PROJECT DESCRIPTION

MOBILE APPLICATION SINGLE SIGN-ON

For Public Safety and First Responders

Paul Grassi
NIST Applied Cybersecurity Division

William Fisher
NIST National Cybersecurity Center of Excellence

FINAL DRAFT
November 2016
PSFR-NCCoE@nist.gov

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

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build integrated, open, end-to-end reference designs that are broadly applicable and repeatable. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes a particular problem that is relevant across the Public Safety and First Responder sector. NCCoE cybersecurity experts will address this challenge through collaboration with members of the Public Safety and First Responder community and vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be used by Public Safety and First Responder organizations.

Abstract

Mobile platforms offer a significant operational advantage to public safety stakeholders by giving them access to mission critical information and services while deployed in the field, during training and exercises, or participating in day-to-day business and preparations during non-emergency periods. However, these advantages can be limited if unnecessary or complex authentication requirements stand in the way of an official providing emergency services, especially when any delay – even seconds – is a matter of containing or exacerbating an emergency situation. The vast diversity of public safety personnel, missions, and operational environments magnifies the need for a nimble authentication solution for public safety. This project will explore various multifactor authenticators currently in use by the public safety community, or those potentially offered in the future as their next generation networks are brought online. The effort will not only build an interoperable solution that can accept various authenticators to speed access to online systems while maintaining an appropriate amount of security, but will also focus on delivering single sign-on (SSO) capabilities to both native and web/browser-based apps. It is not enough to have an authenticator that is easy to use; this project sets out to identify technical options for the public safety community to consider deploying to ensure individuals in the field are not kept from meeting their mission goals by unnecessary authentication prompts. This project will result in a freely available NIST Cybersecurity Practice Guide, detailing the technical decisions, trade-offs, lessons learned, and implementation instructions based on market-dominant standards, such that public safety organizations can accelerate the deployment of a range of mobile authentication and SSO services to their population of users.

Keywords

authentication; biometric; first responder; mobile authentication; multifactor authentication; native applications; public safety; single sign-on; SSO

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

COMMENTS ON NCCOE DOCUMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

Comments on this publication may be submitted to: PSFR-NCCoE@nist.gov

Table of Contents

1. Executive Summary

Purpose

On-demand access to public safety data is critical to ensuring that public safety and first responder (PSFR) personnel can deliver proper care and support during an emergency. This requirement necessitates that PSFR personnel rely heavily on mobile platforms while in the field, which may be used to access sensitive information such as personally identifiable information (PII), law enforcement sensitive (LES) information, or protected health information (PHI). The vast diversity of public safety personnel, missions, and operational environments presents unique challenges to implementing efficient and secure authentication mechanisms in order to protect access to this sensitive information.

The purpose of this project is to help PSFR personnel efficiently and securely gain access to mission data via mobile devices and applications. This project seeks to demonstrate, using standards-based commercially available and open source products, a reference design for multifactor authentication (MFA) and mobile single sign-on (SSO) for native and web applications. Through this effort, the NCCoE intends to:

- help PSFR entities define requirements for MFA and mobile application SSO
- improve interoperability between mobile platforms, applications, and identity providers (IdPs) regardless of the application development platform used in their construction
- develop an architecture and worked example that PSFR entities can quickly transition to their operational domains

The publication of this Project Description is the beginning of a process that will identify project requirements, scope, participants, and hardware and software components for use in a laboratory environment to build open, standards-based, integrated, end-to-end reference designs that will address the challenge of implementing MFA and mobile application SSO for PSFR organizations. The approach may include architectural definition, logical design, build development, testing and evaluation, and security control mapping. This project will result a publicly available NIST Cybersecurity Practice Guide that will help PSFR organizations implement multifactor authentication and mobile application SSO in their own environments.

Scope

The scope of this example solution includes the ability to authenticate to public safety applications via the implementation of MFA to widely adopted commercially available mobile platforms. This effort will then demonstrate subsequent authentications to multiple mobile applications leveraging the initial authentication to accomplish SSO capabilities. As technology and resources allow, this project may also demonstrate application-to-application data sharing through the use of rights delegation platforms. This project will leverage commercially available and open source technology that can be employed for enterprise use. Any demonstration leveraging custom and/or proprietary technology implementations is out of scope for this effort.

Assumptions

The following assumptions will help shape the scope of the mobile SSO solution and provide controlled parameters for the effort such that the focus is centered on delivering a successful solution based closely on the operational environment of public safety officials.

- An inclusive list of possible credentials will not be used; however multiple types will be employed to ensure that the SSO solution can interoperate with a range of possible authentication standards relevant for first responders. The credential standards that will be considered in this use case are as follows:
    - X.509 certificates, with the corresponding private key preferably stored in a hardware-based keystore in the mobile device, according to NIST SP 800-164
    - FIDO UAF 1.x specifications, leveraging a biometric as one factor
    - FIDO U2F 1.x specifications for hardware authenticators, inclusive of authenticators using standard interfaces such as USB, NFC, or BLE
    - password and application based OTP
- The project will select the mobile platforms with the richest native and open capabilities to enable SSO.
- Identity proofing and access control is not in scope. The solution will create synthetic digital identities that represent the identities and attributes of public safety personnel in order to test authentication assertions. This includes the usage of a lab-configured identity repository—not a genuine repository and schema provided by any public safety organization.
- Credential storage is not in scope. For example, this use case is not impacted by the storage of a certificate in software versus hardware, such as a TPM.
- Enterprise mobile management (EMM) is not in scope, though the potential impact and benefits of including EMM will be considered. The solution will assume all applications involved in the SSO experience are allowable via an EMM.

Challenges

This use case was selected explicitly because of the associated challenges of developing an interoperable, secure, user-friendly SSO solution that can be leveraged by first responders in emergencies as well as in day-to-day operations. The scenarios described herein will directly address these challenges such that public safety entities choosing to deploy a solution based on this architecture can feel comfortable that the computing and operational challenges of mobile authentication and information access are accounted for in their selected solution. However, the challenges listed below are specific to the lab environment in which this solution will be deployed, and should be mitigated to provide maximum positive impact to this important sector:

- shared devices and variable operating system (OS) support for multiple identities per device
- lab access to live test instances of actual public safety applications, both native and web-based
- immature and unstable standards for mobile identity and SSO
- multiple credential standards, such as Fast Identity Online (FIDO), PKI certificates, and varying mobile OS support for each

Background

Mobile devices have become critical to the operational effectiveness of public safety institutions. They have the potential to enable essential personnel to be more effective and efficient in responding to emergency situations, which can ultimately help PSFR personnel save more lives. The widespread adoption of mobile devices has led to a spate of mobile applications, many of which can support public safety activities. However, as described in Draft NISTIR 8080, *Usability and Security Considerations for Public Safety Mobile Authentication,* "most commercial off-the-shelf (COTS) mobile devices and applications are not designed with public safety and their unique constraints in mind." More specifically, the document cites, "authenticating to a device, service, or application … can be quite a challenging task when wearing thick gloves and donning a protective mask." [1]

When responding to an emergency, public safety personnel require on-demand access to data. The ability to authenticate quickly and securely in order to access public safety data is critical to ensuring that first responders can deliver proper care and support during an emergency. In order to adequately meet the needs of diverse public safety personnel, missions, and operational environments, authentication mechanisms need to support deployments where devices may be shared amongst personnel and authentication factors have usability constraints.

2. Scenarios

Scenario 1: MFA and Mobile SSO for Native Applications

Multiple mobile devices and OS platforms will be configured to accept the authenticators listed in the assumptions section. Each authenticator will be associated with the same digital identity. The user will access three (3) native applications. The first accessed will trigger a prompt for a valid credential, and the subsequent two will incorporate, if possible, multiple SSO techniques dependent on the standards, OS capabilities, and technologies selected. The application selection sequence will not be fixed, i.e., any application can be selected first, with the remaining two accepting an SSO-based authentication. This scenario will also explore the impact of various session length policies on a per-application basis, as well as the impact of the mobile device being locked by the user or based on a pre-configured OS timeout.

Scenario 2: MFA and Mobile SSO for Web Applications

This scenario will build off of scenario 1, and add two additional web-based applications to the SSO workflow. Each application will be accessed via a mobile web browser. Two browsers will be included in the scenario, not just the default OS browser. As in scenario 1, the user will be able to traverse applications in any order they choose, and will be able to access each application after the first authentication challenge without being prompted for his or her credentials.

Scenario 3: Shared Devices

Adding to the complexity of the previous two scenarios, this scenario will focus on a situation where two or more colleagues share a single mobile device in order to accomplish a mission. The credentials used in scenarios 1 and 2 will be included, but will be associated to multiple digital identities. This scenario will explore situations in which multiple or no profiles are installed on a device, potentially requiring the user to log out prior to giving the device to another user.

Scenario 4: Single Log Out (stretch goal)

In order to ensure only authorized personnel get access to application resources, users must be logged out from application sessions when access is no longer needed, or a session expires. In a single sign on scenario, a user may need to be logged out from one or many applications at a given time. This scenario will demonstrate architectures for tearing down user sessions, clearly communicating to the user which application(s) have active sessions and ensuring active session are not abandoned.

Scenario 5: App-to-App data sharing (stretch goal)

Many applications may wish to share data resources. For example, a municipal law enforcement organization may want to supplement its mobile application data with information from a national law enforcement fusion center. The municipal mobile application needs delegated authorization to access national law enforcement information. This would require the user to authenticate to the national law enforcement application and consent to allow the municipal application to access fusion center data. The benefit of this architecture is that the user controls data sharing from one application to the next, without providing the fusion center credentials to the municipal app. However, prior to consent of data sharing, the user must authenticate. This scenario will add SSO to the authorization and consent required for this type of data sharing workflow.

Scenario 6: Step-up Authentication (stretch goal)

A user will access applications using an acceptable, but low assurance, authenticator. Upon requesting access to an application that requires higher assurance, the user will be prompted for an additional authentication factor. Determinations on whether to step up may be based on risk relevant data points collected by the IdP at the time of authentication, referred to as the authentication context.

3. Architecture

High Level Architecture

Figure 1 illustrates a high-level representation of components and protocols that may achieve the desired capabilities.

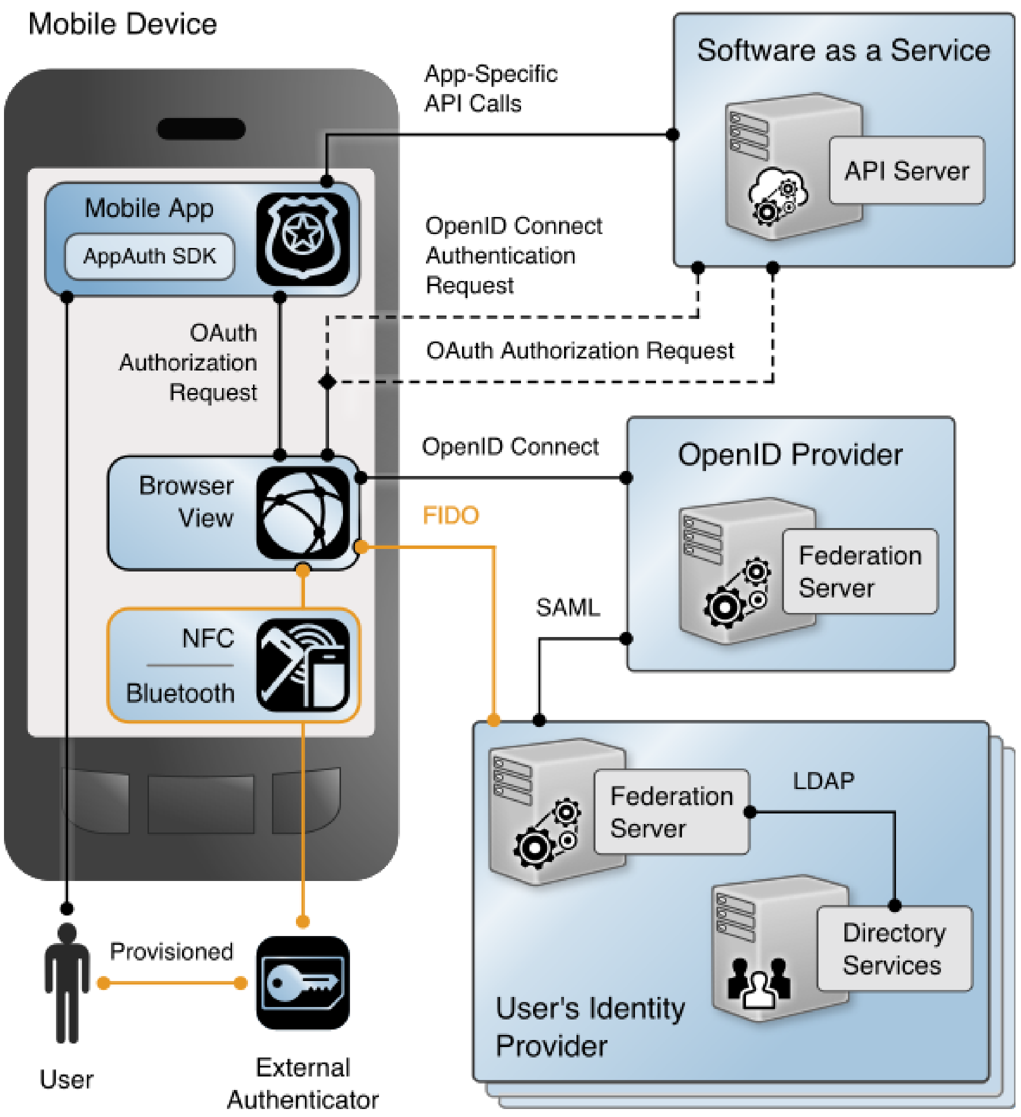
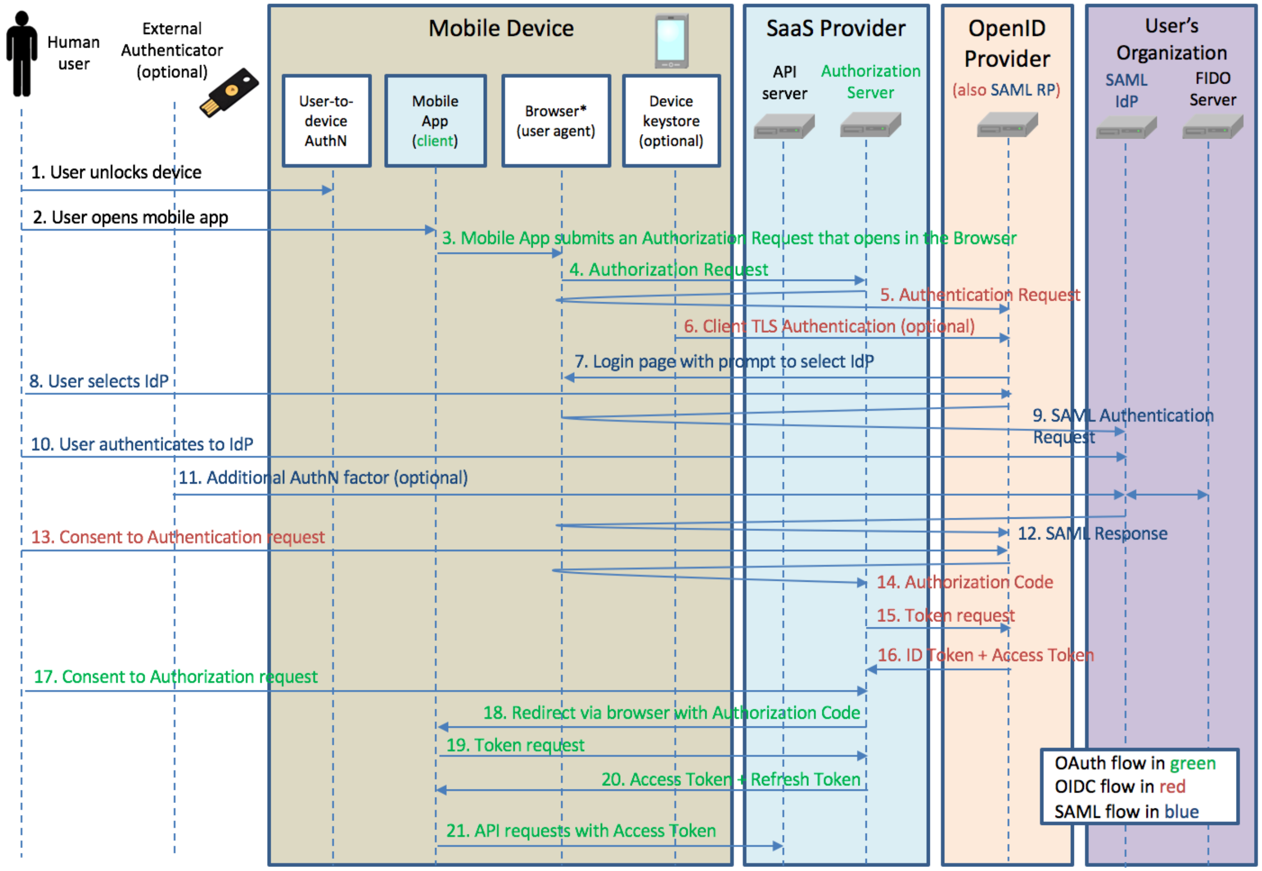


Figure 1 High Level Architecture

Architecture Flow Diagrams

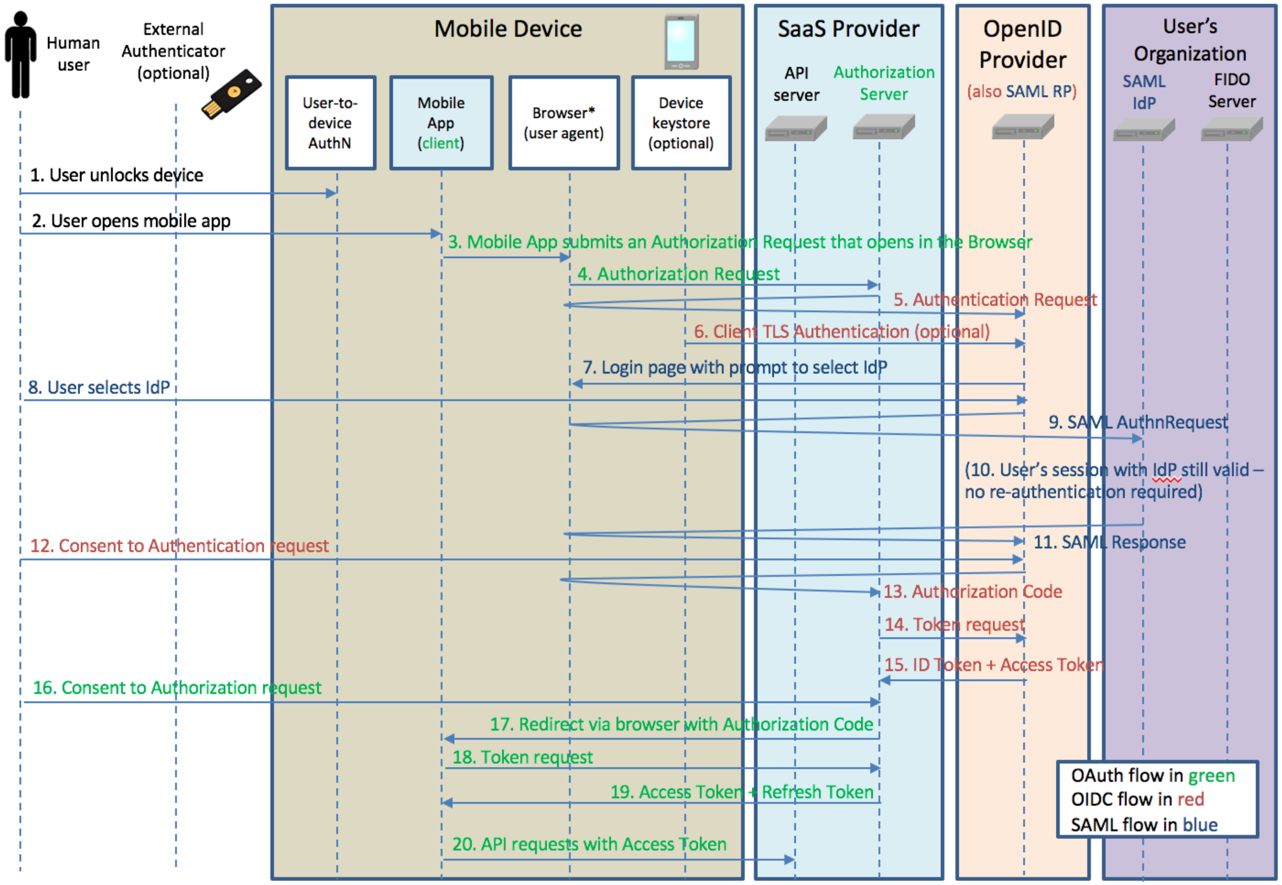
Figure 2 details one potential initial flow between architectural components, depicting the user performing multifactor authentication to a mobile application.


Human user
External Authenticator (optional)
Mobile Device
User-to-device AuthN
Mobile App (client)
Browser* (user agent)
Device keystore (optional)
SaaS Provider
API server
Authorization Server
OpenID Provider
(also SAML RP)
User’s Organization
SAML IdP
FIDO Server
1. User unlocks device
2. User opens mobile app
3. Mobile App submits an Authorization Request that opens in the Browser
4. Authorization Request
5. Authentication Request
6. Client TLS Authentication (optional)
7. Login page with prompt to select IdP
8. User selects IdP
9. SAML Authentication Request
10. User authenticates to IdP
11. Additional AuthN factor (optional)
12. SAML Response
13. Consent to Authentication request
14. Authorization Code
15. Token request
16. ID Token + Access Token
17. Consent to Authorization request
18. Redirect via browser with Authorization Code
19. Token request
20. Access Token + Refresh Token
21. API requests with Access Token
OAuth flow in green
OIDC flow in red
SAML flow in blue

* System browser or other user agent as specified in IETF “OAuth 2.0 for Native Apps” internet-draft (e.g., Chrome custom tab)

Figure 2 Initial Application Authentication

Continuing the flow in Figure 2, Figure 3 shows a user leveraging the initial authentication to sign into additional mobile applications.


Human user
External Authenticator (optional)
Mobile Device
User-to-device AuthN
Mobile App (client)
Browser* (user agent)
Device keystore (optional)
SaaS Provider
API server
Authorization Server
OpenID Provider
(also SAML RP)
User's Organization
SAML IdP
FIDO Server
1. User unlocks device
2. User opens mobile app
3. Mobile App submits an Authorization Request that opens in the Browser
4. Authorization Request
5. Authentication Request
6. Client TLS Authentication (optional)
7. Login page with prompt to select IdP
8. User selects IdP
9. SAML AuthnRequest
(10. User's session with IdP still valid – no re-authentication required)
11. SAML Response
12. Consent to Authentication request
13. Authorization Code
14. Token request
15. ID Token + Access Token
16. Consent to Authorization request
17. Redirect via browser with Authorization Code
18. Token request
19. Access Token + Refresh Token
20. API requests with Access Token
OAuth flow in green
OIDC flow in red
SAML flow in blue

* System browser or other user agent as specified in IETF "OAuth 2.0 for Native Apps" internet-draft (e.g., Chrome custom tab)

Figure 3 Single Sign on to Subsequent Application

Component List

- mobile devices with built-in user-to-device authentication capabilities (including biometric) and cryptographic keystores
- mobile web browser application, Identity Provider application, or built-in device capability that manages authentication to the Identity Provider (using protocols such as FIDO UAF, FIDO U2F, or TLS with client certificate authentication) and interfaces with Relying Party applications to enable SSO
- external hardware authenticators that interoperate with mobile devices over Near Field Communication (NFC) or Bluetooth Low Energy (BLE)
- Software Development Kit (SDK), libraries, or platform APIs that enable mobile SSO capabilities within Relying Party mobile applications and their backend servers
- Identity Provider server with OpenID Connect support

Desired Requirements

This project seeks to develop a reference design and implementation that meets the following requirements:

- a standards-based solution architecture that selects the most effective and secure approach to implementing mobile SSO leveraging native capabilities of the mobile OS
- supports mobile SSO both for authentication and, as technology and resources allow, delegated authorization
- ensures that mobile applications do not have access to user credentials
- supports multiple authenticators, taking into account unique environmental constraints faced by first responders in emergency medical services, law enforcement, and the fire service such as:
    - gloved, one-handed, or hands-free operation
    - use of smoke hoods, fire hoods, or gas masks that may prevent facial or iris recognition
    - proximity based authenticators
    - biometric based authentication mechanisms that meet the requirements of NIST SP 800-63r3B
- allows for multi-user operation of shared mobile devices, where each individual has a unique identity on the mobile platform
- supports MFA and multiple authentication protocols
- supports a spectrum of Bring Your Own Device (BYOD) and Corporate Owned, Personally Enabled (COPE) scenarios

4. Relevant Standards and Guidance

Standards-based and open source activities in the mobile application SSO and rights delegation space that may be leveraged for this effort include:

- IETF: The OAuth Working Group has drafted a Best Current Practice (BCP) for mobile application rights delegation demonstrating how OAuth 2.0 authorization requests can be made from native apps using either an "in-app browser tab" or the "system browser" instead of using the “web-view” approach, which is inherently insecure [2].
- OpenID Foundation: The Connect Working Group has developed an open source implementation for OpenID Connect to enable an SSO model for native applications installed on mobile devices [3] [4].
- FIDO Universal Authentication Framework (UAF) [5]
- FIDO Universal 2nd Factor (U2F) [6]
- W3C Web Auth API (FIDO 2.0) [7]
- *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* [8]
- ISO/IEC 30107, *Biometric Presentation Attack Detection* [9]
- ISO/IEC 27001, *Information Technology – Security Techniques – Information Security Management Systems* [10]
- ISO/IEC 29115, *Information Technology – Security Techniques – Entity authentication assurance framework* [11]
- NIST Cybersecurity Framework - Standards, guidelines, and best practices to promote the protection of critical infrastructure [12]
- NIST SP 800-53, *Recommended Security Controls for Federal Information* [13]
- NIST SP 800-63-3, *Electronic Authentication Guide* [14]
- NIST SP 800-73-4, *Interfaces for Personal Identity Verification* (3 Parts) [15]
- Draft NIST SP 800-164, *Guidelines on Hardware Rooted Security in Mobile Devices*
- Draft NISTIR 8080, *Usability and Security Considerations for Public Safety Mobile Authentication*
- NISTIR 8014, *Considerations for Identity Management in Public Safety Mobile Networks*

5. Security Control Map

Table 1 maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the *Framework for Improving Critical Infrastructure Cybersecurity* (CSF) and other NIST activities. This exercise is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

Table 1: Security Control Map

Solution Characteristic	NIST CSF Category	Informative References
local authentication of user to device	PR.AC-4, PR.DS-5	**NIST SP 800-53 Rev. 4** AC-3, IA-6 **IEC/ISO 27002** 6.2.1, 9.3.1, 9.4.1, 9.4.2, 10.1.1
local user authentication to applications	PR.AC-4, PR.DS-5	**NIST SP 800-53 Rev. 4** AC-3, IA-6 **IEC/ISO 27002** 6.2.1, 9.1.1, 9.3.1, 9.4.1, 9.4.2, 10.1.1
remote user authentication	PR.AC-1, PR.AC-4, PR.DS-5	**NIST SP 800-53 Rev. 4** AC-3, AC-17, IA-2, IA-2(2), IA-2(11), IA-6 **IEC/ISO 27002** 6.2.1, 9.1.1, 9.1.2, 9.3.1, 9.4.1, 9.4.2, 10.1.1, 13.1.1, 14.1.3
remote device authentication	PR.AC-1, PR.AC-3, PR.AC-4	**NIST SP 800-53 Rev. 4** AC-3, AC-17, AC-19, IA-3, IA-3(1), IA-3(4) **IEC/ISO 27002** 6.2.1, 9.1.1, 9.4.1, 10.1.1, 13.1.1, 14.1.3
implementation of user and device roles for authorization	PR.AC-4	**NIST SP 800-53 Rev. 4** AC-3, AC-3(7), AC-6 **IEC/ISO 27002** 6.2.1, 9.1.1
device provisioning and enrollment	ID.AM-1, PR.AC-3, PR.PT-1, PR.PT-2, PR.PT-3	**NIST SP 800-53 Rev. 4** AC-19, CM-7(3), CM-8(4), MP-5(3), MP-7(1) **IEC/ISO 27002** 6.2.1, 8.1.2, 8.1.4, 8.2.3, 8.3.1, 8.3.2, 9.2.2, 11.2.5
credential and token storage and use	PR.AC-1	**NIST SP 800-53 Rev. 4** IA-2, IA-2(10), IA-2(11), IA-2(12), IA-5, IA-5(1), IA-5(2), IA-5(4), IA-5(6), IA-5(9), IA-5(10), IA-5(11), IA-5(12), IA-5(13) **IEC/ISO 27002** 9.2.3, 9.2.4, 9.3.1, 9.4.2, 10.1.1, 10.1.2, 14.1.3
shared authentication state across applications on the device	PR.AC-1	**NIST SP 800-53 Rev. 4** IA-5, AC-2 **IEC/ISO 27002** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3
secure inter-process communication methods	PR.DS-5	**NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 **IEC/ISO 27002** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
remote user authentication using multiple factors	PR.AC-1, PR.AC-3, PR.AC-4, PR.DS-5	**NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-4, AC-5, AC-6, AC-16, AC17, AC-19, AC-20, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 **IEC/ISO 27002** A.6.1.2, A.6.2.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5, A.14.1.2, A.14.1.3, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4

remote user authentication using strong cryptography	PR.AC-1, PR.AC-3, PR.AC-4, PR.DS-5	**NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-4, AC-5, AC-6, AC-16, AC17, AC-19, AC-20, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 **IEC/ISO 27002** A.6.1.2, A.6.2.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5, A.14.1.2, A.14.1.3, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4
contextually based authentication decisions	PR.AC-1, PR.AC-3, PR.AC-4, PR.DS-5	**NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-4, AC-5, AC-6, AC-16, AC17, AC-19, AC-20, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 **IEC/ISO 27002** A.6.1.2, A.6.2.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5, A.14.1.2, A.14.1.3, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4
modularized/pluggable authentication methods	PR.DS-5, PR.PT-3	**NIST SP 800-53 Rev. 4** AC-3, CM-7, AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 **IEC/ISO 27002** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
protection of authentication material using a secure context	PR.AC-4, PR.PT-3	**NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16 **IEC/ISO 27002** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
protection of user biometric data	PR.DS-5	**NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 **IEC/ISO 27002** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
proof of user authentication intent	PR.PT-4	**NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7 **IEC/ISO 27002** A.13.1.1, A.13.2.1

Appendix A – References

[1] Y. Choong, J.M. Franklin, and K.K. Greene, *Usability and Security Considerations for Public Safety Mobile Authentication*, DRAFT NISTIR 8080, National Institute of Standards and Technology, Gaithersburg, Maryland, November 2015, 40pp. http://csrc.nist.gov/publications/drafts/nistir-8080/nistir_8080_draft.pdf.

[2] W. Denniss, Google, J. Bradley, and Ping Identity, *OAuth 2.0 for Native Apps*, Internet Engineering Task Force (IETF) OAuth Working Group Internet-Draft, March 2016. https://tools.ietf.org/html/draft-ietf-oauth-native-apps-01.

[3] *AppAuth for iOS*, GitHub [website], http://openid.github.io/AppAuth-iOS/.

[4] *AppAuth for Android*, GitHub [website], http://openid.github.io/AppAuth-Android/.

[5] Dr. R. Lindemann and D. Baghdasaryan, *FIDO AppID Facet Specification v1.0*, Fast Identity Online (FIDO) Alliance Proposed Standard, December 2014. http://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208.zip.

[6] *Universal 2nd Factor Overview*, Fast Identity Online (FIDO) Alliance Proposed Standard, May 2015. https://fidoalliance.org/specs/fido-undefined-undefined-ps-20150514/fido-u2f-overview-v1.0-undefined-ps-20150514.html.

[7] H. Le Van Gong, D. Balfanz, A. Czeskis, A. Birgisson, J. Hodges, *FIDO 2.0: Web API for accessing FIDO 2.0 credentials*, World Wide Web Consortium (W3C) Member Submission, November 2015. https://www.w3.org/Submission/2015/SUBM-fido-web-api-20151120/.

[8] R. Housley, RSA Laboratories, W. Polk, NIST, W. Ford, VeriSign, D. Solo, Citigroup, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 3280, April 2002. https://www.ietf.org/rfc/rfc3280.txt.

[9] International Organization for Standardization/International Electrotechnical Commission, *Information technology—Biometric presentation attack detection—Part 3: Testing and reporting*, ISO/IEC CD 30107-3.

[10] International Organization for Standardization/International Electrotechnical Commission, *Information technology—Security techniques—Information security management systems—Requirements*, ISO/IEC 27001:2013. 2013.

[11] International Organization for Standardization/International Electrotechnical Commission, *Information technology—Security techniques—Entity authentication assurance framework*, ISO/IEC 29115:2013. 2013.

[12] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[13] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53 Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[14] P.A. Grassi, J.L. Fenton, *Digital Authentication Guideline*, DRAFT NIST Special Publication 800-63-3, National Institute of Standards and Technology, Gaithersburg, Maryland, 2016. https://pages.nist.gov/800-63-3/sp800-63-3.html.

[15] D. Cooper, H. Ferraiolo, K. Mehta, S. Francomacaro, R. Chandramouli, J. Mohler, *Interfaces for Personal Identity Verification—Part 1: PIV Card Application Namespace, Data Model and Representation*, NIST Special Publication 800-73-4, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2015. http://dx.doi.org/10.6028/NIST.SP.800-73-4.

APPENDIX B – GLOSSARY

All definitions in this document are sourced from NIST SP800-63-3 and can be found online here:

https://pages.nist.gov/800-63-3/sp800-63a.html#sec3

https://pages.nist.gov/800-63-3/sp800-63b.html#sec3

https://pages.nist.gov/800-63-3/sp800-63c.html#sec3