

# Mobile Application Single Sign-On

## Improving Authentication for Public Safety First Responders

---

**Volume A:**  
**Executive Summary**

**Bill 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.*

May 2019

SECOND DRAFT

This publication is available free of charge from  
<https://www.nccoe.nist.gov/projects/use-cases/mobile-ss0>

# 1 Executive Summary

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

## 27 CHALLENGE

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

36 Many PSOs are in the process of transitioning from traditional land-based mobile communications to  
37 high-speed, regional or nationwide wireless broadband networks (e.g., FirstNet). These emerging “5G”  
38 systems employ internet protocol-based communications to provide secure and interoperable public  
39 safety communications to support initiatives such as Criminal Justice Information Services, Regional  
40 Information Sharing Systems, and international justice and public safety services such as those provided

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

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

## 50 SOLUTION

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

60 The guide provides

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

66 The NCCoE assembled existing technologies that support the following standards:

- 67     ▪ Internet Engineering Task Force Request for Comments 8252, *OAuth 2.0 for Native Apps*
- 68     ▪ FIDO Universal Second Factor and Universal Authentication Framework
- 69     ▪ Security Assertion Markup Language 2.0
- 70     ▪ OpenID Connect 1.0

71 Commercial, standards-based products, such as the ones that we used, are readily available and  
72 interoperable with existing information technology (IT) infrastructures. While the NCCoE used a suite of  
73 commercial products to address this challenge, this guide does not endorse these particular products,  
74 nor does it guarantee compliance with any regulatory initiatives. Your organization’s information  
75 security experts should identify the products that will best integrate with your existing tools and IT  
76 system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines  
77 in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

78 **BENEFITS**

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

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

87 **SHARE YOUR FEEDBACK**

88 You can view or download the guide at <https://www.nccoe.nist.gov/projects/use-cases/mobile-ss0>. Help  
89 the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt  
90 this solution for your own organization, please share your experience and advice with us. We recognize  
91 that technical solutions alone will not fully enable the benefits of our solution, so we encourage  
92 organizations to share lessons learned and best practices for transforming the processes associated with  
93 implementing this guide.

94 To provide comments or to learn more by arranging a demonstration of this example implementation,  
95 contact the NCCoE at [psfr-nccoe@nist.gov](mailto:psfr-nccoe@nist.gov).

---

96 **TECHNOLOGY PARTNERS/COLLABORATORS**

97 Organizations participating in this project submitted their capabilities in response to an open call in the  
98 Federal Register for all sources of relevant security capabilities from academia and industry (vendors  
99 and integrators). The following respondents with relevant capabilities or product components (identified  
100 as “Technology Partners/Collaborators” herein) signed a Cooperative Research and Development  
101 Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.



102

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

---

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 challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

**LEARN MORE**

Visit <https://www.nccoe.nist.gov>  
[nccoe@nist.gov](mailto:nccoe@nist.gov)  
301-975-0200