NIST SPECIAL PUBLICATION 1800-13A

Mobile Application Single Sign-On:

Improving Authentication for Public Safety First Responders

Volume A:
Executive Summary

William Fisher
Paul Grassi*
Applied Cybersecurity Division
Information Technology Laboratory

Spike E. Dog
Santos Jha
William Kim*
Taylor McCorkill*
Joseph Portner*
Mark Russell*
Sudhi Umarji
The MITRE Corporation
McLean, Virginia

William C. Barker
Dakota Consulting
Silver Spring, Maryland

**Former employee; all work for this publication was done while at employer.*

August 2021

FINAL

The first and second drafts of this publication are available free of charge from https://www.nccoe.nist.gov/library/mobile-application-single-sign-nist-sp-1800-13-practice-guide

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-13.

Executive Summary

- On-demand access to public safety data is critical to ensuring that public safety and first responders (PSFRs) can protect life and property during an emergency.
- This public safety information, often needing to be accessed via mobile or portable devices, routinely includes sensitive information, such as personally identifiable information, law enforcement sensitive information, and protected health information.
- Because the communications are critical to public safety and may include sensitive information, robust and reliable authentication mechanisms that do not hinder delivery of emergency services are required.
- In collaboration with the National Institute of Standards and Technology (NIST) Public Safety Communications Research laboratory and industry stakeholders, the National Cybersecurity Center of Excellence (NCCoE) at NIST built a laboratory environment to demonstrate standards-based technologies that can enable PSFRs to gain access to public safety information efficiently and securely by using mobile devices.
- The technologies demonstrated are currently available and include (1) single sign-on (SSO) capabilities that reduce the number of credentials that need to be managed by public safety personnel, and reduce the time and effort that individuals spend authenticating themselves; (2) identity federation that can improve the ability to authenticate personnel across public safety organization (PSO) boundaries; and (3) multifactor authentication (MFA) that enables authentication with a high level of assurance.
- This NIST Cybersecurity Practice Guide describes how organizations can implement these technologies to enhance public safety mission capabilities by using standards-based commercially available or open-source products. The technologies described facilitate interoperability among diverse mobile platforms, applications, relying parties, identity providers (IdPs), and public-sector and private-sector participants, regardless of the application development platform used in their construction.

CHALLENGE

Recent natural and human-made disasters and crises have highlighted the importance of efficient and secure access to critical information by PSFRs. For decades, much of this information was broadcast to PSFRs by voice over radio. More recently, many PSOs have transitioned to a hybrid model that includes automated access to much of this information via ruggedized mobile laptops and tablets. Further advances in technology have resulted in increasing reliance on smartphones or similar portable devices for field access to public safety information. The increasing reliance on these devices has driven the use of “native app”-based interfaces to access information, in addition to more conventional browser-based methods.

Many PSOs are in the process of transitioning from conventional land-based mobile communications to high-speed, regional or nationwide wireless broadband networks (e.g., FirstNet). These networks employ Internet Protocol-based communications to provide secure and interoperable public safety communications to support initiatives such as Criminal Justice Information Services, Regional Information Sharing Systems, and international justice and public safety services such as those provided

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-13.

by Nlets. This transition will foster critically needed interoperability within and among jurisdictions, but it will create a significant increase in the number of mobile devices that PSOs will need to manage.

Current PSO authentication services may not be sustainable in the face of this growth. There are needs to improve security assurance, limit authentication requirements that are imposed on users (e.g., reduce the number of passwords that are required), improve the usability and efficiency of user account management, and share identities across jurisdictional boundaries. There is no single management or administrative hierarchy spanning the PSFR population. PSFR organizations operate in a variety of environments with different authentication requirements. Standards-based solutions are needed to support technical interoperability and a diverse set of PSO environments.

SOLUTION

To address these challenges, the NCCoE brought together common identity and software application providers to demonstrate how a PSO can implement mobile native and web application SSO, access federated identity sources, and implement MFA. SSO limits the time and effort that PSFR personnel spend authenticating, while MFA provides PSOs with adequate confidence that users who are accessing their information are who they say they are. The architecture supports identity federation that allows PSOs to share identity assertions between applications and across PSO jurisdictions. A combination of all of these capabilities can allow PSFR personnel to authenticate—say, at the beginning of their shift—and leverage that high-assurance authentication to gain cross-jurisdictional access to many other mobile native and web applications while on duty.

The guide provides

- a detailed example solution and capabilities that address risk and security controls
- a demonstration of the approach using commercially available products
- “how to” instructions for implementers and security engineers on integrating and configuring the example solution into their organization’s enterprise in a manner that achieves security goals with minimal impact on operational efficiency and expense

The NCCoE assembled existing technologies that support the following standards:

- Internet Engineering Task Force Request for Comments 8252, *OAuth 2.0 for Native Apps*
- Fast Identity Online (FIDO) Universal Second Factor and Universal Authentication Framework
- Security Assertion Markup Language 2.0
- OpenID Connect 1.0

Commercial, standards-based products, such as the ones that we used, are readily available and interoperable with existing information technology (IT) infrastructures.

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization’s information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution 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 a solution.

BENEFITS

The NCCoE's practice guide to *Mobile Application Single Sign-On* can help PSOs:

- define requirements for mobile application SSO and MFA implementation
- improve interoperability among mobile platforms, applications, and IdPs, regardless of the application development platform used in their construction
- enhance the efficiency of PSFRs by reducing the number of authentication steps, the time needed to access critical data, and the number of credentials that need to be managed
- support a diverse set of credentials, enabling a PSO to choose an authentication solution that best meets its individual needs

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/mobile-sso. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at psfr-nccoe@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

MOTOROLA SOLUTIONS · Nok Nok LABS · Ping Identity · STRONGKEY · yubico

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.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-13.