIFACTOR AUTHENTICATION DRAFT ARCHITECTURE OVERVIEW

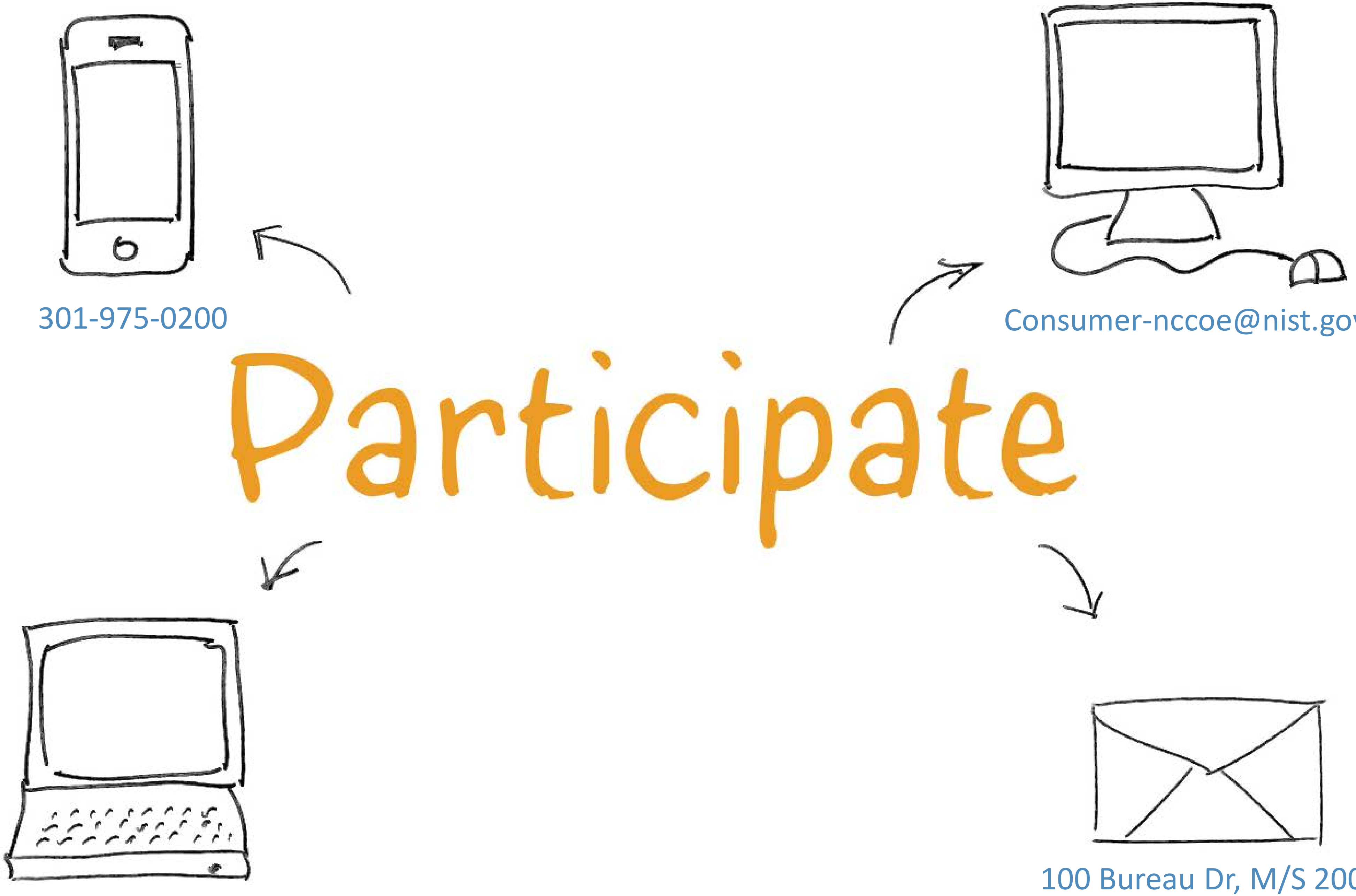


Multifactor Authentication Technology in Retail Environments

- We think that MFA should be part of a system of multiple solutions necessary to successfully reduce e-commerce fraud. What other fraud solutions are available now, and how would MFA fit into your existing anti-fraud paradigms for online retail?
- For retailers, the user’s online shopping experience must not be impeded by additional security mechanisms. With that in mind, where in the lifecycle of an e-commerce transaction would you consider it reasonable to include an MFA mechanism?
- Which types/forms of MFA mechanisms would be realistic to implement?
- Are there significant differences in multifactor authentication for ecommerce transaction architectures depending on the incorporation of Cloud or On-Premise technologies?

Retail Standards

- We are aware of National Retail Federation’s ARTS standards board, NIST, ISO, and PCI standards that may apply and or concern retailers in implementing their systems and system security. Are there other standards we should be aware of and apply to our projects?



Participate

301-975-0200

Consumer-nccoe@nist.gov

http://nccoe.nist.gov

100 Bureau Dr, M/S 2002
Gaithersburg, MD 20899