NIST Internal Report
NIST IR 8523

Multi-Factor Authentication for Criminal Justice Information Systems

Implementation Considerations for Protecting Criminal Justice Information

William Fisher
Jason Ajmo
Sudhi Umarji
Spike E. Dog
Mark Russell
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8523

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Internal Report
NIST IR 8523

Multi-Factor Authentication for Criminal Justice Information Systems

Implementation Considerations for Protecting Criminal Justice Information

William Fisher
Applied Cybersecurity Division
Information Technology Laboratory

Jason Ajmo
Sudhi Umarji
Spike E. Dog
The MITRE Corporation

Mark Russell
Appian Logic

Karen Scarfone
Scarfone Cybersecurity

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8523

September 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added to final publication.]

How to Cite this NIST Technical Series Publication
Fisher W, Ajmo J, Umarji S, Dog S, Russell M, Scarfone K (2025) Multi-Factor Authentication for Criminal Justice Information Systems: Implementation Considerations for Protecting Criminal Justice Information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST internal Report (IR) NIST IR 8523. https://doi.org/10.6028/NIST.IR.8523

Author ORCID iDs
William Fisher: 0009-0004-7569-5668
Jason Ajmo: 0009-0007-4046-6146
Sudhi Umarji: 0000-0001-6842-8167
Spike Dog: 0009-0000-0201-6776
Mark Russell: 0009-0004-1273-392X
Karen Scarfone: 0000-0001-6334-9486

Contact Information
psfr-nccoe@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information

Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8523/final, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

Most recent cybersecurity breaches have involved compromised credentials. Migrating from single-factor to multi-factor authentication (MFA) reduces the risk of compromised credentials and unauthorized access. Both criminal and noncriminal justice agencies need to access criminal justice information (CJI); to reduce the risk of unauthorized access, the Criminal Justice Information Services (CJIS) Security Policy now requires the use of MFA when accessing CJI. This document provides practical information to agencies that are implementing MFA, reflecting on lessons learned from agencies around the country and from CJI-related technology vendors.

Keywords

authentication; credentials; criminal justice information (CJI); identity; identity federation; law enforcement; multi-factor authentication (MFA); single sign-on (SSO).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of information other than national security-related information in federal information systems.

Audience

The audience for this document includes state CJIS information security officers (ISOs) and CJIS systems officers (CSOs), law enforcement agency chief information officers (CIOs) and chief information security officers (CISOs), and anyone else responsible for safeguarding CJI. The audience also includes vendors that supply CJI-related technology products and services to agencies that are subject to the CJIS Security Policy.

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Tables

List of Figures

Acknowledgments

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Chris Weatherly	Federal Bureau of Investigation (FBI) CJIS
Jeff Campbell	FBI CJIS
Holden Cross	ECS
John Beltz	NIST
Hildegard Ferraiolo	NIST
Ryan Galluzzo	NIST
Cheri Pascoe	NIST
Andrew Regenscheid	NIST
Ron Pulivarti	NIST
Julie Chua	NIST

Executive Summary

The Criminal Justice Information Services (CJIS) Security Policy versions 5.9.2 and later [1] require the use of multi-factor authentication (MFA) to protect access to criminal justice information (CJI). MFA is important for protecting against credential compromises and other cyber risks that may threaten CJI. Criminal and non-criminal justice agencies around the country will need to work with their technology vendors to implement this CJIS requirement.

CJI is commonly accessed using computer-aided dispatch (CAD) and record management system (RMS) software, which communicate with a state-level message switch application. CJI MFA architectures will likely need to integrate with one or both of these technologies. As agencies around the country begin to implement MFA solutions, the approaches they use require careful consideration and planning. This document provides a general overview of MFA, outlines design principles and architecture considerations for implementing MFA to protect CJI, and offers specific examples of use cases that agencies face today. It also outlines how CAD/RMS and message switch technologies can support standards and best practices that provide agencies with maximum optionality to implement MFA in a way that promotes security, interoperability, usability, and cost savings.

1. Introduction

Credential compromises represent a critical and pervasive cybersecurity threat, serving as a gateway for malicious actors to infiltrate networks and systems, thus gaining access to sensitive data. Whether through phishing, brute-force attacks, or exploiting vulnerabilities in authentication mechanisms, credential compromise poses a significant risk to organizations and individuals alike. To mitigate this threat, version 5.9.2 and subsequent versions of the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy [1] require multi-factor authentication (MFA) for all users when accessing criminal justice information (CJI). Both criminal and non-criminal justice agencies that receive CJI are subject to this requirement. In this document, we refer to these organizations generically as *agencies*.

As agencies around the country begin to implement this requirement, they face several challenges that require careful consideration and planning. The purpose of this document is to help agencies identify and address their MFA implementation needs by providing insight into MFA architectures and how they can be used to meet law enforcement-specific use cases.

1.1. Approach

To ensure the relevance of this document's contents, the NIST and FBI CJIS team engaged with agencies around the country on their current and future MFA implementations, as well as law enforcement technology vendors on their current and future support for MFA standards and best practices. The architectures, use cases, technologies, and challenges in this document are heavily based on those discussions. Though this document will promote standards and best practices for MFA and identity federation, the overarching goal of this document is to meet agencies "where they are" by providing practical MFA implementation considerations that help inform agency risk decisions while also considering cost, functional requirements, and the potential for centralized and shared MFA services.

1.2. How to Use This Document

This document is intended to aid agencies in their MFA implementations; it does not guarantee that their implementation will meet CJIS Security Policy requirements or will pass a CJIS audit. All questions about how a specific MFA implementation can meet the CJIS Security Policy should be directed to the CJIS Information Security Officer (ISO) team at iso@fbi.gov.

Many of the challenges discussed in this document require collaboration between state, local, tribal, and territorial (SLTT) agencies, as well as collaboration with law enforcement technology providers. Agencies should engage all relevant stakeholders to discuss MFA implementation plans to ensure this collaboration can occur.

Section 2 of this document provides an overview of MFA concepts and the importance of MFA as a cybersecurity control.

Section 3 of this document details MFA design principles, agency stakeholders that should be part of MFA requirements development, considerations for a phased MFA rollout, and examples of where agencies might choose to implement MFA.

Section 4 collects the key considerations for agencies from throughout the document.

The Appendices of this document include detailed MFA architectures and questionnaires that agencies can use to engage their vendors.

This report uses callout boxes to highlight certain types of information, as depicted in Fig. 1. With the exception of **Definition** boxes, which repeat the definitions of key terms or provide more formal definitions for them, callout boxes usually contain new material that is not covered elsewhere in the report. A **Caution** box provides a warning of a potential issue with doing or not doing something. A **Note** box gives additional general information on a topic. A **Tip** box offers advice that may be beneficial to the reader.

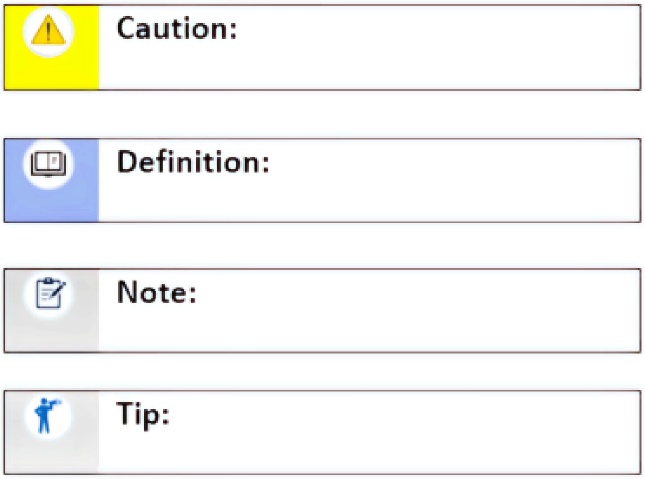


Fig. 1. Callout box formats.

2. An Overview of MFA Technologies and Concepts

This section provides an overview of some key technologies and concepts relevant to MFA deployments, the understanding of which is necessary before addressing specific MFA architectures.

2.1. Introduction to MFA

In 2024, 46% of public safety breaches [2] involved stolen credentials. MFA is a common security control used to reduce the risk of compromised credentials and unauthorized access. Traditional single-factor authentication relies solely on passwords, whereas MFA requires more than one distinct type of authentication factor for successful authentication. So, if an attacker obtains a user's password, they still need access to the additional factor to successfully authenticate.

Definition: *Authentication* is "the process by which a *claimant* proves possession and control of one or more *authenticators* bound to a *subscriber account* to demonstrate that they are the subscriber associated with that account" [3] and involves one or more of the following factors:

i. *something you know* (e.g., password/personal identification number [PIN]);
ii. *something you have* (e.g., cryptographic identification device, token); or
iii. *something you are* (e.g., biometric).

Definition: *MFA* is "an authentication system that requires more than one distinct type of authentication factor for successful authentication. MFA can be performed using a multi-factor authenticator or by combining single-factor authenticators that provide different types of factors." [3]

Definition: An *authenticator* is "[s]omething the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity." [3]

Authenticators used in MFA systems have a wide range of form factors that may include the use of a PIN/password, biometrics, mobile devices, security keys, one-time codes, or other form factors. For a list of different authenticator types and their requirements, see Identification and Authentication within the CJIS Security Policy [1].

2.2. CJIS Requirements for MFA

NIST Special Publication (SP) 800-63 defines three Authentication Assurance Levels (AALs) that help differentiate the inherent security properties that authenticators may possess. Non-sensitive data may only require an AAL1 authenticator, typically a single-factor username and password. However, for information and systems that may cause a detrimental impact if compromised, AAL2 or AAL3 multi-factor authenticators may be required.

Note: NIST does not allow the combination of a *something you know* + a *something you are* factor at AAL2. To attain AAL2, NIST requires a *something you have* factor in combination with either a *something you know* or *something you are* factor.

Because the compromise of CJI would significantly impact agencies across the country, the CJIS Security Policy requires that CJI be protected by MFA at AAL2 or greater. Agencies should reference the Identification and Authentication section of the CJIS Security Policy (versions 5.9.2 or later) [1] for specific requirements.

Caution: NIST SP 800-63 has been updated to revision 4 [3]. The latest CJIS Security Policy as of this writing is based on the final version of revision 3. Agencies should focus on the language in the CJIS Security Policy for all AAL requirements.

2.3. Identity Providers

In the context of identity federation, we often use the terms *identity provider (IdP)* and *relying party (RP)* to refer to the entity that is authenticating the user—the IdP—and to the application or service that is accepting an assertion that authentication was successfully completed—the RP. In this document, we'll refer to an IdP generally as an entity that commonly has the following roles:

- **Authentication** – an application and/or service that receives the authentication request, attempts to verify the user's credential, and determines if authentication is successful or unsuccessful.
- **Credential lifecycle management** – handles the issuance, management, and revocation of authenticators.
- **Issuance of identity assertions** – provides assertions to RPs about the details of a given authentication transaction, which may include authentication success or failure, type of authentication used, and/or attributes about the user.

When deploying an MFA solution, agencies should consider where their users might get the above services from, i.e., where the IdP resides in the overarching MFA architecture, who owns and operates the IdP, and which of the above services it will provide. There are many models that work, depending on the needs of the agencies using the service and the protocols that technology providers support.

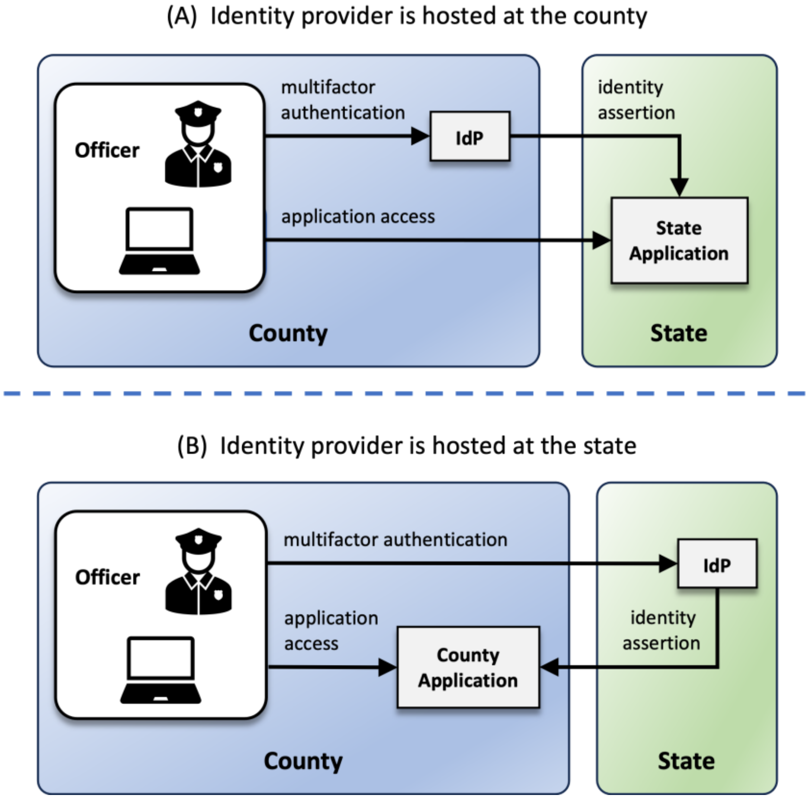
Definition: An *assertion* is "a statement from an IdP to an RP that contains information about an authentication event for a subscriber" [3]. In federation, the assertion is the evidence that the IdP sends to the RP that the user has logged in. It can also contain user identifiers such as a username or email address and information about how the user logged in, such as whether MFA was used.

2.4. Single Sign-On and Identity Federation

Though MFA enhances security, there are both monetary and user friction costs to MFA implementations. Single sign-on (SSO) and identity federation are technologies that support MFA deployments and can alleviate costs by reducing the number of credentials a user needs to manage, reducing the number of times a user needs to authenticate, and allowing users to reuse a single authentication to get access to multiple applications and/or resources.

2.4.1. Benefits of Identity Federation

Federation "is a process that allows for the conveyance of identity and authentication information across a set of networked systems" [3]. Commonly, identity federation protocols such as Security Assertion Markup Language (SAML) 2.0 and OpenID Connect (OIDC) 1.0 allow users to gain access to an application or service—an RP—without the need to register a new identity or credential with that RP. Instead, users are given the option to authenticate using a credential already issued to them by an IdP, often their state or local agency, as shown in Fig. 2. For detailed information on identity federation, please see Appendix B.


(A) Identity provider is hosted at the county

(B) Identity provider is hosted at the state

Fig. 2. The identity provider (IdP) can be at hosted at the state or county, or both.

Identity federation supports MFA architectures by enabling flexibility and optionality for where MFA can be implemented. For example, if a local police department (PD) has implemented MFA and its officers are required to access CJI resources at the state level, identity federation can be used to establish a trust relationship between the local PD (as the IdP) and the state CJI application (as the RP). This can enable a user to authenticate with the MFA credentials issued to them by the county without the need to be issued a second set of MFA credentials by the state.

Definition: *Federation* “is a process that allows for the conveyance of identity and authentication information across a set of networked systems” [3]. This is done in an interoperable way using federation protocols such as OpenID Connect or SAML.

Note: Have you ever navigated to a webpage and been given the option to use an existing Google, Facebook, or other third-party identity rather than creating a new identity at that website? Identity federation protocols enable this capability.

This flexibility has multiple potential benefits. For example, identity federation can enable a shared service model in which multiple local agencies could use a single identity provided by the state identity service to get MFA credentials and access CJI. This model can reduce implementation costs and can be especially useful for small and rural agencies that may not have the resources or expertise to implement MFA but still require access to CJI. An example of this model is explored in Appendix B.4.

Identity federation protocols are also an important tool to ensure that memorized secrets, such as passwords, do not need to be shared between systems to enable authentication or authorization. For more on memorized secrets, see Sec. 3.1.3.

Agencies should work with their technology vendors, specifically CAD/RMS, state message switch, and identity services vendors, to confirm they support identity federation protocols and architectures.

2.4.2. Benefits of Single Sign-On

One major aspect of deploying MFA technology is the impact on user experience and expectations. Any change in the way users authenticate can result in user friction. This is particularly important in law enforcement communities where any authentication delays in the line of duty might impact the ability to respond to an emergency. SSO is one way to alleviate user friction and limit how often a user needs to authenticate. As shown in Fig. 3, SSO enables users to authenticate once and gain access to multiple system resources without the need to reauthenticate as they use each new application or service.

SSO is also a great way to enable MFA. Applications that do not natively support MFA can be integrated with an SSO service, improving security and reducing the number of credentials users need to manage. Agencies may consider integrating both CJI and non-CJI applications with an SSO service to gain additional return on investment and to provide users with a common authentication experience across applications, see Sec. 3.4.2.3.

Agencies interested in implementing SSO should work with their technology vendors, specifically CAD/RMS, state message switch, and identity services vendors, to confirm they support SSO protocols and architectures.

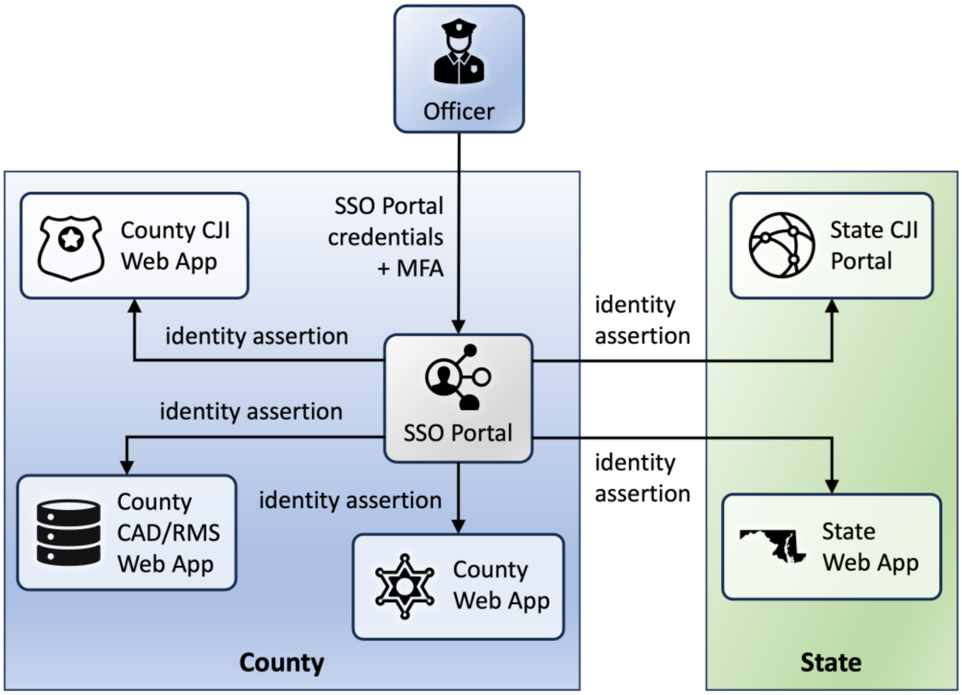


Fig. 3. Single sign-on eliminates repeated MFA challenges to users.

Note: What's the difference between federation and SSO?

Federation and SSO have a lot in common. Both technologies allow applications to trust another system to authenticate users. The difference is that SSO systems typically function inside a single organization, whereas federation technologies focus on bridging the gap between organizations. Many organizations use both SSO and federation systems—for example, they may use Active Directory SSO for internal applications and a federation system for interacting with external partners. Federation systems can provide an SSO experience by not requiring users to authenticate when they access each application, unless policy requires a reauthentication.

2.5. The Importance of Phishing Resistance

All MFA has security benefits compared to using a single factor, but not all forms of MFA are created equal, even if they are at the same AAL. One important differentiator among various types of MFA is the ability for the authenticator to resist phishing attacks. Phishing attacks attempt to lure a user (usually through an email) into interacting with a counterfeit webpage or application and trick the user into revealing information (typically passwords or one-time codes) that can be used to masquerade as that user to the real web page or application. See Fig. 4 for an example of how a phishing attack occurs.

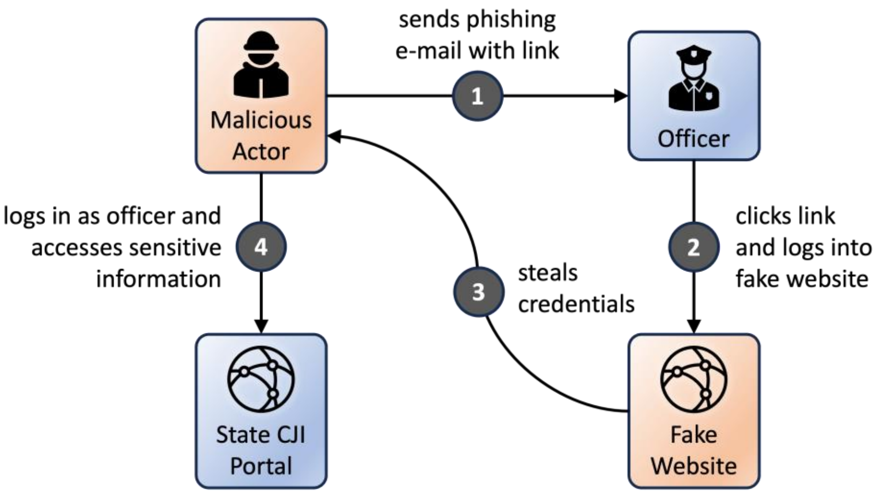

Malicious Actor
sends phishing e-mail with link
1
Officer
clicks link and logs into fake website
2
steals credentials
3
Fake Website
logs in as officer and accesses sensitive information
4
State CJI Portal

Fig. 4. An example of a phishing attack.

Tip: Not all authenticators are phishing resistant, but phishing-resistant MFA solutions are now commonly supported by identity platforms. Commercially, Fast Identity Online (FIDO) authenticators paired with the World Wide Web Consortium's (W3C) Web Authentication API are the most widely available phishing-resistant authenticators. Agencies should ask vendors what phishing-resistant authentication options they support, to include support for phishing-resistant, syncable authenticators as described in NIST 800-63B-4 [4].

Phishing attacks are a significant cybersecurity challenge, as they are often conducted remotely and at scale, meaning that an attacker may send a phishing email to thousands of employees, needing only to trick a single employee into providing their login information to gain unauthorized access to data and/or applications. Phishing-resistant authentication systems do not require the user to recognize an attack and make the right decision, but rather have phishing resistance built into the authentication protocol itself. NIST published a blog post on phishing-resistant authenticators and how they mitigate common attacks [5].

Caution: What makes phishing attacks so dangerous is the way they can bypass physical and network security protections. Simply sending a phishing email to an employee of a target agency could result in the attacker gaining legitimate credentials and using them to access agency systems, potentially including CJI. Phishing attacks do not require physical access to buildings, servers, or data, nor do they require hacking or intrusion. Instead, phishing attacks rely upon tricking users into giving up valid user credentials, effectively letting the attacker through the "front door." Phishing-resistant MFA is the best defense against these attacks. **Although phishing resistance is an optional requirement at AAL2, it is recommended that agencies implement phishing-resistant MFA at AAL2, given the prevalence of phishing attacks.**

3. Choosing an MFA Implementation for Protecting CJI

Criminal justice information systems are used across state, local, tribal, and territorial governments with both criminal and non-criminal justice agencies. Accessing CJI often requires cross-jurisdictional connection of IT systems and collaboration between agencies. For this reason, there are many MFA architectures that could be implemented across the CJIS ecosystem.

depicts a representative architecture with technology components commonly found across most agencies. As the figure demonstrates, there are many ways to implement MFA, each of which can be viable depending on the requirements of the agency. No matter which architecture is chosen, there are cross-cutting principles that agencies should consider that may improve the usability, cost, and security of their MFA solution.

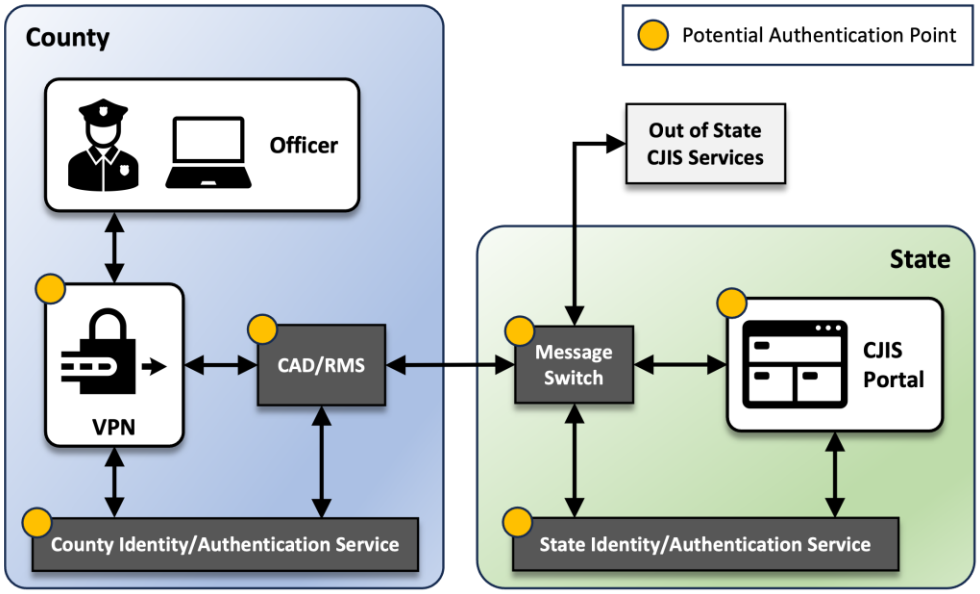

County
Potential Authentication Point
Officer
Out of State CJIS Services
State
VPN
CAD/RMS
Message Switch
CJIS Portal
County Identity/Authentication Service
State Identity/Authentication Service

Fig. 5. MFA implementation points.

This section presents considerations for agencies choosing an MFA implementation for protecting CJI:

- Section 3.1 discusses MFA design principles to provide a foundation for MFA selection.
- Section 3.2 explains the need to conduct a requirements assessment before choosing an MFA solution and indicates which stakeholders may be part of that assessment.
- Section 3.3 provides a notional structure for a phased MFA deployment.
- Section 3.4 explores common MFA architectures and the trade-offs each one faces against the MFA design principles.

Note: The remainder of this document assumes that the reader is familiar with basic components commonly used to access CJI. If the reader is not familiar with these technologies, Appendix A of this document contains a brief overview of each.

3.1. MFA Design Principles

This section highlights four MFA design principles. These principles are **not** required for any given MFA solution. However, they do play an important role in the long-term efficacy and cost of an MFA solution. Agencies should consider these principles before selecting an MFA implementation. Moreover, state, local, tribal, and territorial agencies should collaborate to determine how these principles could be attained through partnership and/or shared services.

3.1.1. Principle 1: Authenticator Reusability

Law enforcement and other personnel accessing CJI already manage multiple user identities and may already manage multiple MFA tokens for those identities. To the greatest extent feasible, agencies should consider MFA architectures that minimize the number of separate MFA credentials that need to be issued to users and managed. For instance, if a user has an MFA credential to access a state CJIS portal and another MFA credential to get access to their CAD/RMS system, there may be opportunities to avoid the user having to manage two sets of credentials. Moreover, each MFA implementation requires a management system, a support staff to assist users with obtaining, registering, and using their MFA credentials, and administrative processes that drive costs in both time and money. Agencies should consider integrating CJI applications and/or services with existing IdPs that can or already support MFA. This might include leveraging SSO services, as mentioned in Sec. 2.4.2.

3.1.2. Principle 2: Authenticator Optionality

Agencies typically have a diverse set of user authentication requirements. For example, mobile devices are commonly not allowed in department of corrections facilities and thus, MFA methods that use mobile phones are not viable for users inside these facilities. Agencies will benefit if their MFA solutions support multiple authenticator types and methods. This allows organizations to select the type of authenticator that best meets the needs of a given user base, context, or environment in which CJI is accessed. CAD/RMS, message switch, and virtual private network (VPN) vendors may provide multiple MFA methods, but generally, the greatest level of MFA optionality is offered by dedicated identity service providers.

3.1.3. Principle 3: Minimize the Passing of Memorized Secrets

The passing of memorized secrets, such as passwords, between agency applications and state message switches is a practice that is sometimes used to allow a state switch to authorize a user before getting access to CJI. However, there are security concerns with this model. To the greatest extent feasible, agencies should consider solutions that do not require the passing of memorized secrets across networked systems and amongst applications. Token-based systems such as Kerberos and identity federation protocols are viable options for integrating CJI applications and/or services with other applications and identity services.

Tip: Token-based protocols like Kerberos, SAML 2.0, and OIDC 1.0 are designed to alleviate the need to share memorized secrets between applications. They provide a greater level of flexibility and control.

3.1.4. Principle 4: Ensure MFA Is Integrated to Protect CJI

When deploying an MFA solution, agencies should ensure that the MFA implemented is integrated with the application or service that contains CJI. For example, if MFA is enforced only at the network level, such as a VPN service, but not at the application level, users might have to manage two separate credentials, MFA for the VPN and a username and password for the application. Moreover, if the application is only protected by a password, even if MFA was completed to gain network access, the application itself might be at risk of phishing attacks or a password database breach if a bad actor obtains network access. This "crunchy outside, soft inside" security model is not recommended. Ideally, CJI applications would be tied into an SSO service or directly integrated with an identity service such that the MFA completed at the network level can be enforced at the application level. Section 3.4.3 provides more detail about integrating MFA with VPN services.

3.2. MFA Requirements Assessment

When deploying an MFA solution, all agencies should conduct a requirements assessment to help determine the MFA solution that will best meet agency needs. This assessment should include, but is not limited to, engaging with the applicable stakeholders discussed in this section.

3.2.1. MFA Users

Before implementing any MFA solution, it is critical that agencies understand the common use cases and corner cases of the user population the MFA solution is intended to support. As mentioned in Sec. 3.1.2 on authenticator optionality, agencies will likely have varied requirements across their user base. For example, an MFA solution that works for individuals who reside primarily in an office environment might not be acceptable for an officer in the field.

Because the average agency user may not be familiar with MFA systems, agency personnel responsible for MFA deployment should conduct market research on potentially viable MFA solutions and present them to a representative portion of the user base to facilitate feedback and to enumerate requirements.

Implementing any MFA solution likely requires users to change the way they conduct daily interactions with their IT systems. Because of this, it is important that once an MFA solution is selected, agencies educate users with clear instructions on how to obtain and use any new authenticators, as well as provide easy access to help desk or support personnel who can assist users in setting up and using the new MFA solution. Section 3.3 provides a notional plan for a phased MFA rollout to different user bases.

3.2.2. IT Support Staff

As with any technology change, implementing an MFA solution will result in both users and administrative staff needing support as they become familiar with new processes. Agencies should establish appropriate communication channels for their user base to work with internal IT support and/or MFA vendors to help answer questions and troubleshoot problems. Agencies should expect an initial increase in IT support and help desk calls after MFA has been deployed. Help desk and support staff should be trained to assist users with the technology, and clearly communicated processes should exist for escalating difficult cases, including processes for bringing in vendor support.

3.2.3. Other Agencies

Before deploying an MFA solution, **state agencies** should consult local, tribal, and territorial agencies within their state to determine how these agencies might make use of or integrate with the state MFA solution. If the state intends to issue and manage MFA credentials for local, tribal, and territorial users, these agencies should be consulted for feedback on use cases, corner cases, and general requirements for the MFA solution. If local, tribal, and territorial agencies already have an MFA solution in place, the state should explore options to allow that solution to integrate with the state solution.

Before deploying an MFA solution, **local, tribal, and territorial agencies** should consult with their state agencies, as appropriate, to discern ways in which MFA requirements may be met through collaboration. For example, state agencies may already have an MFA solution that could be leveraged to meet local agency requirements. Additionally, state agencies may have purchase agreements in place that allow other agencies to cut costs through bulk purchasing or to save on procurement administration.

Where applicable, **all agencies** should consult with peer agencies inside or outside their state that are in the process of or have already deployed MFA solutions. This first-hand experience can offer valuable insight into how peer agencies have solved MFA challenges, enumerate feedback on vendors and solutions, and provide examples of how MFA technology was justified with leadership and procured.

3.2.4. Procurement Teams

Procurement teams play a support role in helping agencies navigate potential procurement vehicles and vendor engagement. For MFA deployments, agencies should work with procurement teams to ensure that applicable MFA requirements are written into requests for information and requests for proposal. Many of these requirements can be found under the IA-5 requirements in the Identification and Authentication section of the CJIS Security Policy [1]. Agencies should also work with procurement teams to explore and apply for potential grants that may be offered by agencies such as the Department of Homeland Security (DHS) or the Department of Justice (DOJ) [6]. Such grants could be used to assist in the procurement of hardware and software to deploy MFA capabilities.

3.2.5. Compliance Teams

Compliance teams should be engaged early and often during any MFA deployment. Despite commonality in architectures and underlying requirements, each agency implementing MFA will likely undergo a unique process of determining how their specific MFA implementation meets compliance requirements. Agencies should enumerate the CJIS Security Policy and any other compliance requirements at the onset of their MFA deployment to ensure they can work with all the applicable stakeholders to design a solution that meets compliance needs. The FBI CJIS ISO team should be consulted on all questions on how MFA deployments might meet the CJIS Security Policy. See Sec. 1.2 of this document for more information.

3.2.6. Legal Teams

Agencies should consult legal teams as part of their general cybersecurity risk management program. Agencies may have legal restraints that impact which MFA authenticator types they can use. Agencies should also check state privacy laws to determine how they might impact the collection of biometric information as an authenticator.

> ⚠ **Caution:** Mobile devices are commonly used as something-you-have authenticators and may be deployed as Corporately Owned Personally Enabled (COPE) or Bring Your Own Device (BYOD). However, if an agency allows the use of personal mobile devices as an authenticator platform, the devices may be subject to subpoena in criminal investigations. Agencies should consult their legal team to better understand the relevance of this risk to MFA implementations.

3.2.7. Technology Vendors

Agencies should work with technology vendors, including identity service providers and message switch, VPN, and CAD/RMS vendors, to determine how they can best support an MFA solution that meets agency requirements. For any vendor offering an MFA solution, agencies should request a demonstration of the solution and all available authenticator types. Agencies should also consult these vendors on how they support MFA architectures that utilize identity federation, SSO capabilities, and phishing-resistant MFA. It is important that agencies set expectations that vendors work collaboratively to help determine how each vendor solution meets agency requirements, including CJIS Security Policy requirements. Appendix C provides vendor questionnaires that may aid in this discussion.

> ⚠ **Caution:** It is important to keep your overall MFA strategy in mind when engaging with vendors. Asking a CAD/RMS vendor and a message switch vendor to implement MFA may result in two different MFA implementations that are not interoperable. If MFA can be integrated with an SSO or federation system instead of each application, it may be better to ask the application vendors to support compatible federation or SSO protocols rather than to implement MFA directly in their systems.

3.3. Phased MFA Deployment

As with most technology deployments, MFA is best deployed in phases. Agencies should seek to grow user MFA adoption over time, eschewing the expectation that all or even a large majority of users will adopt an MFA solution as soon as it is available. Table 1 offers an example of a phased MFA deployment.

Table 1. Example of a phased MFA deployment.

Phase	User Base	Rationale	Outcome
1	IT support and help desk personnel	IT support and help desk personnel are tech-savvy users who can also anticipate potential support issues that the larger user base may have with the solution.	• Test multiple authenticator types and gain feedback on the processes of obtaining and using each authenticator. • Enumerate potential support issues. • Gain feedback on MFA instructions and communication tools. • Confirm authenticator type selection.
2	General IT staff	This is a larger, but still technically literate, user base.	• Test authenticators selected from phase 1. • Gain feedback on MFA instructions and communication tools. • Update communications and/or policy based on feedback.
3	General user cohort	A representative cohort of general users can help test the MFA solution before a general user rollout.	• Take volunteers or a selection of the general cohort to test the MFA solution. • Test IT support and help desk procedures. • Hold user feedback sessions. • Update communications and/or policy based on feedback.
4	General user rollout	Once agencies are satisfied with testing from phases 1-3, it is time to proceed to a general rollout. This may not include some user populations that fall into corner cases.	• Provide multiple waves of communication around the MFA transition. • Allow for questions, answers, and feedback. • Provide a clear deadline for making the transition. • Update communications and/or policy based on feedback. • Monitor and grow adoption over time.
5	Corner case users	Corner case requirements may require alternate MFA solutions.	• Enumerate requirements and potential solutions for corner cases. • Test potential solutions with phases 1-3 before rolling out to corner case users.

3.4. Choosing Where to Deploy MFA

As previously mentioned, there are many potential places where MFA could be deployed. This section covers architectures commonly deployed at agencies, how those architectures might change when implementing MFA, and the trade-offs different architectures face against the MFA design principles. Section 3.4.1 focuses on local agency MFA and Sec. 3.4.2 covers state agency MFA. Section 3.4.3 discusses implementing MFA with VPNs.

Note: In general, agencies should seek to implement MFA once and then layer on supporting technologies such as identity federation or SSO to extend the value of that initial MFA implementation. Implementing MFA at multiple points in the architecture could result in increased technology costs as well as increased burden on users who need to manage and utilize multiple MFA credentials.

Appendix A provides an overview of CAD/RMS and message switch technology. See Appendix B for an in-depth look at MFA implementations based on federated identity architectures.

3.4.1. Local Agency MFA Architectures

Figure 6 details common technologies for accessing CJI at local agencies. Agencies are likely to consider implementing MFA either at an application used to access CJI, such as the CAD/RMS systems, or at a locally deployed identity and authentication service. In some cases, the state message switch that the local agency connects through may present users with an MFA challenge as well. While any of these options are viable MFA solutions, the following sections discuss the trade-offs local agencies might make involving the MFA principles, depending on which of these options they choose.

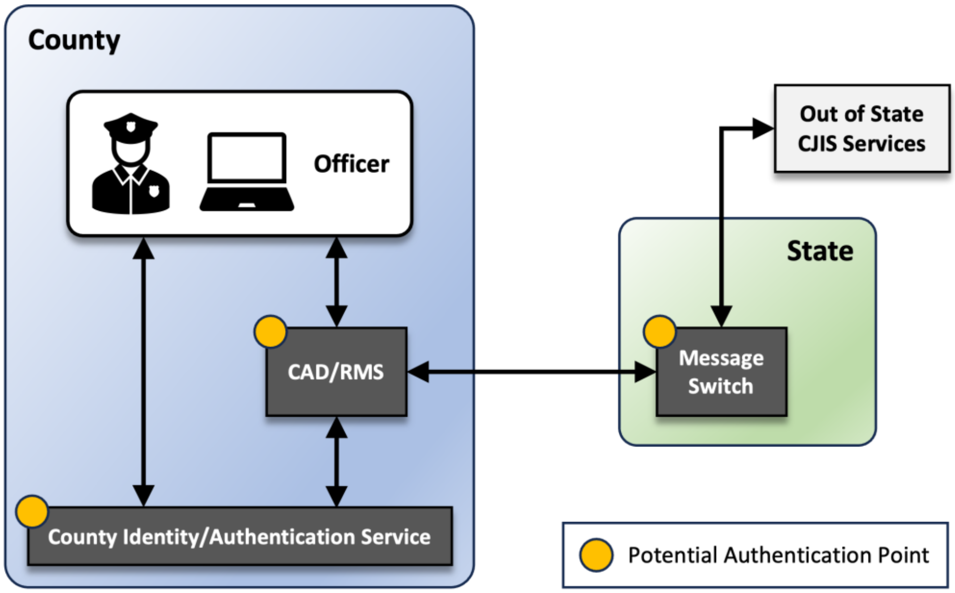

County
Officer
CAD/RMS
County Identity/Authentication Service
Out of State CJIS Services
State
Message Switch
Potential Authentication Point

Fig. 6. Potential authentication points for local agencies.

3.4.1.1. MFA Provided by a CAD/RMS Application

Figure 7 details an MFA solution implemented by the CAD/RMS application.

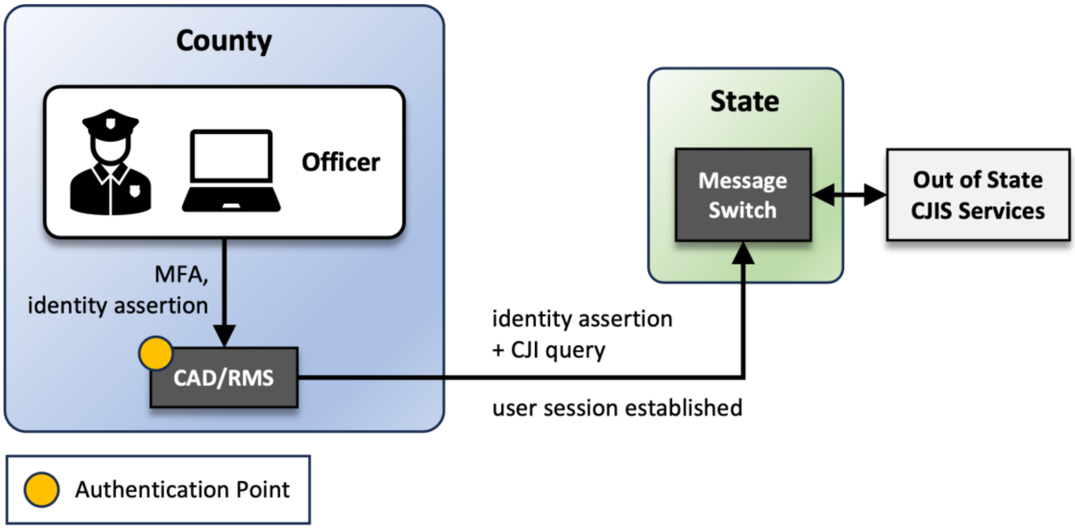


Fig. 7. MFA at the CAD/RMS application.

Agencies choosing to implement an MFA solution provided by their CAD/RMS vendor should consider a few key architecture elements:

- **Which authenticator types the CAD/RMS solution offers:** It is important for agencies to work with their CAD/RMS vendors to understand the MFA options they offer. Because CAD/RMS products do not include dedicated identity solutions, there may be limited MFA options available "out of the box." Agencies should consider if these options will adequately meet the requirements in the CJIS Security Policy and fulfill the MFA needs of agency users. If agencies cannot get the desired MFA optionality—as described in Sec. 3.1.2—from their CAD/RMS vendor, they should seek to integrate their CAD/RMS applications with a dedicated identity service that might better meet agency MFA needs.

- **Support for identity federation protocols:** To support authenticator reuse, agencies should consult their CAD/RMS vendors to determine if their product implements identity federation standards as mentioned in Sec. 2.4. These protocols allow for the passing of identity information in a trusted and secure fashion between networked systems and may reduce the need for MFA to be implemented at downstream applications or resources. For example, if a user has successfully completed MFA at the CAD/RMS, that successful authentication could be conveyed to a state message switch via federation protocols rather than having the user complete a secondary authentication at the switch. This promotes the ability to reuse the initial MFA and can help reduce the number of credentials that users need to manage.

  If CAD/RMS applications do not support identity federation, agencies should consider the potential burden on users should they have to manage multiple MFA credentials and seek to minimize that burden when reasonable.

- **Avoiding the passing of memorized secrets:** When CAD/RMS applications send user queries to the state message switch, agencies should consider solutions that do not require the passing of memorized secrets between the CAD/RMS application and the state message switch, as described in Sec. 3.1.3. Instead, identity information (which might be needed downstream for auditing and logging) could be passed to the message switch using identity federation protocols such as SAML or OpenID Connect.

Note: Appendix C provides a sample list of questions for agencies to ask their CAD/RMS vendors about their MFA implementations.

3.4.1.2. MFA Implemented at Local Agency Identity Service

As detailed in Fig. 8, agencies may choose to integrate their CJIS applications and resources with a dedicated identity service.

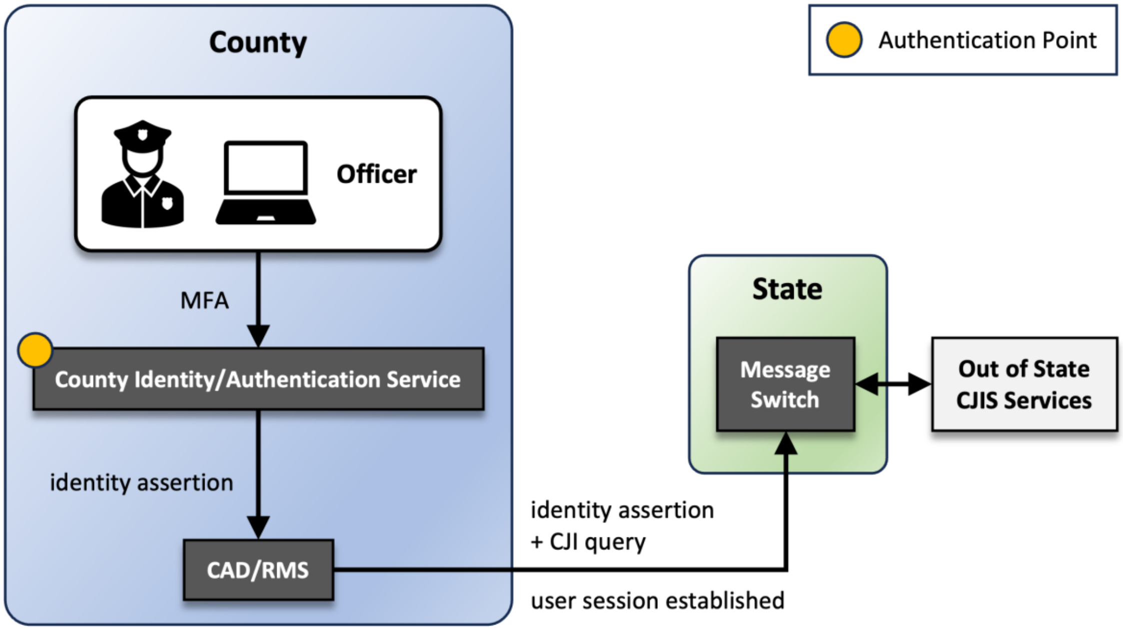


Fig. 8. Local agency identity service Integrated with CAD/RMS using identity federation.

Agencies choosing to implement an MFA solution provided by an identity service vendor should consider a few key architecture elements:

- **Which authenticator types the identity service offers:** These services are generally able to maximize authenticator optionality and reusability since they emphasize providing more features and functionality. As mentioned previously, agencies should consult their identity vendors to determine the types of authenticators—including phishing-resistant authenticators—supported by the identity service. It is recommended that agencies receive a demo of each authenticator type and request that the vendor provide details as to how each authenticator meets AAL2 requirements. Agencies should also inquire about technical documentation, instructions, and communication resources the vendor may have that can support an MFA deployment.

- **Support for integrating applications:** Since identity service providers are commonly external to the applications they provide services to, agencies will need to determine how the identity service will integrate with CJIS applications. Agencies should inquire about support for federation protocols and Kerberos, as well as SSO capabilities.

Appendix B provides technical details and guidelines for integrating CAD/RMS systems using federated architectures.

> **Note:** Both message switches and CAD/RMS applications may have to support compatible federation or token-based protocols for a successful integration. These protocols allow for the sharing of identity information between all these systems without sharing passwords.

3.4.1.3. MFA Implemented by a State Identity Service for Use by Local Agencies

State agencies that have already implemented MFA may decide to offer an MFA service to local agencies within their jurisdiction, as shown in Fig. 9. This model might be offered only to small or rural agencies who may lack the necessary funding and/or knowledge to implement MFA on their own, or the state might consider a shared service model where identity services are offered to all eligible and interested agencies within the state. Such an approach could result in economies of scale that could save costs for both state and local agencies and could also reduce the number of MFA architectures and implementations needed across the state. Establishing a state-shared service might also afford agencies greater ability to influence vendor capabilities and updates, including updates to support standards and best practices for MFA.

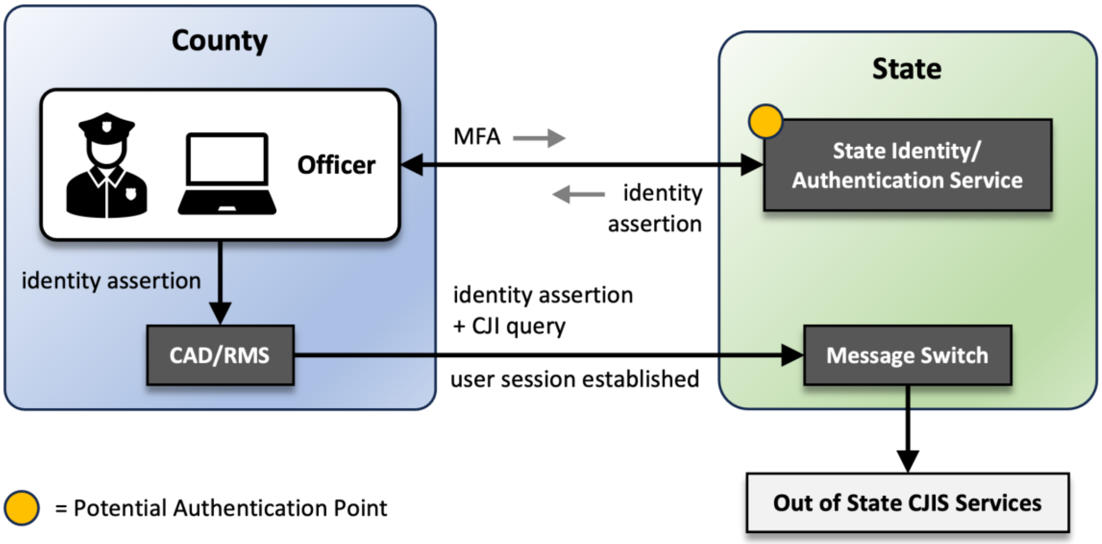

County
Officer
identity assertion
CAD/RMS
MFA
identity assertion
identity assertion + CJI query
user session established
State
State Identity/ Authentication Service
Message Switch
Out of State CJIS Services
● = Potential Authentication Point

Fig. 9. State-provided identity service for use by a local agency.

A few key considerations should be noted about this model:

- The identity service would be owned and operated by the state; however, the state may grant local agencies permission to manage their own employees within the state identity service.
- To integrate with local CJIS applications and limit the passing of secrets in a shared service model, both the state identity service and the local applications will likely need to support identity federation protocols. Appendix B.4.1 and B.4.2 provide technical details and guidelines for integrating architectures when the identity services at the state support both local agency (county or city) and state employees.
- Additionally, state agencies seeking to implement this model will need to enumerate MFA requirements and use cases from their local agency jurisdictions and should work with their vendor to determine the authenticator optionality that might meet these requirements.

3.4.2. State MFA Deployments

In addition to applications like CAD/RMS, most states have a portal—managed and run at the state level—through which authorized users across the state can access CJI. Figure 10 demonstrates an architecture commonly seen when accessing CJI through a state portal. Authentication might be provided by the portal application itself, or the portal could be integrated with an identity service.

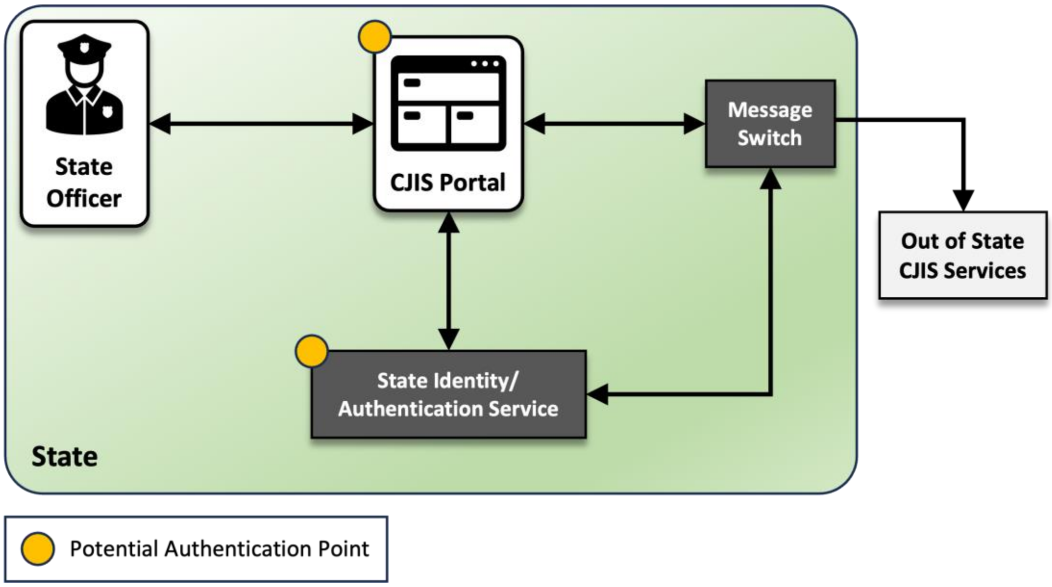

State Officer
CJIS Portal
Message Switch
Out of State CJIS Services
State Identity/ Authentication Service
State
Potential Authentication Point

Fig. 10. Common technology in state portal deployment.

3.4.2.1. MFA Implemented Directly with State Portal

Considerations for implementing MFA directly with state portal applications are similar to those discussed in Sec. 3.4.1.1 around implementing MFA directly with CAD/RMS applications. A common architecture is depicted in Fig. 11. Agencies should consider authenticator optionality and reuse when implementing MFA directly at a state portal application. Agencies will need to consult their portal vendor to determine which authenticator options might be available and determine if those options will meet the needs of the user base across the state.

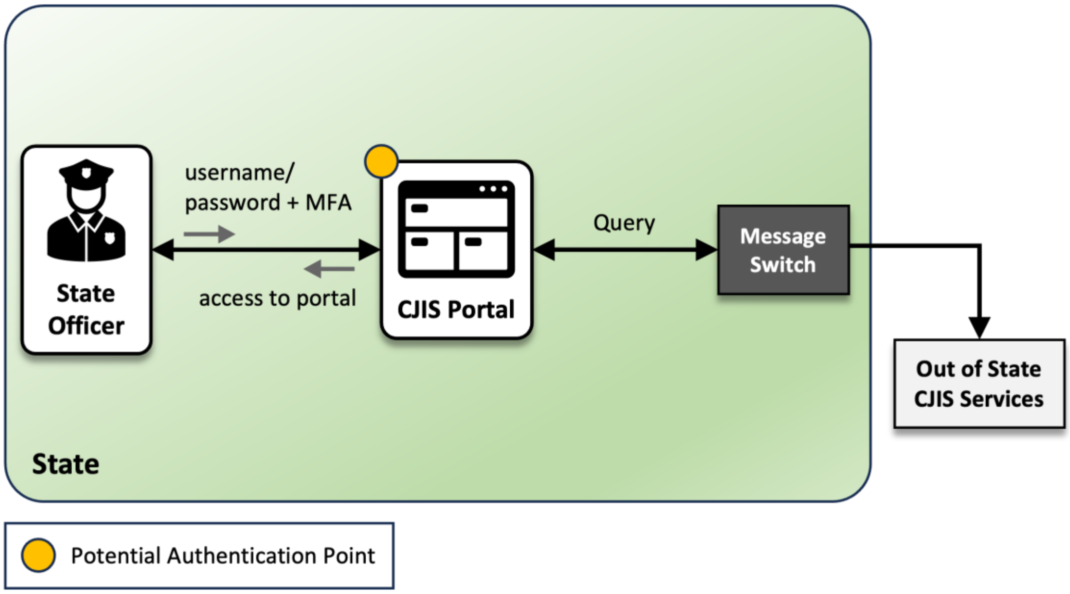


Fig. 11. Common architecture for implementing MFA directly with state portal.

Since state CJIS portals often provide services to users across the state, agencies should offer multiple MFA options to meet user needs. For example, if the state portal offers a software one-time passcode (OTP) option via an application installed on a mobile device, that solution may not meet the needs of department of corrections facilities that do not allow mobile devices into secure facilities. Since state portal applications are not dedicated identity providers, direct MFA integration will likely not provide MFA reuse. Where possible, agencies should consider implementing identity federation protocols that can integrate with identity services across the state and allow users to bring their own identity if they have already authenticated using MFA. See Appendix B for more information on implementing identity federation.

Additionally, state CJIS portals will need to integrate with the state message switch to submit queries to resources out-of-state (and, depending on the implementation, possibly other in-state resources as well). If the portal sends user queries to the state message switch, agencies should consider solutions that do not require the passing of memorized secrets, such as passwords, as described in Sec. 3.1.3. Agencies should look towards identity federation protocols or other token-based systems that can support this integration.

3.4.2.2. MFA Implemented at State Agency Identity Service

Alternatively, agencies may seek to integrate their state portal with a dedicated identity service platform, as Fig. 12 depicts. This option will likely provide agencies with a greater level of authenticator optionality and potential for authenticator reuse.

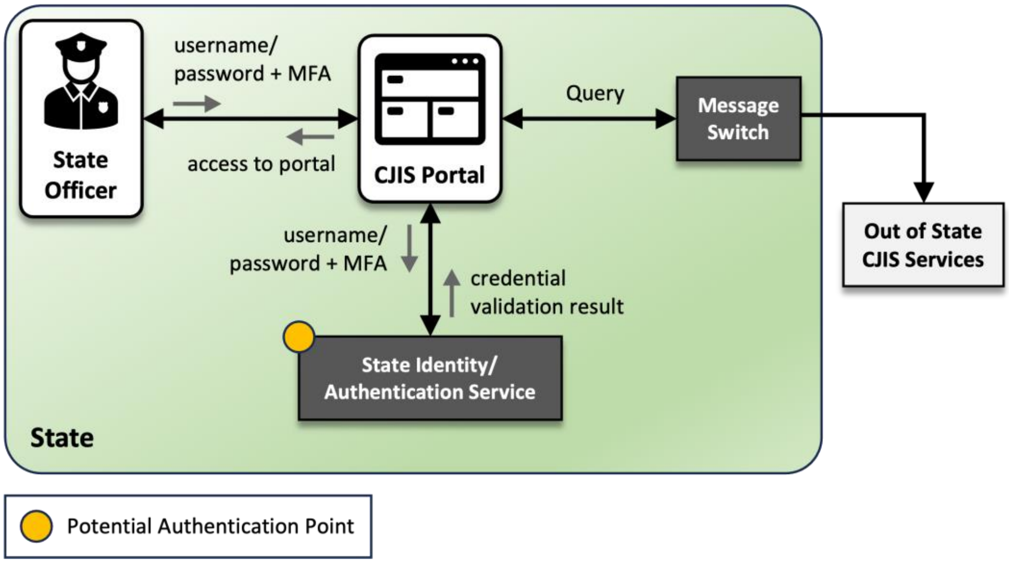

State Officer
username/ password + MFA
access to portal
CJIS Portal
Query
Message Switch
Out of State CJIS Services
username/ password + MFA
credential validation result
State Identity/ Authentication Service
State
Potential Authentication Point

Fig. 12. Common architecture for implementing MFA at state agency identity service.

Agencies should consult with their vendor to determine which authenticator types—including phishing-resistant authenticators—are supported, as well as which identity federation protocols the vendor can implement. State agencies should discuss with vendors and local jurisdictions the possibility of integrating the state identity solution with local agency identity services so that local agency users accessing the state portal can reuse any MFA they have implemented at their home agency.

Tip: State agencies commonly manage user accounts and credentials for their state CJIS portal, serving as the IdP for users across the state. The cost of this function, both in upfront costs of procuring and implementing MFA and in ongoing costs in help desk support and authenticator lifecycle management, might be alleviated if local, tribal, and territorial agencies had the option to integrate their local identity services with the state portal using identity federation protocols. Section 3.4.2.3 details an example architecture that supports this functionality.

3.4.2.3. MFA Implemented in a State-Provided Dashboard

In addition to CJI, agencies may have other data, applications, or resources that warrant the use of MFA. Commonly, enterprises seek to integrate applications with an application dashboard that can serve as a front-end, providing a single interface for users to access multiple applications and act as a centralized point for implementing MFA.

Figure 13 shows a state-hosted application dashboard that integrates several applications, including a CJIS portal that can be accessed by both state and local users. Many dashboard vendors are also identity services providers that support a variety of MFA authenticators and identity federation protocols. Agencies could leverage the identity and authentication services native to the dashboard or integrate the dashboard with existing agency identity services and allow the dashboard to provide an SSO service. Either way, the user would authenticate once using MFA and use SSO to access all applications available on the dashboard.

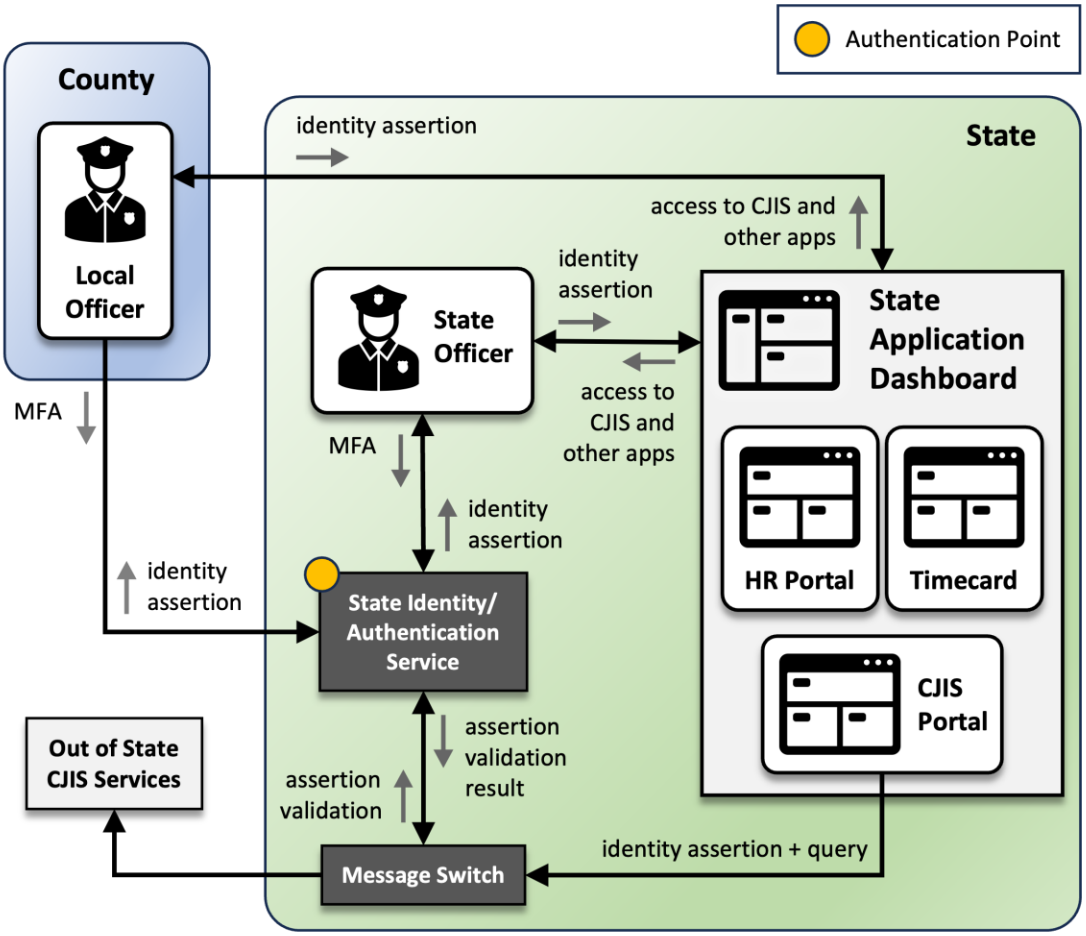

Authentication Point
County
Local Officer
State
identity assertion
access to CJIS and other apps
identity assertion
State Officer
access to CJIS and other apps
State Application Dashboard
HR Portal
Timecard
CJIS Portal
MFA
MFA
identity assertion
identity assertion
State Identity/ Authentication Service
Out of State CJIS Services
assertion validation result
assertion validation
identity assertion + query
Message Switch

Fig. 13. State application dashboard.

Appendix B.4.1 and B.4.4.1 provide technical details and guidelines for integrating architectures when the state implements an application dashboard to support both local (county or city) and state employees. This model promotes authenticator reuse through SSO and authenticator optionality via integrated identity services. It also offers the potential to create a shared service model where economies of scale in pricing might be realized by bringing multiple jurisdictions under a single service. A single identity service that multiple agencies can leverage also has the potential to limit the number of architectures and integration models needed across a state.

Note: Many states likely have small and rural agencies that lack the ability to implement MFA on their own. To support these agencies and to ensure that all users accessing CJI within a state are using MFA, state agencies should consider offering shared identity services that local agencies can opt into. Additionally, if local agencies choose to implement their own MFA, they should be provided an option to integrate with the state service using identity federation protocols.

⚠ **Caution:** Some agencies may find that their state already owns and operates an application dashboard for non-CJI applications that could be integrated with CJIS applications. This option may save agencies time and money. However, if the application dashboard is managed by a non-criminal justice agency, the contracting agency must make sure that a Security Addendum or Management Control Agreement is in place to ensure that the application or service meets CJIS Security Policy requirements and that administrative rights for managing access to CJIS applications are given only to those personnel who are authorized to access CJI.

3.4.3. Implementing MFA with VPNs

Almost all agencies use a VPN service to provide secure communications when accessing agency networks. Because of this, agencies may seek to leverage MFA solutions offered by their VPN providers. In this situation, it is important that agencies consider not only how MFA is integrated with their VPN service but also how users will access the CJIS application after they have successfully completed authentication and gained network access.

Figure 14 details a VPN architecture that also provides MFA services. In this example, the user authenticates to the VPN service by presenting a password, which is validated with agency directory services, along with a second authentication factor, which is validated with the MFA server. The MFA server may have several options for second factors, such as a hardware token or a software one-time code. Once the user successfully completes the MFA challenge to gain network access, they are subsequently asked to present a username and password when accessing the CJIS application.

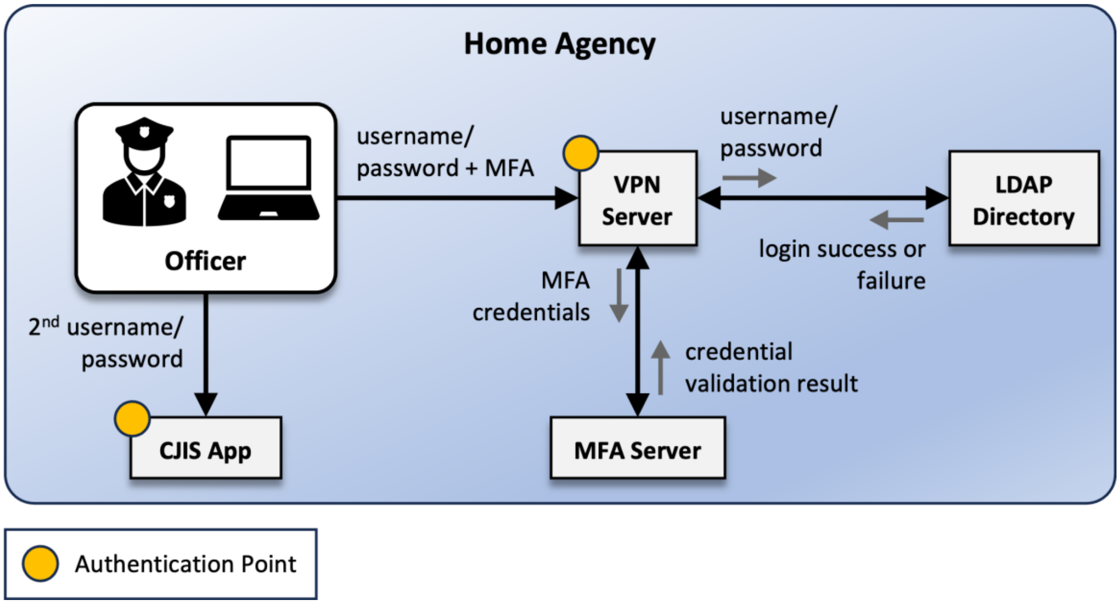


Fig. 14. VPN with MFA is not integrated with the CJIS application.

In the above example, the user must authenticate twice: despite having already completed MFA, they still need to maintain and use a secondary password with the CJIS application. This occurs because the MFA implementation is “in front” of the CJIS application but not integrated with it, resulting in MFA being enforced at the network but not at the application. If a bad actor were to get agency network access, the CJIS application might be vulnerable to phishing, brute-force password guessing attempts, or password database breaches. This architecture also does not prevent CJIS application password sharing or misuse among insiders with legitimate VPN credentials. To minimize these risks and to promote authenticator reuse, agencies should seek to integrate their CJIS application with an identity service that eliminates the need for a secondary username and password. The following sections offer two examples of how this might be accomplished.

⚠ **Caution:** Agencies may meet their MFA requirements through a VPN service, but they should avoid presenting users with a secondary single-factor authentication when accessing CJIS applications on the network.

3.4.3.1. Integrating VPN-Based MFA with CJIS Applications Using Kerberos

Figure 15 shows how MFA implemented at a VPN service might be integrated with a CJIS application using Kerberos SSO.

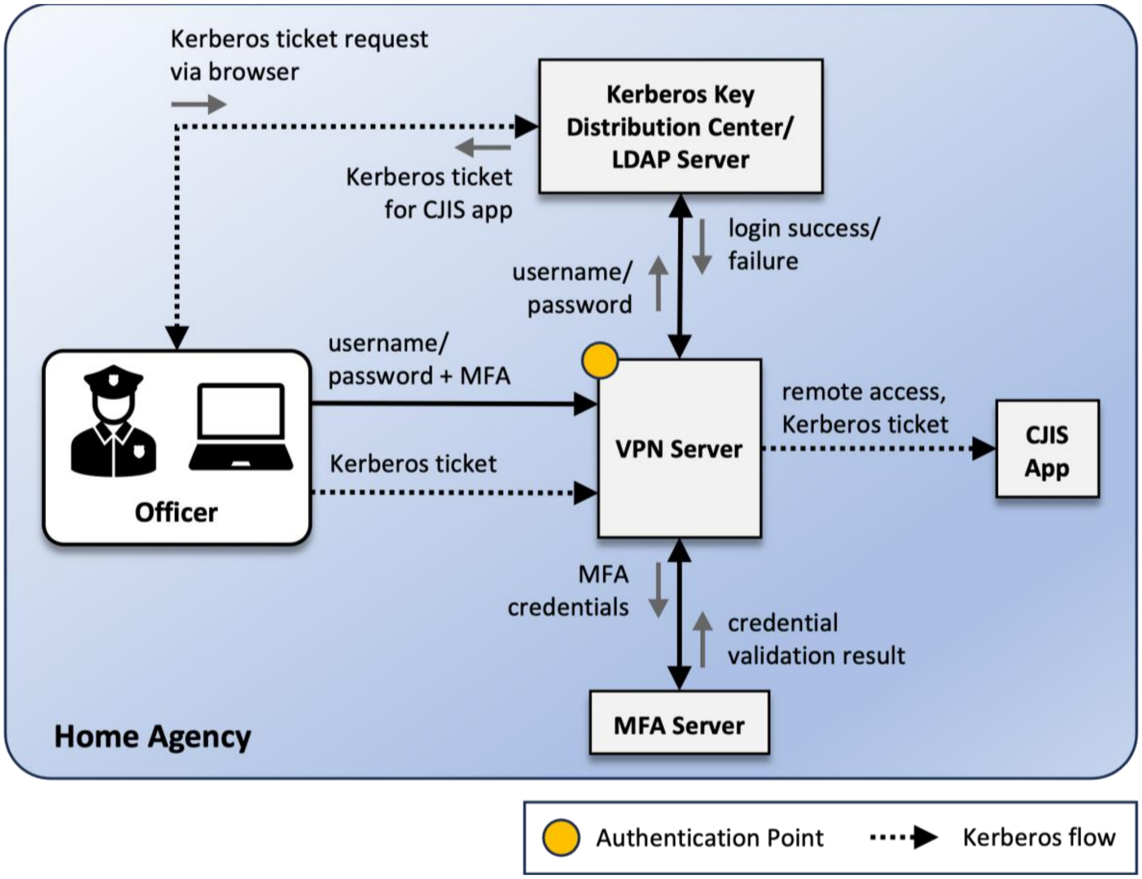


Fig. 15. Integrating MFA for a VPN with Kerberos.

In this model, the user authenticates to the VPN service by presenting a password, which is validated with agency directory services, along with a second authentication factor, which is validated with the MFA server. Once the user is on the network and navigates to the CJIS app, the user is redirected to the key distribution service. This service recognizes that the user has already authenticated and issues the user a Kerberos ticket with a session key. The user's system can then present this ticket to the CJIS application to establish a session without the need for a secondary authentication. Appendix B.5.1 provides technical details and guidelines for integrating architectures for VPN integration with Kerberos.

⚠ **Caution:** Any agency implementing Kerberos should be aware of "Kerberoasting" attacks. Similar to password brute-force attacks, if an attacker can gain access to a legitimate user account, they may try to escalate privileges by requesting Kerberos tickets for service accounts and perform an offline brute-force attack to try and obtain control of service account credentials. Since service accounts do not have MFA controls protecting them, agencies should implement strong service account password length requirements as well as avoid weaker encryption algorithms such as RC4 [7].

3.4.3.2. Integrating VPN-Based MFA with CJIS Applications Using Identity Federation

Identity federation protocols offer another approach to integrating a VPN service with a CJIS application. Figure 16 shows the VPN redirecting the user to an IdP for authentication. Upon successful authentication, the IdP issues the user an identity assertion—typically OpenID Connect or SAML federation tokens—that can be used to establish sessions with both the VPN server and the CJIS application. With this approach, users do not need to manage a secondary credential, and there is no need for the CJIS application to manage credentials. Appendix B.5.2 provides technical details and guidelines for integrating architectures for VPN integration using identity federation.

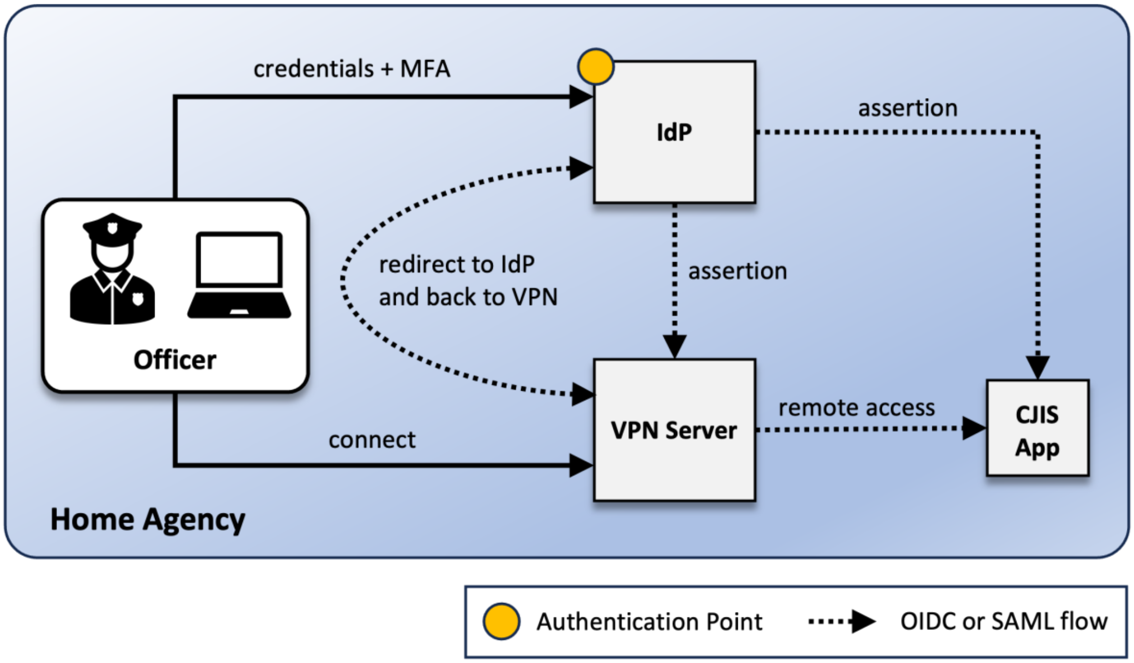


Fig. 16. Integrating MFA for a VPN with federation.

Note: The approach illustrated in Fig. 16 requires the IdP to be publicly accessible so that users can connect to it before the VPN connection is established. Identity-as-a-Service providers generally offer publicly accessible IdP services. Self-hosted IdP services are frequently not publicly accessible, depending on the agency's risk analysis and implementation.

4. Key Takeaways

This section collects the key takeaways for agencies from throughout the document.

Section 1, Introduction:

- Many of the challenges discussed in this document require collaboration between state, local, tribal, and territorial (SLTT) agencies, as well as collaboration with law enforcement technology providers. Engage all relevant stakeholders to discuss MFA implementation plans to ensure this collaboration can occur. All questions about how a specific MFA implementation can meet the CJIS Security Policy should be directed to the FBI CJIS ISO team at iso@fbi.gov. (from Sec. 1.2)

Section 2, An Introduction to MFA Technologies and Concepts:

- Because the compromise of CJI would significantly impact agencies across the country, the CJIS Security Policy requires that CJI be protected by MFA at AAL2 or greater. Agencies should reference the Identification and Authentication section of the CJIS Security Policy (versions 5.9.2 or later) for specific requirements. (from Sec. 2.2)
- When deploying an MFA solution, consider where users might get authentication, credential lifecycle management, and identity assertion issuance services from. In other words, decide where the IdP resides in the overarching MFA architecture, who owns and operates the IdP, and which of the services it will provide. (from Sec. 2.3)
- Work with the agency's technology vendors, specifically CAD/RMS, state message switch, and identity services vendors, to confirm they support identity federation protocols and architectures. (from Sec. 2.4.1)
- Consider integrating both CJI and non-CJI applications with an SSO service to gain additional return on investment and to provide users with a common authentication experience across applications. Agencies interested in implementing SSO should work with their technology vendors, specifically CAD/RMS, state message switch, and identity services vendors, to confirm they support SSO protocols and architectures. (from Sec. 2.4.2)
- Implement phishing-resistant MFA at AAL2, given the prevalence of phishing attacks. (from Sec. 2.5)

Section 3, Considerations for Implementing MFA to Protect CJI:

- To the greatest extent feasible, consider MFA architectures that minimize the number of separate MFA credentials that need to be issued to users and managed. Agencies should consider integrating CJI applications and/or services with existing IdPs that can or already support MFA. (from Sec. 3.1.1)
- Agencies will benefit if their MFA solutions support multiple authenticator types and methods. This allows organizations to select the type of authenticator that best meets the needs of a given user base, context, or environment in which CJI is accessed.

Generally, the greatest level of MFA optionality is offered by dedicated identity service providers. (from Sec. 3.1.2)

- Consider solutions that do not require passing memorized secrets across networked systems and amongst applications. Token-based systems such as Kerberos and identity federation protocols are viable options for integrating CJI applications and/or services with other applications and identity services. (from Sec. 3.1.3)
- When deploying an MFA solution, ensure that the MFA implemented is integrated with the application or service that contains CJI. Ideally, CJI applications would be tied into an SSO service or directly integrated with an identity service such that the MFA completed at the network level can be enforced at the application level. (from Sec. 3.1.4)
- When an agency is choosing its approach to MFA implementation, it should do the following (from Sec. 3.2):
    - Conduct a requirements assessment to help determine the MFA solution that will best meet agency needs. It is critical that agencies understand the common use cases and corner cases of the user population the MFA solution is intended to support.
    - Consult with other agencies within the state (state, local, tribal, and/or territorial) to discern ways in which MFA requirements may be met through collaboration.
    - Consult legal teams to identify legal restraints, including state privacy laws, impacting which MFA authenticator types they can use.
    - Work with technology vendors, including identity service providers and message switch, VPN, and CAD/RMS vendors, to determine how they can best support an MFA solution that meets agency requirements. (See Appendix C for vendor questionnaires.)
- Deploy MFA in phases and seek to grow user MFA adoption over time. It is unrealistic to expect that all or even a large majority of users will adopt an MFA solution as soon as it is available. (from Sec. 3.3)
- In general, seek to implement MFA once and then layer on supporting technologies such as identity federation or SSO to extend the value of that initial MFA implementation. Choosing to implement MFA at multiple points in the architecture could result in increased technology costs as well as an increased burden on users who need to manage and utilize multiple MFA credentials. See Appendix B for an in-depth look at MFA implementations based on federated identity architectures. (from Sec. 3.4)

References

[1] U.S. Department of Justice (2024) Criminal Justice Information Services (CJIS) Security Policy, Version 6.0. CJISSECPOL v6.0. Available at https://le.fbi.gov/file-repository/cjis_security_policy_v6-0_20241227.pdf

[2] Wisconsin Law Enforcement Network (2024) Public Safety Threat Report: 2024 Threat Landscape. https://wilenet.widoj.gov/sites/default/files/public_files-2025-02/ijis-2024-threat-landscape-report.pdf

[3] Temoshok D, Proud-Madruga D, Choong YY, Galluzzo R, Gupta S, LaSalle C, Lefkovitz N, Regenscheid A (2025) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-4. https://doi.org/10.6028/NIST.SP.800-63-4

[4] Temoshok D, Fenton JL, Choong YY, Lefkovitz N, Regenscheid A, Galluzzo R, Richer JP (2025) Digital Identity Guidelines: Authentication and Authenticator Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63B-4. https://doi.org/10.6028/NIST.SP.800-63B-4

[5] Regenscheid A, Galluzzo R (2023) Phishing Resistance – Protecting the Keys to Your Kingdom. https://www.nist.gov/blogs/cybersecurity-insights/phishing-resistance-protecting-keys-your-kingdom

[6] Cybersecurity and Infrastructure Security Agency (2025) List of Federal Financial Assistance Programs Funding Emergency Communications. https://www.cisa.gov/safecom/emergency-comms-grants-list

[7] Weston D (2024) Microsoft's guidance to help mitigate Kerberoasting. (Microsoft Corporation, Redmond, WA.) Available at https://www.microsoft.com/en-us/security/blog/2024/10/11/microsofts-guidance-to-help-mitigate-kerberoasting/

[8] Fisher W, Russell M, Umarji S, Scarfone K (2021) Background on Identity Federation Technologies for the Public Safety Community. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report 8336. https://doi.org/10.6028/NIST.IR.8336-draft

[9] Grassi PA, Nadeau EM, Richer JP, Squire SK, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Federation and Assertions. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63C, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63C

Appendix A. Technology Components Relevant to MFA for CJIS Access

This appendix outlines some of the technology components currently deployed by agencies to support their public safety missions. Some of these components may have to be upgraded to meet CJIS MFA requirements and have been referenced in this document. This appendix includes a brief description of each component.

- The **computer-aided dispatch (CAD) system** is the principal application used by public safety agencies to manage law enforcement, fire, and emergency medical services (EMS) incidents from the initial time an incident is reported to the conclusion of the incident. CAD is also used to track the status and location of resources and for post-incident analysis of the response. A CAD system consists of either a single software application or a suite of integrated software packages used to initiate a public safety call service record, dispatch and maintain the status of responding units and resources in the field, and generally manage the incident. It is typically used by emergency communications dispatchers, call takers, and telecommunicators in public safety communications centers. Modern CAD systems are usually extended out to field personnel (responders) through their mobile digital computers (MDCs), remote connections, and/or other mobile devices such as smartphones. Some CAD systems enable the user to query local and national databases containing CJI. CAD systems may also embed a message switch plug-in to enable interoperability with a state message switch.
- A **record management system (RMS)** is an agency-wide system that provides for the storage, retrieval, retention, manipulation, archival, and viewing of information, records, documents, and other files pertaining to law enforcement operations. Such records include incident and accident reports, arrests, citations, warrants, case management, field contacts, and other operations-oriented records. Some agencies integrate CAD and RMS into a single function referred to as CAD/RMS.
- **Message switch systems** are generally installed in agencies or bureaus within state government and are often housed within the state police, a cabinet-level agency such as the Department of Public Safety, or the Attorney General's Office. These message switches are a hub through which all users in a state access information in other states. These message switches support the format and protocols native to each connecting system, such as FBI CJIS, Nlets, DMV IT systems, and state hot files.
- Specialized third-party **middleware solutions** are used by some agencies to facilitate continuous, efficient communication and data exchange between systems that require different data formats. Such middleware commonly sits between the CAD/RMS system and a downstream message switch to ensure compatibility and interoperability between them. The middleware typically has no direct user interface; therefore, the user interface is provided by a CAD/RMS application. The middleware stores configuration information, processes scripts, etc., and can convert data from the CAD/RMS format to the message switch format that the message switch can understand.

Appendix B. Federated Identity Architectures

As described in Sec. 2.4, although MFA enhances security, there are both monetary and user friction costs to MFA implementations. Technologies such as identity federation can help to alleviate these costs by reducing the number of credentials a user needs to manage, reducing the number of times a user needs to authenticate, and allowing users to reuse a single authentication to get access to multiple applications and/or resources. Section 3.4 describes common architectures that agencies are likely to consider when implementing an MFA; many of those solutions are based on federated identity architectures. This appendix provides detailed technical information regarding these architectures.

Though federated identity is not a new concept, very few agencies that access CJI have implemented this technology. Federation can be incorporated into the current authentication and message routing infrastructure to communicate user identity and attributes.

This section uses terms related to the authentication and authorization standards SAML, OIDC, and OAuth 2.0. These terms include identity federation, IdP, RP, and several others. For an introduction to these terms, please refer to Draft NIST IR 8336, *Background on Identity Federation Technologies for the Public Safety Community* [8].

B.1. Establishing Federation Trust

Before an RP application can interact with an IdP or authorization server using federation protocols, a relationship must be established and configured between the RP application and the IdP. Establishing this relationship typically involves both technical and administrative requirements. On the administrative side, the organization that owns the IdP and the organization that owns the RP will need to establish a trust relationship. This may include establishing points of contact between the organizations, security agreements or memoranda, or a service contract if the IdP is a commercial service provider. The technical aspects of integration include providing the IdP's public signing key to the RP application so that it can verify the signatures on assertions. The RP may also optionally provide a public key to the IdP to use for encryption of assertions. Protocol options, such as which bindings will be used, must be configured along with the relevant URLs and endpoints for each system. SAML defines a metadata standard that IdPs and RP applications can use to generate an XML document containing the public keys and required parameters to enable automated configuration of a SAML connection.

Definition: "Trust" has multiple meanings in federation. Cryptographic trust is established through a public key that can be used to validate digital signatures provided by an IdP or other system. It provides assurance that a message came from a known entity, is genuine, and has not been altered. Federation partners also establish trust in the more traditional sense of assurance that each partner follows standards and policies and behaves in a reliable, trustworthy way. This type of trust may be formalized in contracts or trust frameworks.

Public keys for SAML IdPs and RPs are typically communicated using X.509 certificates. However, in most cases it is not necessary to establish or use a trusted certificate authority to issue certificates for SAML signatures or encryption. When certificates are used to assert the identity of a website or an email address, accepting only certificates from trusted certificate authorities is critical. When establishing a SAML integration, however, trust is explicitly established in a specific signing or encryption key; it is not inherited from a trusted authority.

Message switches today do not commonly support SAML for user authentication. Switch vendors may take different approaches to SAML implementation. A SAML assertion could be used to authenticate a user and initiate a session for a defined period during which the user could submit multiple queries. Other designs are possible; for example, the switch might not maintain session state and instead might require a SAML assertion to be sent along with each individual query. The approach may be dependent on the specific vendor technology and implementation.

The rest of this appendix covers the following topics:

- Challenges in using federation technologies for message switch use cases (Appendix B.2)
- Meeting FAL requirements in complex federation scenarios (Appendix B.3)
- Options for federated architecture configurations (Appendix B.4)
- VPN integration (Appendix B.5)

B.2. Challenges in Using Federation Technologies for Message Switch Use Cases

In a typical federation architecture, there are three parties: the user, the IdP, and the RP (for example, a CAD/RMS system). The IdP provides a user identity assertion containing proof of authentication and identity information to the CAD/RMS system. If the CAD/RMS system needs to connect to a message switch for access to CJI, the message switch also needs user identity information, but it does not fit into the typical user/IdP/RP scenario. The message switch is "behind" the RP, and the user has no direct communications with it. Figure 17 illustrates this scenario.

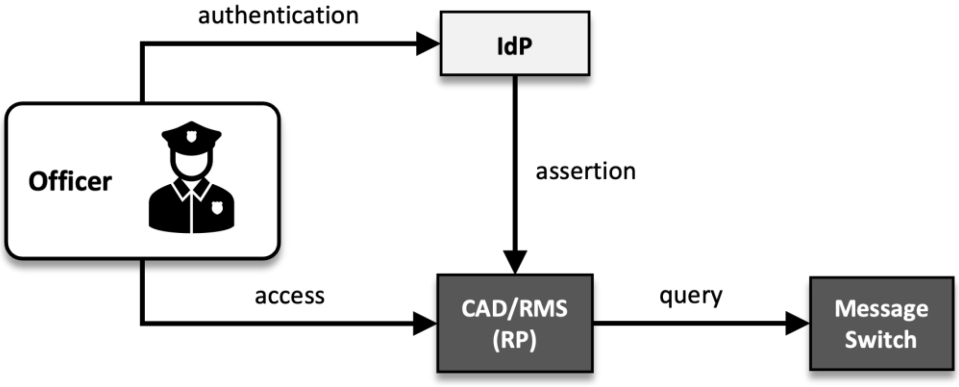


Fig. 17. Federation in a message switch use case.

It would seem efficient for the CAD/RMS system to simply forward the assertion it has received from the IdP on to the message switch to securely convey the user information. RPs cannot forge or alter assertions since the IdP digitally signs them, so the assertion can still be trusted despite passing through the RP on its way to the message switch. However, forwarding assertions in this way can introduce vulnerabilities, and security mechanisms built into federation protocols can render this approach infeasible. These mechanisms include:

- **Audience Restrictions** – OIDC and SAML implement an "audience" parameter to indicate which RP is the intended recipient of the assertion. RPs check the audience parameter of any assertion they receive and reject assertions that do not contain their identifier as the audience. Without audience restrictions, a valid assertion could be passed on to any RP that trusts the IdP. Malicious or compromised RPs, or attackers who manage to intercept valid assertions, could use them to impersonate the authorized user to any RP. In Fig. 17, the audience of the assertion is the CAD/RMS system. If this assertion is passed to the message switch, the message switch should recognize that it is not the intended audience and reject the assertion. NIST SP 800-63C [9] requires that assertions include audience restrictions and that RPs enforce them.
- **Encrypted Assertions** – Assertions can be encrypted using the RP's public key or a symmetric key shared between the RP and IdP. Assertions are encrypted at the message layer, in addition to transit encryption provided by Hypertext Transfer Protocol Secure (HTTPS). NIST SP 800-63C requires encrypted assertions at Federation Assurance Levels (FAL) FAL2 and FAL3. In the message switch example above, the assertion would be encrypted using a key held by the CAD/RMS system. If the assertion is forwarded to the message switch, the switch will be unable to decrypt the assertion unless key material is shared between the CAD/RMS system and the message switch, which is in violation of standard cryptographic principles. The CAD/RMS system also cannot typically send the decrypted assertion to the switch, since SAML assertions are typically signed and then encrypted, and sending a decrypted assertion would violate security requirements.

In some environments, additional security measures, like proof-of-possession or holder-of-key assertions, would present additional obstacles to forwarding the assertion.

> **Definition:** In federation systems, the *audience* is the application or system that is meant to receive an assertion. If an officer logs into a CAD/RMS system using an IdP, the assertion's "audience" parameter will limit the use of that assertion to the CAD/RMS system. This can limit the damage an attacker could do by intercepting and using that assertion. They would be unable to forward it on to gain access to other agency systems or applications.

Applying federation technologies to the message switch scenario is challenging because it is not a traditional identity federation scenario, but rather delegated authorization. The CAD/RMS system initiates a transaction with the message switch on the user's behalf. The user is not directly involved in this transaction; they are one step removed from it. Authorization protocols like Kerberos and the OAuth 2.0 Authorization Framework are designed for these types of transactions. However, Kerberos is not typically deployed across organizational boundaries, and OAuth 2.0 is not yet widely deployed in the public safety environment. Therefore, this document presents two options for implementing this scenario with the widely used SAML 2.0 standards:

- **Proxy IdP** – A Proxy IdP accepts an assertion from an IdP and uses it to create its own assertion to provide to another RP, effectively acting as an IdP to that other RP. In the above example, the CAD/RMS system could use the identity information received in the assertion from the IdP to craft its own assertion, sign it with its own private key, and pass it on to the message switch, adjusting the audience parameter and other fields to reflect the intended use of this new assertion. Refer to Appendix A.3.1 of [8] for more details on the Proxy IdP concept.
- **WS-Trust** – WS-Trust is another federation standard that the CAD/RMS system can use to request a new assertion from the IdP that is intended to be presented to the message switch. The CAD/RMS system would send a WS-Trust Security Token Request to the IdP, providing the SAML assertion it received earlier, to obtain a new SAML assertion that is addressed to the message switch with the proper audience parameter value and optionally also encrypted with a key held by the message switch. Both the CAD/RMS system and message switch must be configured as RPs to the IdP in this scenario.

These two approaches are further described and illustrated in Appendix B.4.

B.3. Meeting FAL Requirements in Complex Federation Scenarios

NIST SP 800-63C addresses requirements for IdP proxies and states that when proxies are used, the FAL of the overall authentication flow is equal to the lowest FAL in use between participants in a proxy scenario. This means that it is possible to meet FAL2 and FAL3 in a Proxy IdP scenario as long as the requirements of the FAL are met through all interactions between the participants. NIST SP 800-63C does not address token exchange scenarios like the WS-Trust integration described above. However, the NIST SP 800-63C principles can be applied to this WS-Trust integration to achieve a similar level of trust.

> **Definition:** Federation Assurance Levels (FAL) are defined in NIST SP 800-63C and provide three security levels for federation implementations. Agencies use the guidelines in NIST SP 800-63-4 to choose the required FAL based on a risk assessment. The FALs can be summarized as follows:
>
> **FAL1:** Assertion digitally signed by the IdP
>
> **FAL2:** Assertion digitally signed by the IdP and encrypted
>
> **FAL3:** Holder-of-key assertion requiring the RP to prove possession of a cryptographic key

FAL2 requires that assertions be encrypted with a private key held by the RP. In the Proxy IdP case, this means that the assertion issued by the IdP to the CAD/RMS system must be encrypted using a key held by the CAD/RMS system, and the assertion issued by the CAD/RMS system to the message switch must be encrypted using a separate key held by the message switch. In the WS-Trust case, the assertion issued by the IdP to the CAD/RMS system must be encrypted using a key held by the CAD/RMS system, and the second assertion issued by the IdP to the message switch must be encrypted using a separate key held by the message switch. For WS-Trust, this would require the use of symmetric encryption between the IdP and the CAD/RMS system, since the CAD/RMS system sends the initial SAML assertion back to the IdP in the security token request and the IdP must be able to decrypt and read it.

FAL3 requires the use of holder-of-key assertions, which are bound to a public or shared key. When presenting a holder-of-key assertion, the presenter must prove possession of the key to which the assertion is bound, typically through mutual Transport Layer Security (TLS) authentication using a client certificate. In the Proxy IdP case, FAL3 could be met by having the user authenticate to both the IdP and the CAD/RMS system with the same client certificate, to which the assertion would be bound. The second assertion issued by the CAD/RMS system to the message switch would be bound to a client certificate held by the CAD/RMS system and used in mutual TLS authentication between the CAD/RMS system and both the IdP and the message switch. The FAL3 requirements for the WS-Trust example are similar, with the first assertion bound to the user's client certificate and the second assertion bound to a different certificate held by the CAD/RMS system.

The above discussion is focused on the core elements of the federation protocols as they apply to message switch scenarios. NIST SP 800-63C includes other requirements for FAL2 and FAL3 beyond those discussed here, such as cryptographic module requirements that must also be met for FAL2 and FAL3 compliance.

B.4. Federated Architectures for Access to CJI

State and local agencies have several options to consider when deciding how they deploy federated architectures to suit their requirements for access to CJI. This section presents several options that agencies might consider:

- Both the CAD/RMS web app and IdP at the state agency (Appendix B.4.1)
- CAD/RMS thick client at the county with the IdP at the state agency (Appendix B.4.2)
- Both the CAD/RMS web app and IdP at the county agency (Appendix B.4.3)
- Integrations with OAuth 2.0 and OIDC (Appendix B.4.4)

As described in Sec. 2.4.1, federation systems can be a central integration point for providing MFA to multiple applications.

B.4.1. Both CAD/RMS Web App & IdP at the State Agency

The architectures in this section describe a web-based CAD/RMS application (a web app) and a SAML IdP, both hosted by a state agency that is used by state, county, and other authorized local users within the state. The state also hosts a web-based application dashboard, which displays a list of applications available to each authenticated user based on their assigned authorizations and entitlements. One of the applications displayed in the list is the CAD/RMS web app. The application dashboard and CAD/RMS web app are both integrated with the IdP as

RPs. From a protocol perspective, federation can be achieved by using a SAML Proxy IdP or by implementing WS-Trust. Each of these options is described in more detail below.

B.4.1.1. Both CAD/RMS Web App & IdP at the State Agency – IdP Proxy

In the Proxy IdP approach, the CAD/RMS web app must be capable of acting as a Proxy IdP and generating a SAML assertion based on the assertion it receives from the state IdP. The CAD/RMS web app does not directly authenticate the user but rather trusts an assertion from the state IdP, to which the CAD/RMS web app is an RP, as shown in Fig. 18.

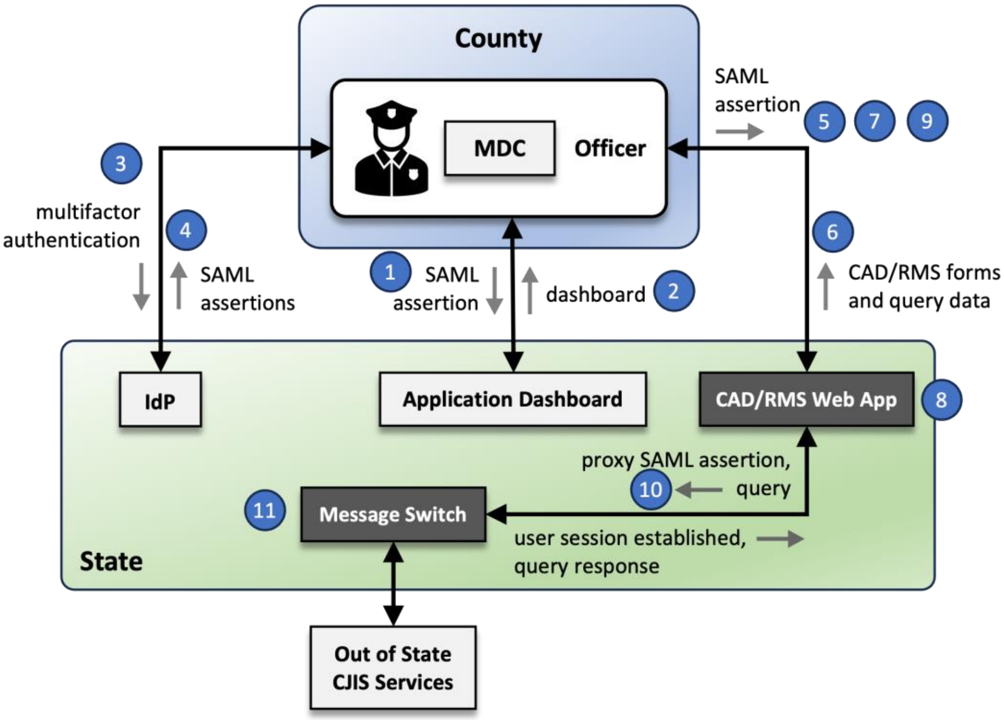


Fig. 18. Web app and IdP at state (SAML proxy).

It uses the user identifiers and other attributes it has received from the state IdP to create its own SAML assertion, sign it with its own key pair, and send this assertion to the state message switch. The state message switch must have an RP trust with the IdP function of the CAD/RMS web app, and it has no direct interaction with the state IdP. The sequence of interactions in this scenario is as follows:

1. The officer accesses the application dashboard.
2. The application dashboard redirects the officer to the IdP to authenticate.
3. The officer authenticates to the IdP with their credentials and MFA.
4. The IdP redirects the officer's browser to the application dashboard with a SAML assertion. The dashboard validates the SAML assertion, logs in the officer, and presents a set of application links based on their authorizations.

5. The officer clicks a link to the CAD/RMS system.
6. The CAD/RMS system redirects the officer's browser to the IdP to authenticate.
7. Since the officer has an active session with the IdP, they do not need to authenticate. The IdP redirects the officer's browser to the CAD/RMS system with a SAML assertion.
8. The CAD/RMS system validates the assertion and logs in the officer.
9. The officer submits a query to the CAD/RMS system.
10. The CAD/RMS system creates a new SAML assertion including the user identifiers and attributes it received from the IdP. The CAD/RMS system sends this new SAML assertion and the query to the message switch.
11. The message switch validates the assertion and extracts the user's identity and attributes. The message switch can use these attributes to authorize the query.

B.4.1.2. Both CAD/RMS Web App & IdP at the State Agency – WS-Trust

Unlike the previous section, this approach does not require the CAD/RMS web app to act as a SAML IdP. In accordance with industry best practices for SAML, SAML assertions should be targeted to a specific recipient using the audience parameter, as explained in Appendix B.2. Instead of forwarding a response already used to log into the CAD/RMS web app, a new SAML assertion is obtained that identifies the proper audience (the state message switch). Because the end user does not connect directly to the message switch, the standard SAML SSO profile cannot be used to obtain this assertion.

The WS-Trust specification provides a standards-compliant way for the CAD/RMS web app to request a SAML assertion directly from the IdP that it can present to the message switch. For this implementation, shown in Fig. 19, the state IdP must support the Security Token Service functionality of the WS-Trust protocol, and the CAD/RMS web app must support WS-Trust as a client.

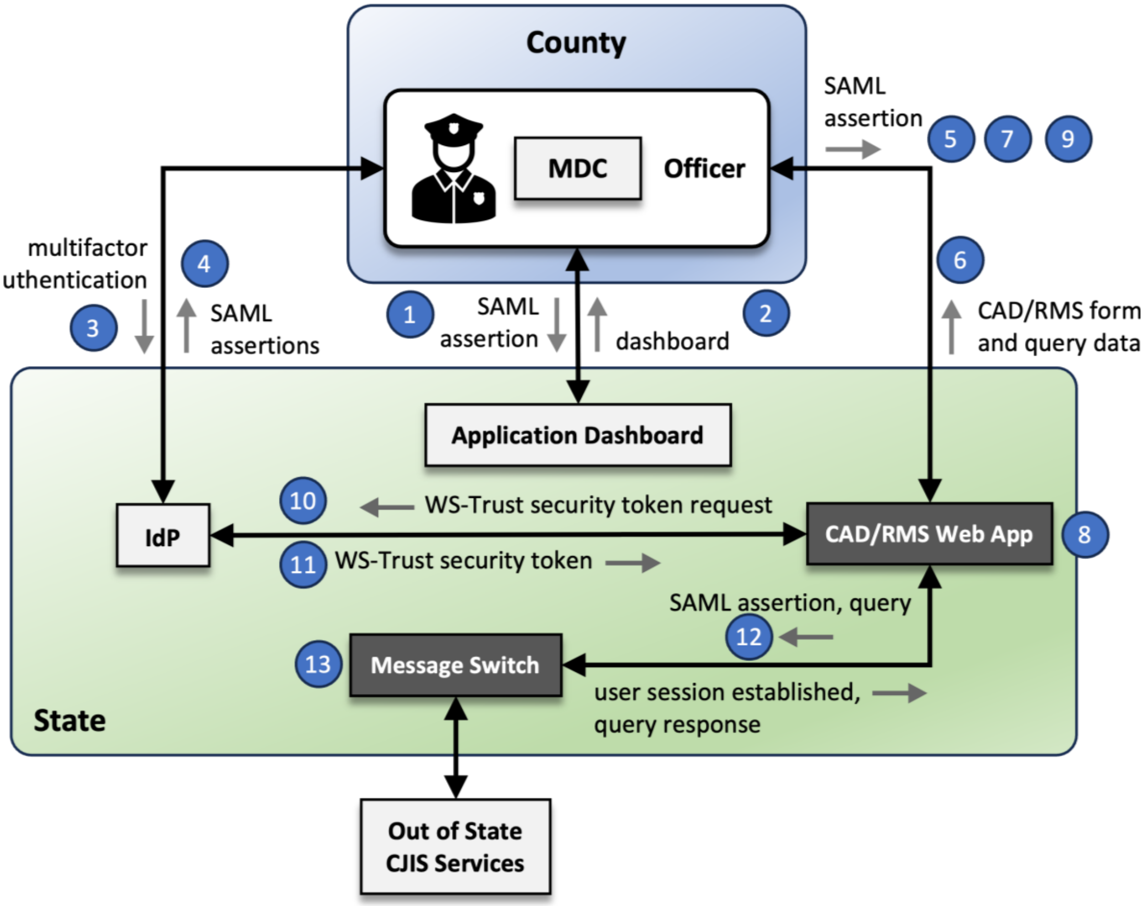


Fig. 19. Web app and IdP at state (WS-Trust).

The SAML and WS-Trust interactions in this scenario are as follows. Note that steps 1-9 are identical to those in the prior figure:

1. The officer accesses the application dashboard.
2. The application dashboard redirects the officer to the IdP to authenticate.
3. The officer authenticates to the IdP with their credentials and MFA.
4. The IdP redirects the officer's browser to the application dashboard with a SAML assertion. The dashboard validates the SAML assertion, logs in the officer, and presents a set of application links based on their authorizations.
5. The officer clicks a link to the CAD/RMS system.
6. The CAD/RMS system redirects the officer's browser to the IdP to authenticate.
7. Since the officer has an active session with the IdP, they do not need to authenticate. The IdP redirects the officer's browser to the CAD/RMS system with a SAML assertion.
8. The CAD/RMS system validates the assertion and logs in the officer.
9. The officer submits a query to the CAD/RMS system.

10. The CAD/RMS system sends a WS-Trust Security Token Request to the IdP, including the SAML assertion it received earlier in the onBehalfOf element to indicate that the request is for a token to present to the message switch on behalf of the previously authenticated user.
11. The IdP creates a new SAML assertion with the officer as the subject and with a suitable audience parameter for the message switch. The IdP returns this SAML assertion to the CAD/RMS system in a WS-Trust Request Security Token Response message.
12. The CAD/RMS system sends this new SAML assertion and the query to the message switch.
13. The message switch validates the assertion and extracts the user's identity and attributes. The message switch can use these attributes to authorize the query.

B.4.2. CAD Thick Client at the County with the IdP at the State Agency

This section considers the case where the CAD/RMS system is a client/server application hosted at the county level and accessed through a "thick client" software application installed on the MDC. For this section, we also assume that county users authenticate to a state-hosted IdP. The thick client introduces a challenge for SAML integration. The common SAML SSO interactions rely on web functionality such as HTTP redirect and POST messages and the use of a browser for interactive authentication to the IdP. However, the MDC operating systems typically provide mechanisms for thick client applications to interact with the web browser that can be used to implement SAML and other authentication and authorization protocols like OIDC and OAuth. Two types of interactions are required:

- The thick client application must be able to launch a web browser and direct it to the IdP's SSO service endpoint, supplying a SAML authentication request as a parameter. The browser provides the user interface for authentication to the IdP.
- After the user has authenticated to the IdP, the thick client application must receive a response from the IdP using one of the standard SAML bindings (typically redirect or POST). In either case, the browser must be able to send a message to the application.

Methods of accomplishing these operations are OS-specific. However, all common desktop OSs provide mechanisms for these actions. For example, applications can be registered with the OS to handle specific URLs either by defining a custom URL scheme (e.g., "vendor-name://") or by associating ordinary HTTPS URLs with the client application. With the OS configured to recognize the thick client application as the designated handler for specific URLs, the IdP can redirect the browser (or trigger it to submit a POST message) to one of the designated URLs, and the OS will provide the message along with any parameters and POST body to the client application. The thick client can then extract and process the response, including any SAML assertions, errors, or other protocol messages.

The following subsections present two variations on the thick client use case:

- Appendix B.4.2.1 describes a CAD/RMS thick client that supports SAML. It uses SAML to authenticate users and acts as an IdP proxy, creating a SAML assertion to pass to the message switch.
- Appendix B.4.2.2 describes a CAD/RMS thick client that does not support SAML. SAML is still used in the broader architecture, but the CAD/RMS thick client uses WS-Trust to obtain a SAML assertion to pass to the message switch.

B.4.2.1. CAD/RMS Thick Client at the County with IdP at the State Agency – IdP proxy

In this use case, the CAD/RMS thick client acts as an IdP proxy. The CAD/RMS system supports SAML for user authentication and can act as a SAML IdP proxy, as shown in Fig. 20.

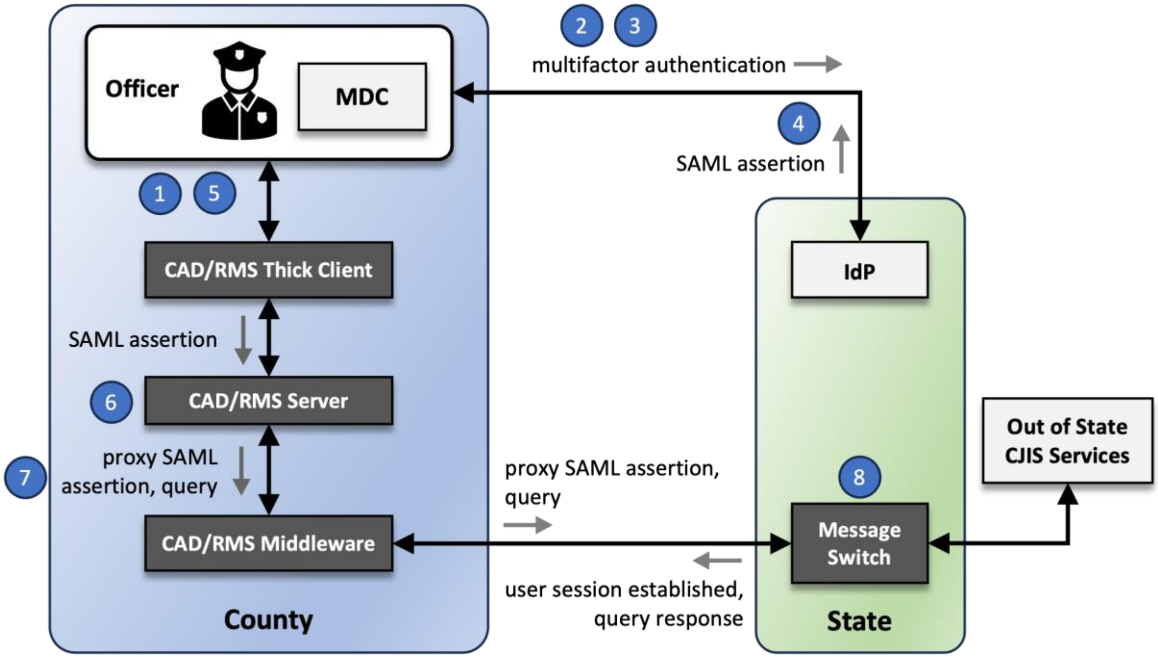


Fig. 20. Thick client CAD/RMS and Proxy IdP at county, state IdP.

The sequence of interactions is as follows:

1. The officer opens the CAD/RMS thick client application, which connects to the CAD/RMS server. The CAD/RMS server recognizes that the officer does not have an active session and responds to the CAD/RMS thick client with a SAML authentication request. The details of this interaction are proprietary and depend on the specific CAD/RMS application's design.
2. The CAD/RMS thick client opens the login URL of the state IdP in the built-in browser on the officer's MDC, sending the SAML authentication request as a parameter.
3. The IdP prompts the officer to log in with a username/password and issues an MFA challenge to the officer after validating the officer's login credentials.

4. The IdP validates the MFA challenge-response and creates a new user session for the officer, generates a SAML assertion, signs it with its private signing key, encrypts it with the CAD/RMS system's public encryption key, and returns it to the browser in a redirect to the CAD/RMS thick client.
5. The browser invokes the thick client and passes the SAML assertion to it. This is done by redirecting to a URL that is configured to be handled by the CAD/RMS thick client in the MDC's OS (e.g., using an app URI handler). The thick client sends the SAML assertion to the CAD/RMS server.
6. The CAD/RMS server decrypts the SAML assertion using its own private encryption key and validates the signature on the SAML assertion using the IdP's public signing key. The CAD/RMS server extracts the officer's account identifier and any other required attributes from the assertion and establishes the officer's session in the CAD/RMS application.
7. The CAD/RMS server generates a SAML assertion acting as a Proxy IdP using the user's identifiers and attributes received from the state IdP. It signs the assertion with its private signing key and encrypts it with the public encryption key of the message switch. The CAD/RMS server passes the SAML assertion and query parameters to the middleware layer. The middleware sends the SAML assertion to the state message switch.
8. The message switch validates the assertion and extracts the user's identity and attributes. The message switch can use these attributes to authorize the query.

B.4.2.2. CAD/RMS Thick Client at the County with IdP at the State Agency – WS-Trust

In this scenario, we assume that the CAD/RMS client/server system does not support SAML. We also assume that the user authenticates to the CAD/RMS system through some other means (e.g., Kerberos). To authenticate the user to the message switch, the CAD/RMS thick client redirects the user to a URL at the state IdP that triggers an IdP-initiated SAML authentication flow. The IdP responds with a SAML assertion, which the CAD/RMS thick client sends to the CAD/RMS server, which in turn makes a WS-Trust request to the state IdP to obtain a SAML assertion that it can present to the message switch. The CAD/RMS server is not required to create a SAML authentication request or to parse or validate the SAML responses from the IdP. To the CAD/RMS server, the SAML messages themselves are opaque XML documents, and it simply passes them along. This integration requires configuring the state IdP with parameters for the CAD/RMS system as if it were an RP.

Further, we assume that the state IdP supports IdP-initiated SSO and has a URL configured to trigger an IdP-initiated login to the CAD/RMS thick client. Both the IdP and the CAD/RMS system must also support WS-Trust for this integration. This architecture is shown in Fig. 21.

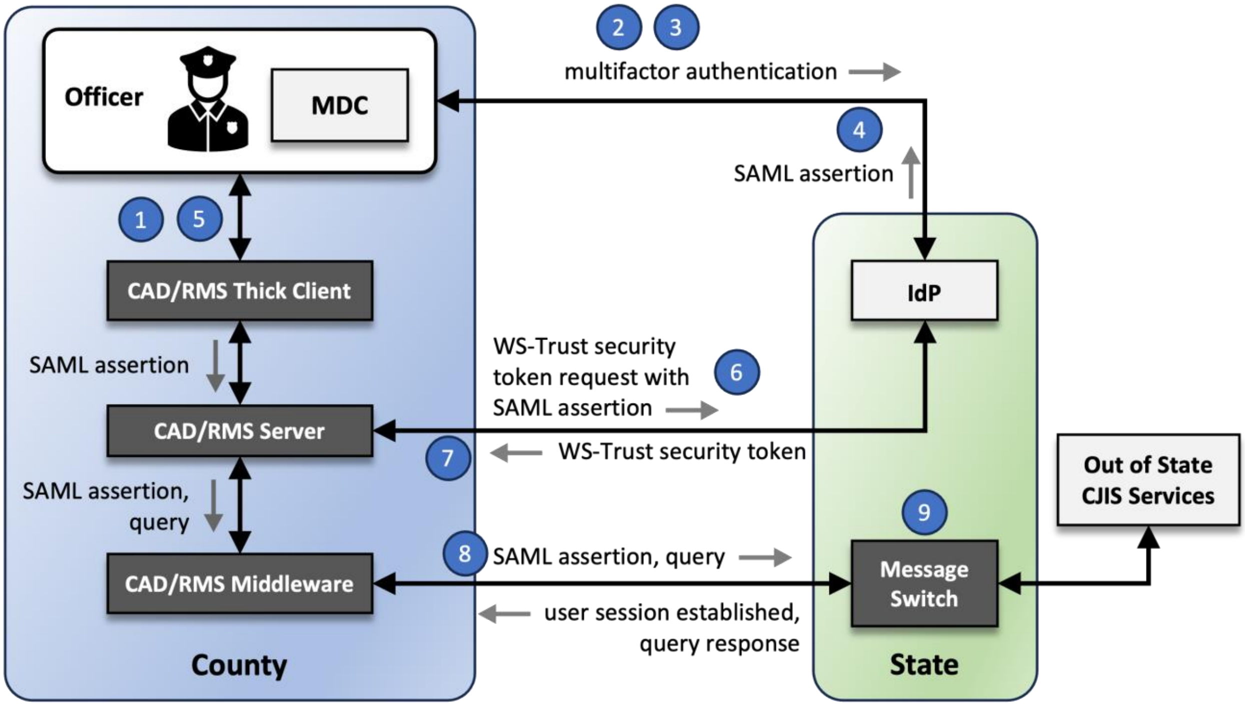


Fig. 21. Thick client CAD/RMS at county, state IdP (WS-Trust).

The sequence of interactions is as follows:

1. The officer opens the CAD/RMS thick client application, which connects to the CAD/RMS server. The officer authenticates using a non-SAML method, such as Kerberos. The details of this interaction are proprietary and depend on the CAD/RMS application's design.
2. The officer submits a query that must be submitted to the state message switch. To authenticate the officer, the CAD/RMS thick client opens the IdP-initiated SSO URL of the state IdP in the built-in browser on the officer's MDC.
3. The IdP prompts the officer to log in with a username/password and issues an MFA challenge to the officer after validating the officer's login credentials.
4. The IdP validates the MFA challenge-response and creates a new user session for the officer, generates a SAML assertion, signs it with its private signing key, encrypts it with a symmetric key shared with the CAD/RMS system, and returns it to the browser in a redirect to the CAD/RMS thick client.
5. The browser invokes the thick client and passes the SAML assertion to it. This is done by redirecting to a URL that is configured to be handled by the CAD/RMS thick client in the MDC's operating system (e.g., using an app URI handler). The thick client sends the SAML assertion to the CAD/RMS server.
6. The CAD/RMS server cannot decrypt or validate the assertion. It sends a WS-Trust Security Token Request to the IdP, including the SAML assertion it received earlier in the

onBehalfOf element to indicate that the request is for a token to present to the message switch on behalf of the previously authenticated user.

7. The IdP creates a new SAML assertion with the officer as the subject and with a suitable audience parameter for the message switch. The IdP returns this SAML assertion to the CAD/RMS server in a WS-Trust Request Security Token Response message.
8. The CAD/RMS server sends this new SAML assertion and the query to the message switch.
9. The message switch validates the assertion and extracts the user's identity and attributes. The message switch can use these attributes to authorize the query.

B.4.3. Both the CAD/RMS Web App and IdP at a County Agency

In this scenario, the CAD/RMS web app and IdP are both hosted by the county. For this implementation, shown in Fig. 22, the state message switch must have an RP trust with the county IdP.

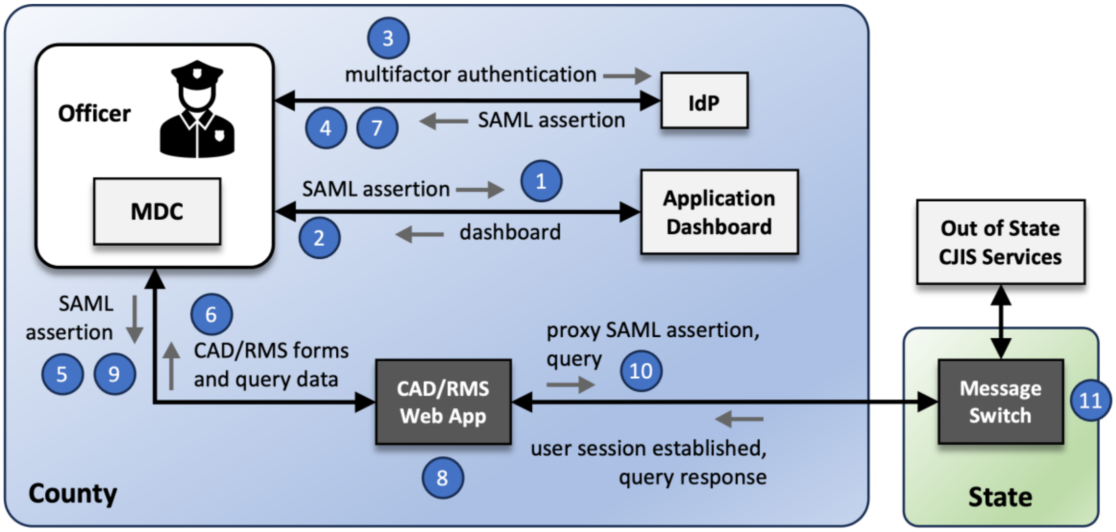

3
multifactor authentication
IdP
Officer
4
7
SAML assertion
MDC
SAML assertion
1
Application Dashboard
2
dashboard
Out of State CJIS Services
SAML assertion
5
9
6
CAD/RMS forms and query data
proxy SAML assertion, query
10
CAD/RMS Web App
Message Switch
11
user session established, query response
8
County
State

Fig. 22. CAD/RMS web app and IdP at county (SAML proxy).

The sequence of interactions is as follows:

1. The officer accesses the county application dashboard.
2. The application dashboard redirects the officer to the county IdP to authenticate.
3. The officer authenticates to the IdP with their credentials and MFA.
4. The IdP redirects the officer's browser to the application dashboard with a SAML assertion. The dashboard validates the SAML assertion, logs in the officer, and presents a set of application links based on their authorizations.
5. The officer clicks a link to the county CAD/RMS system.
6. The CAD/RMS system redirects the officer's browser to the IdP to authenticate.

7. Since the officer has an active session with the IdP, they do not need to authenticate. The IdP redirects the officer's browser to the CAD/RMS system with a SAML assertion.
8. The CAD/RMS system validates the assertion and logs in the officer.
9. The officer submits a query to the CAD/RMS system.
10. The CAD/RMS system creates a new SAML assertion including the user identifiers and attributes it received from the IdP. The CAD/RMS system sends this new SAML assertion and the query to the state message switch.
11. The message switch validates the assertion and extracts the user's identity and attributes. The message switch can use these attributes to authorize the query.

B.4.4. Integrations with OAuth 2.0 and OIDC

Though SAML is well-suited for integration with the XML-based web services that are prevalent in the CJIS environment, the commercial world has already adopted REST architectures and current-generation authentication and authorization protocols such as OIDC and OAuth 2.0. These protocols require new data formats such as JavaScript Object Notation (JSON) and the related JavaScript Object Signing and Encryption (JOSE) suite of standards in place of the XML signature and encryption specifications. Though OAuth and OIDC are commonly implemented in a REST environment, there is no technical obstacle to integrating them with XML-based web services.

OAuth 2.0 is designed for delegated authorization scenarios where a system accesses another system on behalf of a user. The scenario where a user is logged into a CAD/RMS system that must then access a message switch on the user's behalf is exactly the type of delegation scenario for which OAuth was designed. OAuth natively supports this delegation flow in a widely supported protocol without the need for the CAD/RMS system to act as a Proxy IdP or to support WS-Trust. The following subsection provides an example of how one of the use cases described previously could be implemented using OAuth and OIDC.

B.4.4.1. Both CAD/RMS Web App & IdP at the State Agency – OIDC and OAuth

This is the same scenario presented previously with SAML and WS-Trust in Appendix B 4.1.2. OIDC is used to authenticate the officer to the portal and CAD/RMS application, and OAuth 2.0 is used to authorize the officer's request to the state message switch, as shown in Fig. 23. This sequence can be implemented using the Authorization Code flow of OAuth and OIDC. It is assumed that the state IdP is also an OAuth Authorization Server (AS) that can issue tokens for the state message switch. The officer's identity and attributes can be passed to the message switch in the access token in JSON Web Token (JWT) format, or the message switch could retrieve them from the state IdP's token introspection endpoint.

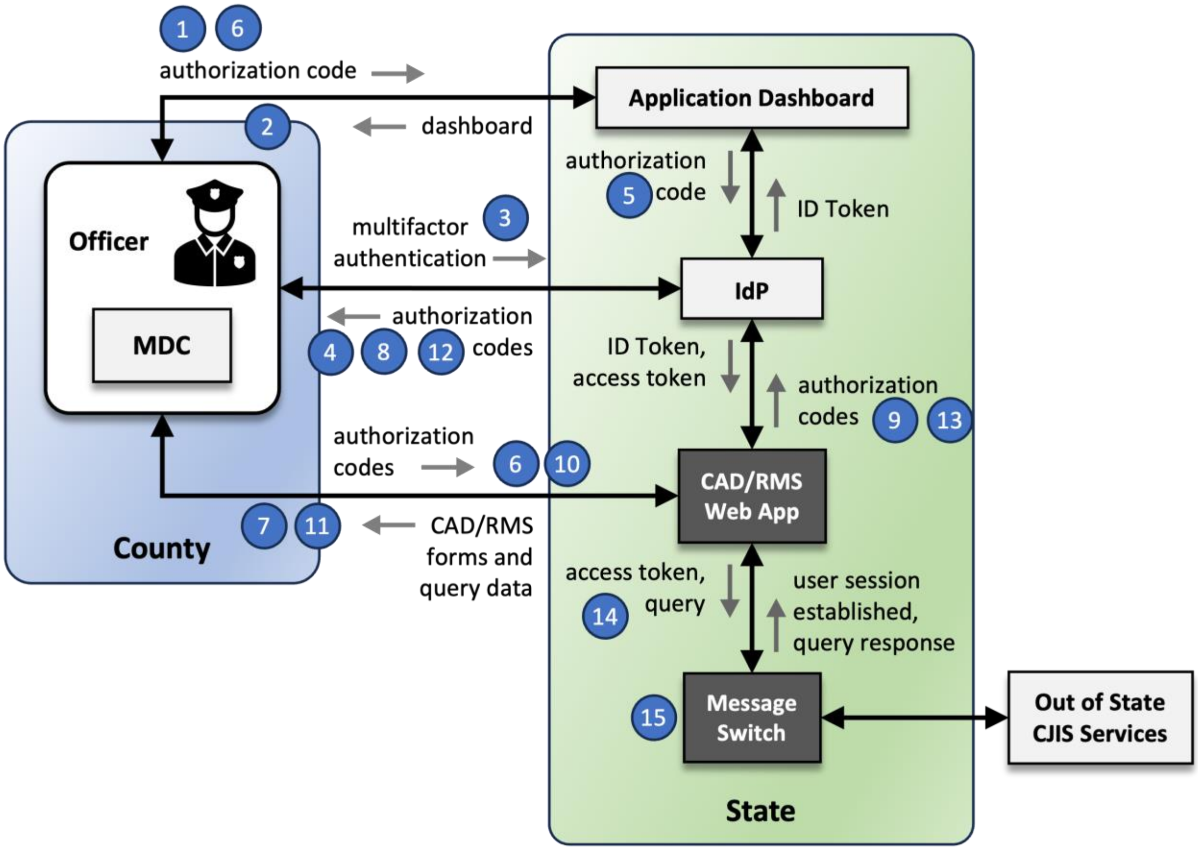


Fig. 23. CAD/RMS web app and IdP at state – OIDC and OAuth 2.0.

This sequence includes the following OIDC and OAuth interactions:

1. The officer accesses the application dashboard.
2. The application dashboard redirects the officer to the IdP to authenticate.
3. The officer authenticates to the IdP with their credentials and MFA.
4. The IdP redirects the officer’s browser to the application dashboard with an authorization code.
5. The application dashboard sends the authorization code to the IdP’s token endpoint, authenticating to the IdP with its own client secret or cryptographic credentials. The IdP returns an ID token to the dashboard. The dashboard validates the ID token, logs in the officer, and presents a set of application links based on their authorizations.
6. The officer clicks a link to the CAD/RMS system.
7. The CAD/RMS system redirects the officer’s browser to the IdP to authenticate.
8. Since the officer has an active session with the IdP, they do not need to authenticate. The IdP redirects the officer’s browser to the CAD/RMS system with an authorization code.

9. The CAD/RMS system sends the authorization code to the IdP’s token endpoint, authenticating to the IdP with its own client secret or cryptographic credentials. The IdP returns an ID token to the CAD/RMS system. The CAD/RMS system validates the ID token and logs in the officer.
10. The officer submits a query to the CAD/RMS system.
11. The CAD/RMS system redirects the officer’s browser to the IdP with an OAuth 2.0 authorization request.
12. Since the officer has an active session with the IdP, they do not need to authenticate. The IdP (acting as an OAuth 2.0 authorization server) redirects the officer’s browser to the CAD/RMS system with an authorization code.
13. The CAD/RMS system sends the authorization code to the IdP’s token endpoint, authenticating to the IdP with its own client secret or cryptographic credentials. The IdP returns an access token to the CAD/RMS system in the form of a JSON Web Token (JWT), cryptographically signed and encrypted using a key held by the message switch.
14. The CAD/RMS system sends the access token and the query to the message switch.
15. The message switch decrypts and validates the access token and extracts the user’s identity and attributes. The message switch can use these attributes to authorize the query.

B.5. VPN Integration

This section only applies to agencies that use VPNs in their architecture. If your agency requires users to authenticate to both the device (e.g., laptop or mobile device) and to a VPN server (or gateway) to obtain remote access to the agency's enterprise network, this section will be of interest.

Figure 24 shows an implementation where both the VPN service and the CAD/RMS web app use the same LDAP directory service, such as Microsoft Active Directory. The sequence of interactions commonly implemented is as follows (it is assumed that the officer has already logged into the laptop):

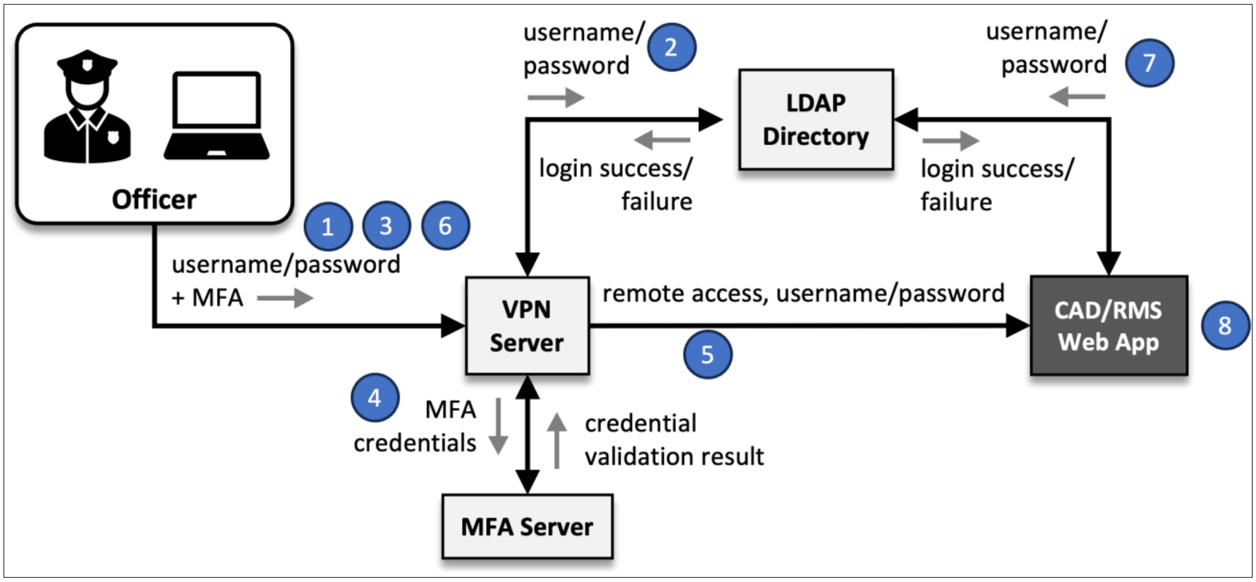


Fig. 24. VPN with an LDAP directory.

1. The officer activates a VPN client on the laptop and is prompted to log in with a username and password. The VPN client sends the username and password to the VPN server.
2. The VPN server sends the submitted username and password to the LDAP server to validate the credentials. The LDAP server returns a login success message.
3. The VPN client prompts the officer for MFA credentials (e.g., an OTP) and sends the credentials to the VPN server.
4. The VPN server sends the MFA credentials to the MFA server for validation. The MFA server returns an authentication success message.
5. Having authenticated the officer, the VPN server establishes a remote access session. The officer accesses an internal CAD/RMS web app.
6. The CAD/RMS app prompts the user for a username/password. The user enters the same username and password used earlier to authenticate to the VPN. These credentials are associated with the officer's user account in the enterprise LDAP directory.
7. The CAD/RMS app sends the submitted username and password to the LDAP server to validate the credentials. The LDAP server returns a login success message.
8. The user's session with the CAD/RMS server is established.

Although the officer only needs to use one username/password credential and one MFA credential, there is no SSO user experience since the user needs to enter the password twice. If MFA is not required at the CAD/RMS web app, the session is susceptible to phishing, as described in Sec. 2.5. If, on the other hand, the CAD/RMS web app enforced MFA a second time, the user would need to respond to the MFA prompt again. Repeated authentication and

MFA prompts pose a burden on the user and can take focus away from the critical work they need to do.

B.5.1. VPN Integration with Kerberos but without Federation

Figure 25 shows a single system acting as both a Kerberos Key Distribution Center and an LDAP Server, such as an Active Directory domain controller. The sequence in this scenario is as follows. (Again, it is assumed that the officer has already logged into the laptop with username and password.)

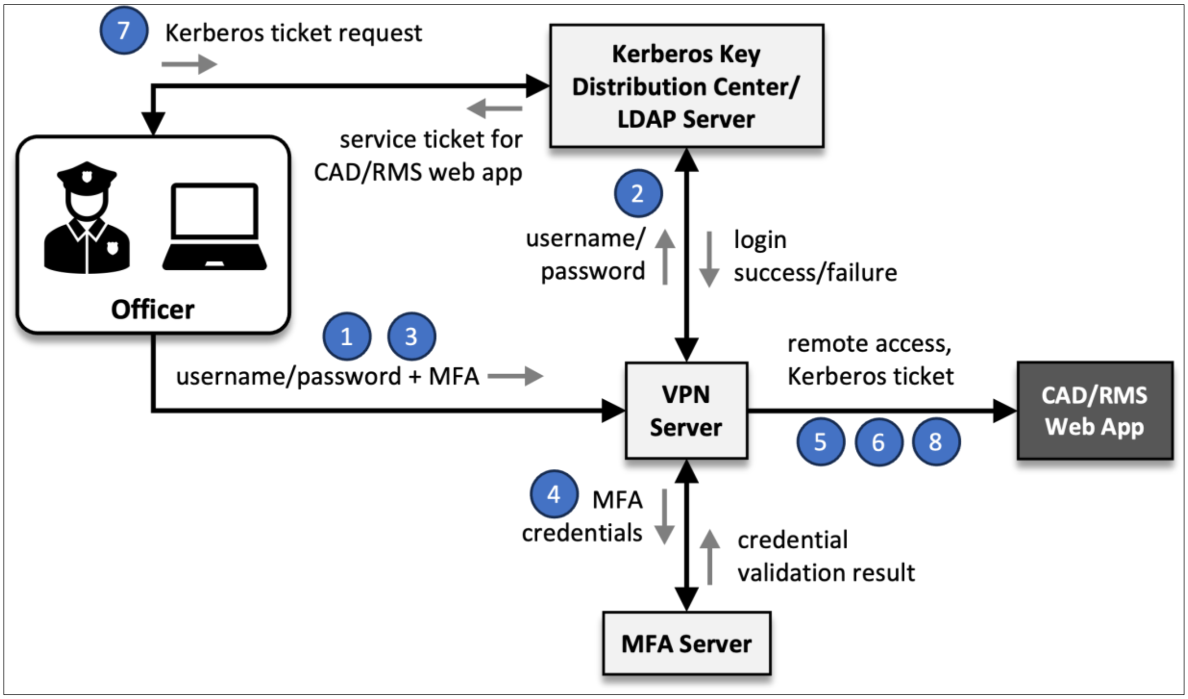


Fig. 25. VPN with Kerberos.

1. The officer activates a VPN client on the laptop and is prompted to log in with a username and password. The VPN client sends the username and password to the VPN server.
2. The VPN server sends the submitted username and password to the LDAP server to validate the credentials. The LDAP server returns a login success message.
3. The VPN client prompts the officer for MFA credentials (e.g., an OTP) and sends the credentials to the VPN server.
4. The VPN server sends the MFA credentials to the MFA server for validation. The MFA server returns an authentication success message.
5. Having authenticated the officer, the VPN server establishes a remote access session. The officer accesses an internal CAD/RMS web app.

6. The CAD/RMS app returns an "unauthorized" error code to the browser with headers indicating that Kerberos authentication can be used.
7. Since the laptop is connected to the VPN, the Kerberos client component of the OS can connect to the Kerberos Key Distribution Center and obtain a Kerberos ticket for the CAD/RMS system.
8. The browser sends the Kerberos ticket to the CAD/RMS system, which validates the ticket and establishes the user's session.

This integration provides an SSO experience that requires the user to only provide the username/password and MFA credentials once (apart from the initial login to the laptop).

Though the Kerberos approach reduces the number of authentication challenges, the user's credentials are only accepted within the organization (e.g., the local or county agency). If the users need to access additional applications at the state level, they would need different state credentials unless federation technologies are used to provide authentication across security domains. Integrating the VPN with an IdP, as described in the next section, makes this possible.

B.5.2. VPN Integration with an Identity Provider

Another approach to reducing this additional authentication burden is to integrate the VPN gateway with the IdP. In this scenario, the VPN gateway redirects the user to authenticate with the IdP using MFA. This also creates a session with the IdP that the user can then leverage to authenticate to other applications without additional MFA prompts. This approach requires the IdP to be accessible from the public internet since the user must access it prior to authenticating to the VPN. This is a common configuration for identity-as-a-service platforms but less common for internally hosted SSO systems. Figure 26 illustrates this approach with a VPN gateway integrated with an enterprise IdP.

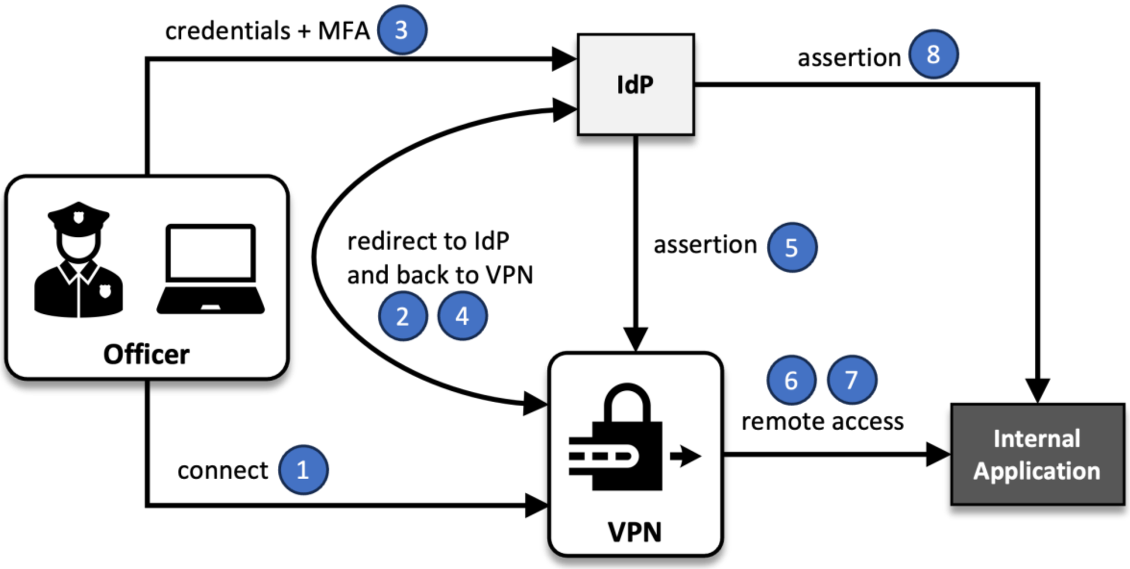


Fig. 26. VPN gateway integration with enterprise SSO.

The sequence of events in this scenario is as follows:

1. The user connects to the VPN gateway.
2. The VPN gateway redirects the user to the IdP for authentication.
3. The user authenticates to the IdP with their credentials and MFA.
4. The IdP redirects the user back to the VPN gateway.
5. The VPN gateway receives the assertion from the IdP (either from the user’s browser or directly from the IdP, depending on the protocol) and establishes the user’s remote access session.
6. The user accesses an internal application through the VPN. The application redirects the user to the same IdP used in step 2 for authentication.
7. Because the user already has a session at the IdP, they are not required to authenticate again and are redirected back to the application.
8. The application receives the assertion from the IdP and establishes the user’s application session.

The impact of multiple MFA prompts can also be mitigated by choosing MFA credentials that require less user interaction. Using a smart card, for example, to authenticate to the client laptop, the VPN gateway, and an SSO system provides phishing-resistant MFA and a relatively seamless user experience. The user is required to enter a short numeric PIN to unlock the smart card. In many cases, the workstation can cache the PIN to avoid further PIN prompts as the user authenticates to additional systems. Hardware authenticators can offer similar convenience.

Appendix C. Questions to Ask Your Technology Vendors

This appendix provides lists of questions that agencies can ask vendors to evaluate the efficacy of their MFA implementation in meeting CJIS Security Policy requirements and the principles of MFA design as outlined in this document. Each questionnaire is specific to one of the following vendor categories:

- CAD/RMS vendors (Appendix C.1)
- Identity services vendors (Appendix C.2)
- Message switch vendors (Appendix C.3)
- VPN vendors (Appendix C.4)

If you import these questions into your own custom document that you transmit to your vendor, please include a link to this document (NIST IR 8523) so that the vendors have context for the terms introduced in this document.

C.1. Questionnaire for CAD/RMS Vendors

1. Please identify your CAD/RMS application as:
    a. Thick client
    b. Web application
    c. Other (Please describe in detail)
2. How does your CAD/RMS application meet the AAL2 MFA requirements in the CJIS Security Policy? Please provide a detailed list of how you meet each requirement.
3. As part of your service, do you offer an MFA solution that comes directly integrated with your CAD/RMS application, or do you anticipate agencies having or procuring their own MFA implementation with which your CAD/RMS solution will be integrated?
4. If you offer MFA as part of your service, please specify which types of multi-factor authenticators your solution offers. For each type, list what the two factors are for the MFA system. Please include a detailed sequence diagram showing the authentication flow for the authenticator. Please identify the specific authenticator vendor and brand, and provide a list of agencies with reference points of contact (POCs) where your implementation has been deployed for each use case.
5. Authenticator optionality is defined in IR 8523. Can the authenticators listed under question 3 be deployed alongside each other to allow agencies to offer different authenticators to different user groups (prisons, sworn law enforcement officers, detectives, dispatch centers, etc.) who may have different MFA needs and use cases? Please provide a list of agencies with reference POCs where your implementation has been deployed for each use case.
6. How do you support phishing resistance with your MFA solution?

7. Do you support identity federation protocols and architectures such as SAML 2.0, Open ID Connect 1.0, OAuth 2.0, and IdP proxies? If yes, can you please provide examples of how you have deployed these technologies for other agencies? Where possible, please provide a detailed sequence diagram of the authentication flow and highlight which protocols were used and between which components. Please also include the make and model of the technologies used.

8. Describe your integration approach with VPN solutions. Please provide a detailed sequence diagram showing the authentication flow for each use case, as well as a list of agencies with reference POCs where your implementation has been deployed for each use case below. Please include the names of specific LDAP, VPN, or other applicable vendors in each case:

    a. Integration using LDAP

    b. Integration using Kerberos

    c. Integration using federated identity services (refer to IR 8523 for examples)

9. Refer to IR 8523, which defines the principles of MFA design. Please include a description of how your product demonstrates the principles of MFA design as outlined in IR 8523 regarding:

    a. Authenticator Reusability – Minimize the number of separate MFA credentials that users must use and manage.

    b. Authenticator Optionality – Support a diversity of use case environments such as department of corrections, law enforcement officers, dispatch centers, etc.

    c. Minimize the Passing of Shared Memorized Secrets – Avoid forwarding memorized secrets such as passwords to entities such as message switches to enable authentication.

    d. Ensure MFA Is Integrated to Protect CJI – Tie into SSO services and avoid multiple challenges for MFA.

C.2. Questionnaire for Identity Services Vendors

1. How does your product support the AAL2 MFA requirements in the CJIS Security Policy? Please provide a detailed list of how you meet each requirement.
2. Please specify which types of multi-factor authenticators your solution offers. For each type, list what the two factors are for the MFA system and if it supports phishing resistance.
    a. Please include a detailed sequence diagram showing the authentication flow for the authenticator. Please identify the specific authenticator vendor and brand, and provide a list of agencies with reference points of contact (POCs) where your implementation has been deployed.
    b. If phishing resistance is supported, list which phishing-resistant authentication protocols are used (e.g., FIDO2/WebAuthn/PIV Smart Card).
3. Authenticator optionality is defined in IR 8523. Can the authenticators listed under question 2 be deployed alongside each other to allow agencies to offer different authenticators to different user groups (prisons, sworn law enforcement officers, detectives, dispatch centers, etc.) who may have different MFA needs and use cases? Please provide a list of agencies with reference POCs where your implementation has been deployed for each use case.
4. How do you support phishing resistance with your MFA solution?
5. Do you support identity federation protocols and architectures such as SAML 2.0, Open ID Connect 1.0, OAuth 2.0, and IdP proxies? If yes, can you please provide examples of how you have deployed these technologies for other agencies? Where possible, please provide a detailed sequence diagram of the authentication flow and highlight which protocols were used and between which components. Please also include the make and model of the technologies used.
6. Describe your integration approach with CAD/RMS applications. Please provide a detailed sequence diagram showing the authentication flow for each use case, as well as a list of agencies with reference POCs where your implementation has been deployed for each use case below. Please include the names of the specific VPN vendors in each case.
7. Describe your integration approach with message switch applications. Please provide a detailed sequence diagram showing the authentication flow for each use case, as well as a list of agencies with reference POCs where your implementation has been deployed for each use case below. Please include the names of the specific VPN vendors in each case.
8. Describe your integration approach with VPN solutions. Please provide a detailed sequence diagram showing the authentication flow for each use case, as well as a list of agencies with reference POCs where your implementation has been deployed for each use case below. Please include the names of the specific VPN vendors in each case.

9. Refer to IR 8523, which defines the principles of MFA design. Please include a description of how your solution demonstrates the principles of MFA design as outlined in IR 8523 regarding:

    a. Authenticator Reusability – Minimize the number of separate MFA credentials that users must use and manage.

    b. Authenticator Optionality – Support a diversity of use case environments such as department of corrections, law enforcement officers, dispatch centers, etc.

    c. Minimize the Passing of Shared Memorized Secrets – Avoid forwarding memorized secrets such as passwords to entities such as message switches to enable authentication.

    d. Ensure MFA Is Integrated to Protect CJI – Tie into SSO services and avoid multiple challenges for MFA.

C.3. Questionnaire for Message Switch Vendors

1. How does your message switch application meet the AAL2 MFA requirements in the CJIS Security Policy? Please provide a detailed list of how you meet each requirement.
2. As part of your service, do you offer an MFA solution that comes directly integrated with your message switch? For agencies that have or will soon be deploying MFA at third-party applications such as CAD/RMS or identity service providers, how does your message switch integrate with these solutions?
3. If you offer MFA as part of your service, please specify which types of multi-factor authenticators your solution offers. For each type, list what the two factors are for the MFA system and if it supports phishing resistance.
    a. Please include a detailed sequence diagram showing the authentication flow for the authenticator. Please identify the specific authenticator vendor and brand, and provide a list of agencies with reference points of contact (POCs) where your implementation has been deployed.
    b. If phishing resistance is supported, list which phishing-resistant authentication protocols are used (e.g., FIDO2/WebAuthn/PIV Smart Card).
4. Authenticator optionality is defined in IR 8523. Can the authenticators listed under question 3 be deployed alongside each other to allow agencies to offer different authenticators to different user groups (prisons, sworn law enforcement officers, detectives, dispatch centers, etc.) who may have different MFA needs and use cases? Please provide a list of agencies with reference POCs where your implementation has been deployed for each use case.
5. How do you support phishing resistance with your MFA solution?
6. Do you support identity federation protocols and architectures such as SAML 2.0, Open ID Connect 1.0, OAuth 2.0, and IdP proxies? If yes, can you please provide examples of how you have deployed these technologies for other agencies? Where possible, please provide a detailed sequence diagram of the authentication flow and highlight which protocols were used and between which components. Please also include the make and model of the technologies used.
7. Refer to IR 8523, which defines the principles of MFA design. Please include a description of how your solution demonstrates the principles of MFA design as outlined in IR 8523 regarding:
    a. Authenticator Reusability – Minimize the number of separate MFA credentials that users must use and manage.
    b. Authenticator Optionality – Support a diversity of use case environments such as department of corrections, law enforcement officers, dispatch centers, etc.
    c. Minimize the Passing of Shared Memorized Secrets – Avoid forwarding memorized secrets such as passwords to entities such as message switches to enable authentication.

d. Ensure MFA Is Integrated to Protect CJI – Tie into SSO services and avoid multiple challenges for MFA.

C.4. Questionnaire for VPN Vendors

1. How does your VPN solution meet the AAL2 MFA requirements in the CJIS Security Policy? Please provide a detailed list of how you meet each requirement.
2. As part of your service, do you offer an MFA solution that comes directly integrated with your VPN application, or do you anticipate agencies having or procuring their own MFA implementation with which your VPN solution will be integrated?
3. If you offer MFA as part of your service, please specify which types of multi-factor authenticators your solution offers. For each type, list what the two factors are for the MFA system, and if it supports phishing resistance.
    a. Please include a detailed sequence diagram showing the authentication flow for the authenticator. Please identify the specific authenticator vendor and brand, and provide a list of agencies with reference points of contact (POCs) where your implementation has been deployed.
    b. If phishing resistance is supported, list which phishing-resistant authentication protocols are used (e.g., FIDO2/WebAuthn/PIV Smart Card).
4. Authenticator optionality is defined in IR 8523. Can the authenticators listed under question 3 be deployed alongside each other to allow agencies to offer different authenticators to different user groups (prisons, sworn law enforcement officers, detectives, dispatch centers, etc.) who may have different MFA needs and use cases? Please provide a list of agencies with reference POCs where your implementation has been deployed for each use case.
5. How do you support phishing resistance with your MFA solution?
6. Describe your integration approach with CAD/RMS vendors. Please provide a detailed sequence diagram showing the authentication flow for each use case, and a list of agencies with reference POCs where your implementation has been deployed for each use case below. Please include the names of specific LDAP or other applicable vendors in each case:
    a. Integration using LDAP
    b. Integration using Kerberos
    c. Integration using federated identity services (refer to IR 8523 for examples)
7. Do you support identity federation protocols and architectures such as SAML 2.0, Open ID Connect 1.0, OAuth 2.0, and IdP proxies? If yes, can you please provide examples of how you have deployed these technologies for other agencies? Where possible, please provide a detailed sequence diagram of the authentication flow and highlight which protocols were used and between which components. Please also include the make and model of the technologies used.

8. Refer to IR 8523, which defines the principles of MFA design. Please include a description of how your solution demonstrates the principles of MFA design as outlined in IR 8523 regarding:

    a. Authenticator Reusability – Minimize the number of separate MFA credentials that users must use and manage.

    b. Authenticator Optionality – Support a diversity of use case environments such as department of corrections, law enforcement officers, dispatch centers, etc.

    c. Minimize the Passing of Shared Memorized Secrets – Avoid forwarding memorized secrets, such as passwords, to other entities to enable authentication.

    d. Ensure MFA Is Integrated to Protect CJI – Tie into SSO services and avoid multiple challenges for MFA.

Appendix D. List of Symbols, Abbreviations, and Acronyms

AAL
Authentication Assurance Level

AS
Authorization Server (OAuth)

BYOD
Bring Your Own Device

CAD
Computer-Aided Dispatch

CIO
Chief Information Officer

CISO
Chief Information Security Officer

CJI
Criminal Justice Information

CJIS
Criminal Justice Information Services

COPE
Corporately Owned Personally Enabled

CSO
CJIS Systems Officer

DHS
Department of Homeland Security

DOJ
Department of Justice

FAL
Federation Assurance Level

FIDO

Fast Identity Online

HTTPS
Hypertext Transfer Protocol Secure

IdP
Identity Provider

IR
Interagency Report or Internal Report

ISO
Information Security Officer

JOSE
JavaScript Object Signing and Encryption

JSON
JavaScript Object Notation

JWT
JSON Web Token

LDAP
Lightweight Directory Access Protocol

MDC
Mobile Digital Computer

MFA
Multi-Factor Authentication

OIDC
OpenID Connect

OS
Operating System

OTP
One-Time Passcode

PD
Police Department

PIN
Personal Identification Number

POC
Point of Contact

REST
Representational State Transfer

RMS
Record Management System

RP
Relying Party

SAML
Security Assertion Markup Language

SLTT
State, Local, Tribal, and Territorial

SP
Special Publication

SSO
Single Sign-On

TLS
Transport Layer Security

URI
Uniform Resource Identifier

VPN
Virtual Private Network

W3C

World Wide Web Consortium

XML
Extensible Markup Language