

MOBILE APPLICATION SINGLE SIGN-ON

Improving Authentication for Public Safety First Responders

The National Cybersecurity Center of Excellence (NCCoE) and its collaborators are helping the Public Safety and First Responder (PSFR) community address the challenge of securing sensitive information accessed on mobile applications. This fact sheet provides an overview of NIST SP 1800-13, *Mobile Application Single Sign-On*. As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this Practice Guide, or would like to schedule a demonstration, please email psfr-nccoe@nist.gov.

CHALLENGE

PSFR personnel need immediate access to public safety data to ensure they deliver the proper care and support during an emergency, especially when any delay—even seconds—is a matter of containing or exacerbating an emergency situation. Mobile technologies, like cell phones, tablets, laptops, and their associated applications, have helped make this data available on demand; however, the broad range of public safety personnel, missions, and working conditions presents unique challenges. Public safety organizations (PSOs) still need to ensure data security while easing authentication requirements for their users (e.g., reduce the number of passwords that are required), improving account management, and sharing identities across jurisdictional boundaries.

SOLUTION

In response to these challenges, the NCCoE has collaborated with industry and the information technology (IT) community, including vendors of cybersecurity solutions, to develop a step-by-step how-to guide. NIST SP 1800-13, *Mobile Application Single Sign-On*, demonstrates how a PSO can provide a reduced number of required sign-ons for mobile applications, easier access to federated identity sources, and improved security via multifactor authentication (MFA) to PSFR in the field, all while using standards-based, commercially available, and open source products.

This guide:

- provides a detailed example solution and capabilities that address risk and security controls
- demonstrates standards-based MFA, identity federation, and mobile single sign-on (SSO) for native and web applications
- supports multiple authentication methods, taking into account unique environmental issues faced by first responders in emergency medical services, law enforcement, and fire services

BENEFITS

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

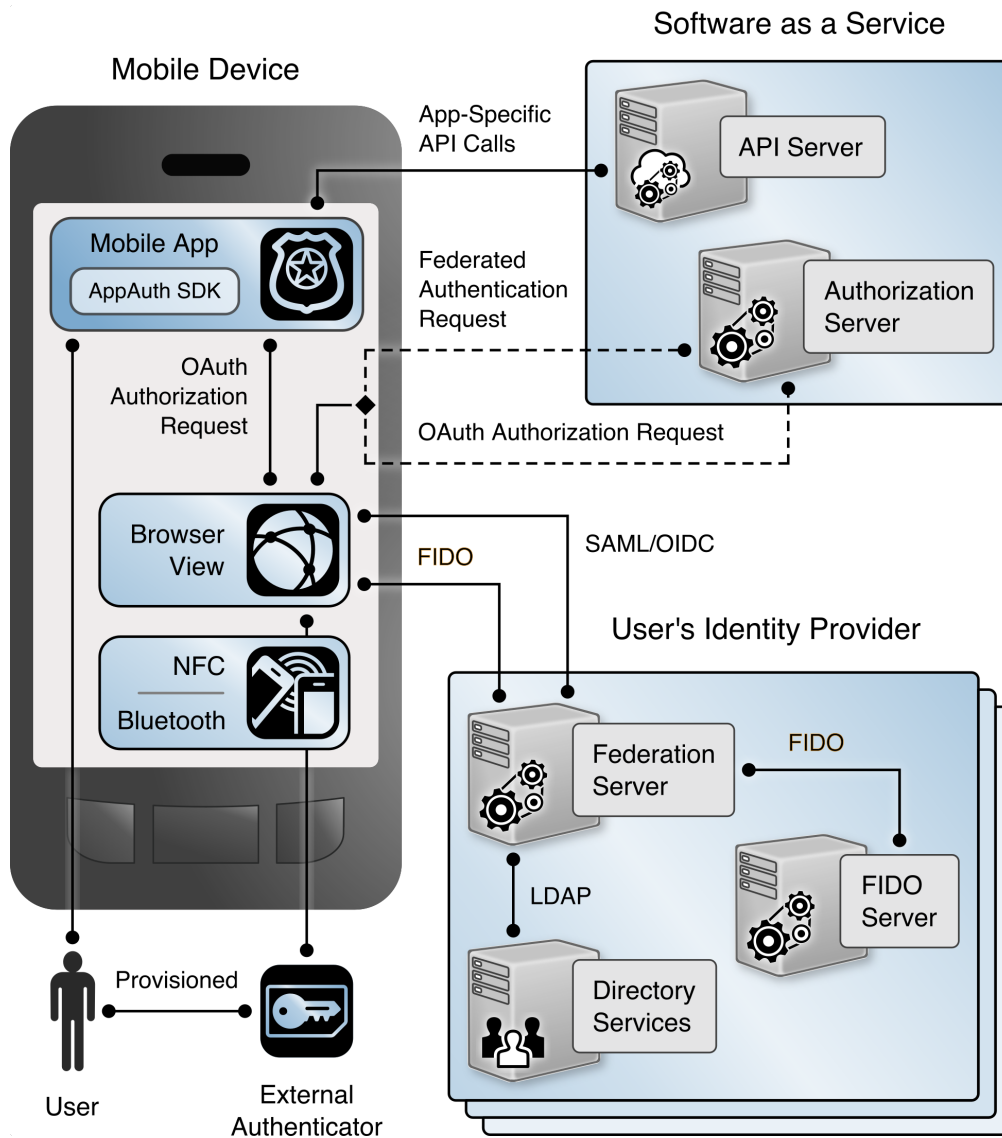
- define requirements for mobile application SSO and MFA implementation
- improve interoperability between mobile platforms, applications, and identity providers, regardless of the application development platform used in their construction
- enhance the efficiency of PSFRs by reducing the number of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

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 ABOUT NCCOE
Visit <https://www.nccoe.nist.gov>

CONTACT US
nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE



TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who are participating in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:



Certain commercial entities, equipment, or materials may be identified 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, materials, or equipment are necessarily the best available for the purpose.

DOWNLOAD THE PRACTICE GUIDE

To learn more about this project, visit <https://www.nccoe.nist.gov/projects/use-cases/mobile-ss0>.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking collaborators, insights, and expertise from businesses, the public, and technology vendors. If you have questions about this project or would like to join the public safety first responder community of interest, please contact psfr-nccoe@nist.gov.