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

Considerations for Implementing MFA to Protect Criminal Justice Information

NIST Information Technology Lab

Applied Cybersecurity Division

National Cybersecurity Center of Excellence

This webinar is being recorded

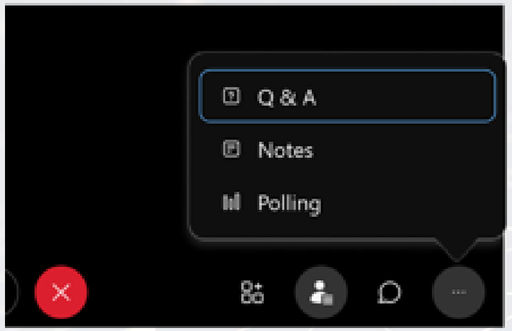
May 16th, 2024

Agenda

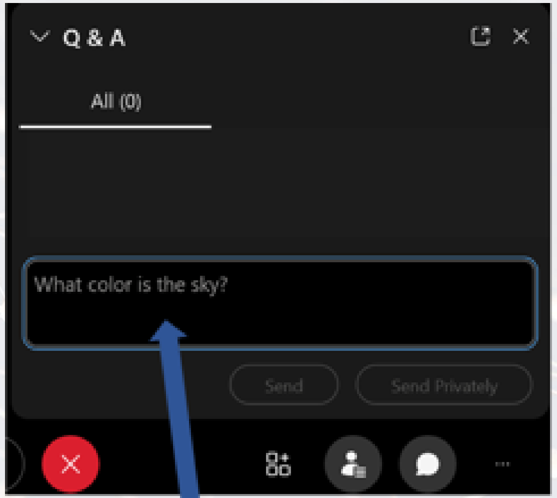
- Opening Remarks
- Introductions
- Project Overview
- MFA deployment Considerations
- MFA Use Cases
- Discussion & Questions

Submitting Questions

During the presentation please use the Q&A window to enter your questions.



1. To open the Q&A panel, click on the ellipses at the bottom of the screen for 'More Panels' and click on Q&A.



What color is the sky?

2. Type your question in the text box and click Send

We'll have time for open mic questions and discussion after the presentation.

If we are unable to answer your question please e-mail us: ps-mfa@list.nist.gov

Opening Remarks

Team Introduction

Bill Fisher
Security Engineer, NCCoE

Sudhi Umarji
ICAM Engineer, MITRE Coporation

DISCLAIMER

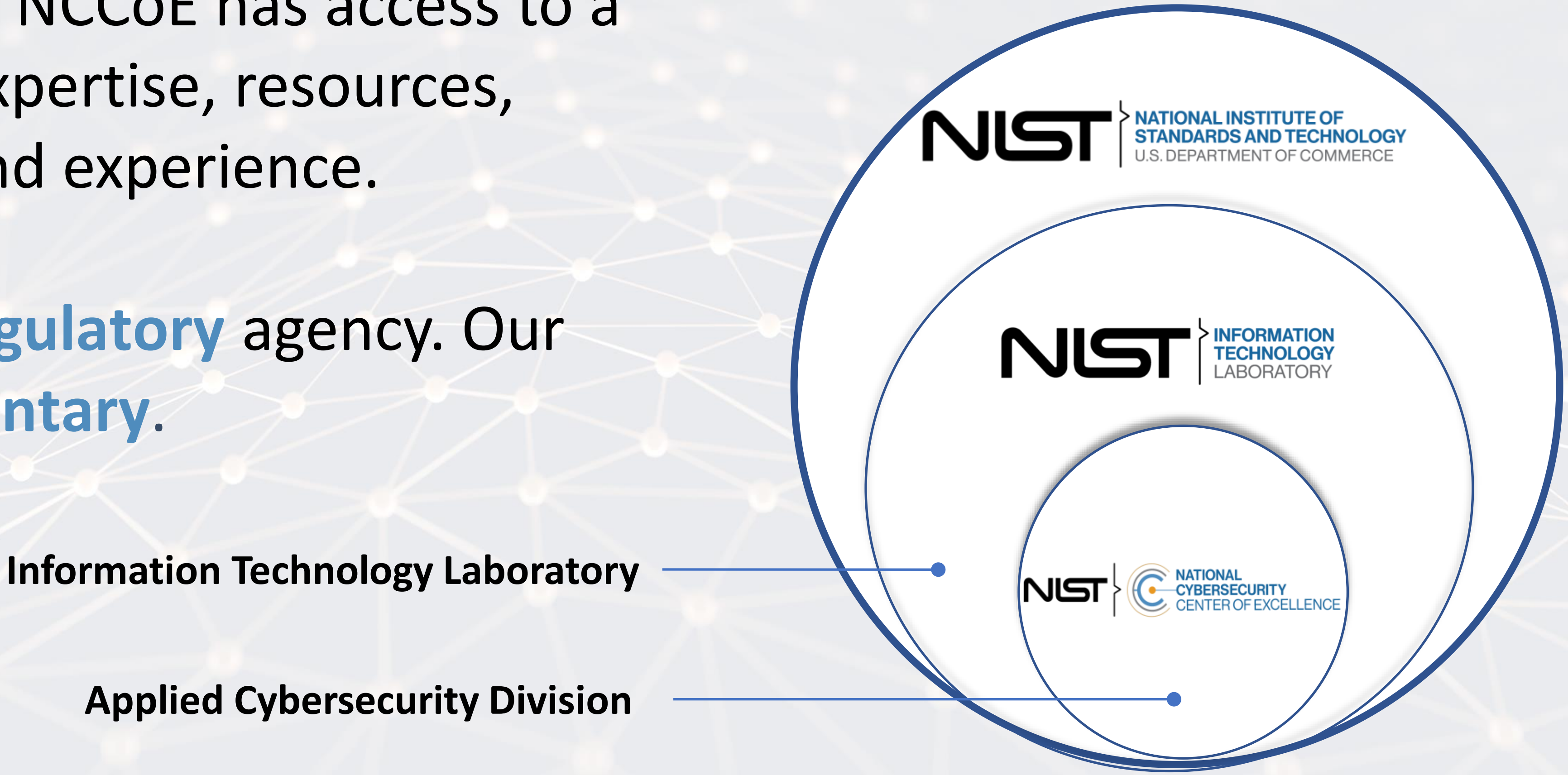
The information in this presentation is intended to aid agencies in their MFA implementations but in no way guarantees that their implementation will meet CJIS Security Policy requirements or will pass a CJIS audit.

All questions for how a specific MFA implementation can meet the CJIS Security Policy should be directed to the CJIS ISO team at iso@fbi.gov.

Who is the NCCoE

Part of NIST, the NCCoE has access to a foundation of expertise, resources, relationships, and experience.

NIST is a **non-regulatory** agency. Our guidance is **voluntary**.


NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE
NIST INFORMATION TECHNOLOGY LABORATORY
NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
Information Technology Laboratory
Applied Cybersecurity Division

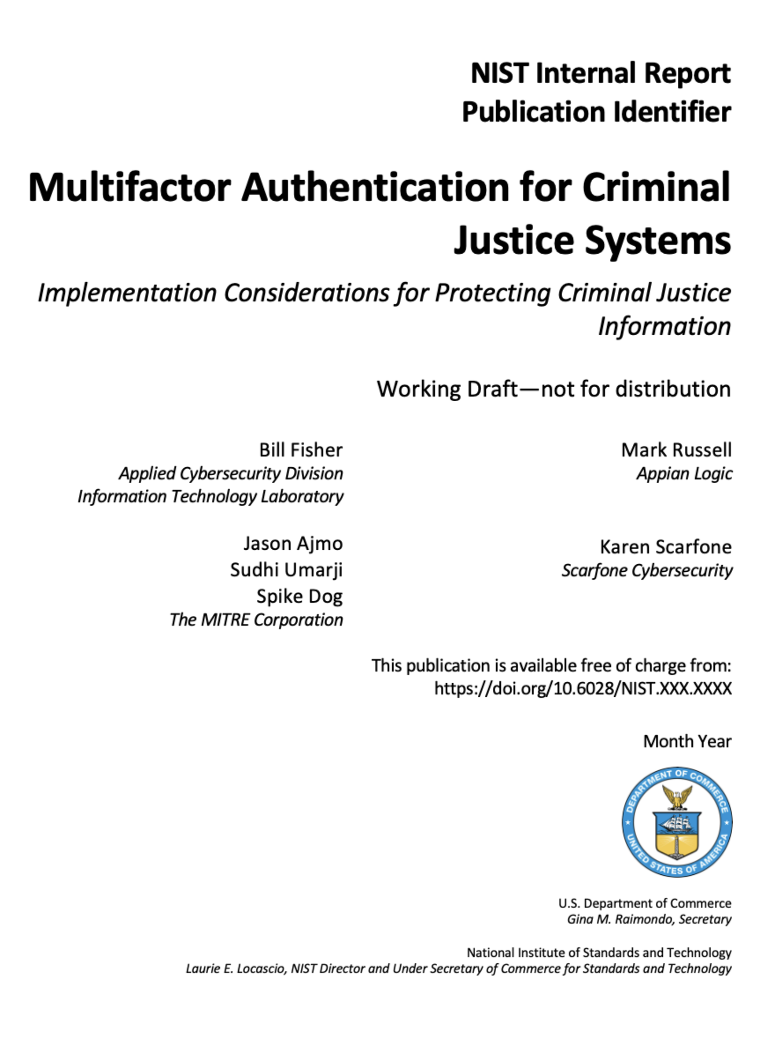
NCCoE MFA Project Overview

Background: 8+ years of working with Public Safety communities and their cybersecurity challenges.

Project Goal: Assist agencies nationwide who need access to CJI with their MFA implementations.

Methodology: We’ve spent the last 6 months chatting with agencies around the county about MFA use cases, technologies and pain points.

Output: A NISTIR detailing what we learned and considerations for implementing MFA in the context of criminal justice systems.



NIST Internal Report
Publication Identifier

Multifactor Authentication for Criminal Justice Systems

Implementation Considerations for Protecting Criminal Justice Information

Working Draft—not for distribution

Bill Fisher
Applied Cybersecurity Division
Information Technology Laboratory

Mark Russell
Appian Logic

Jason Ajmo
Sudhi Umarji
Spike Dog
The MITRE Corporation

Karen Scarfone
Scarfone Cybersecurity

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

Month Year

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

During this workshop…

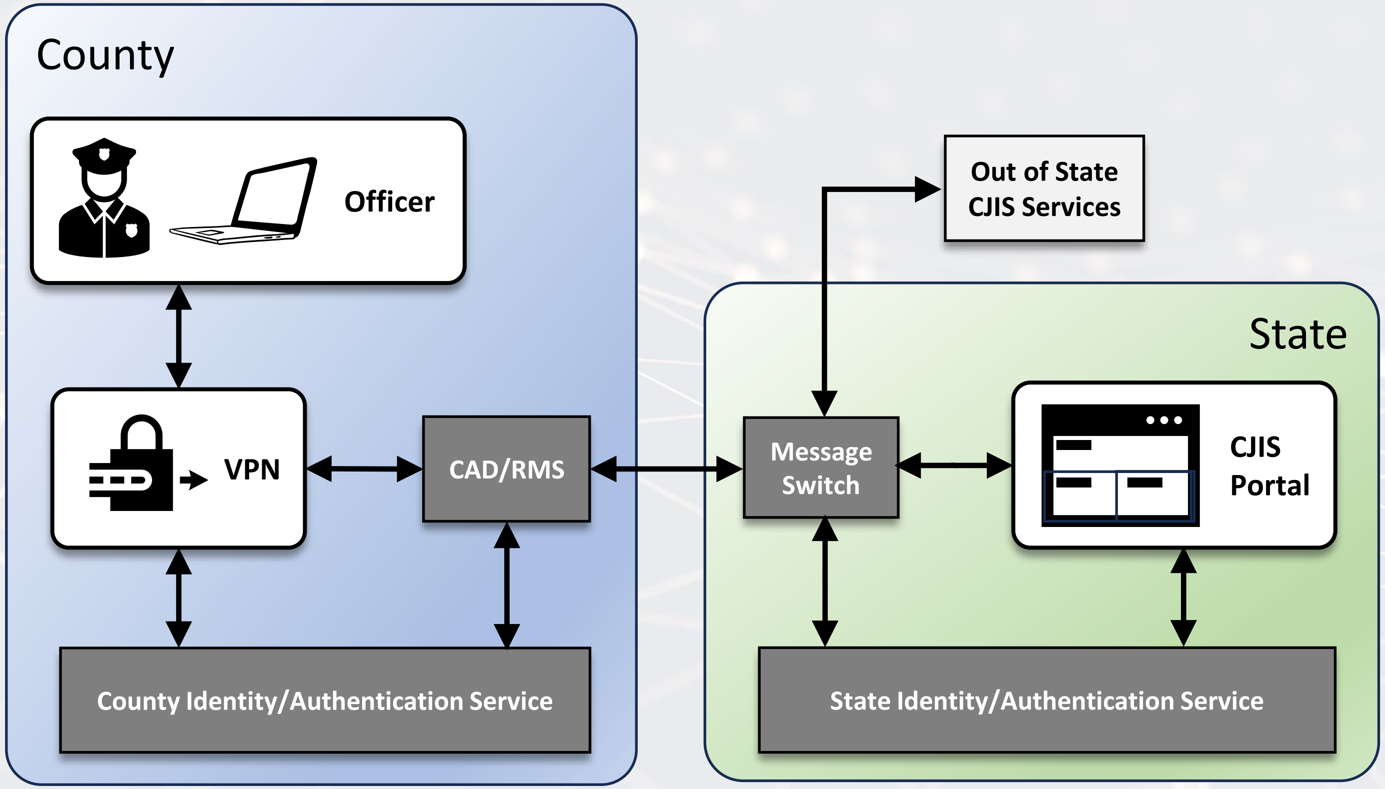
We hope to foster a greater understanding of the technology, architectures, challenges and potential MFA options for protecting CJI. Two common themes:

"It Depends" – there are many ways to implement MFA. What works for one organization or user base may not be best for another. This webinar seeks to explore many different architectures and to provide some key MFA implementation principles should be consider across all implementations.

"It Takes a Village" – CJI systems are used across state, local, tribal and territorial governments with both criminal and non-criminal justice agencies. Accessing CJI often requires the cross-jurisdictional connection of information technology systems and collaboration between multiple agencies. Everyone on this call has a role to play in helping agencies implement MFA.

What we have heard

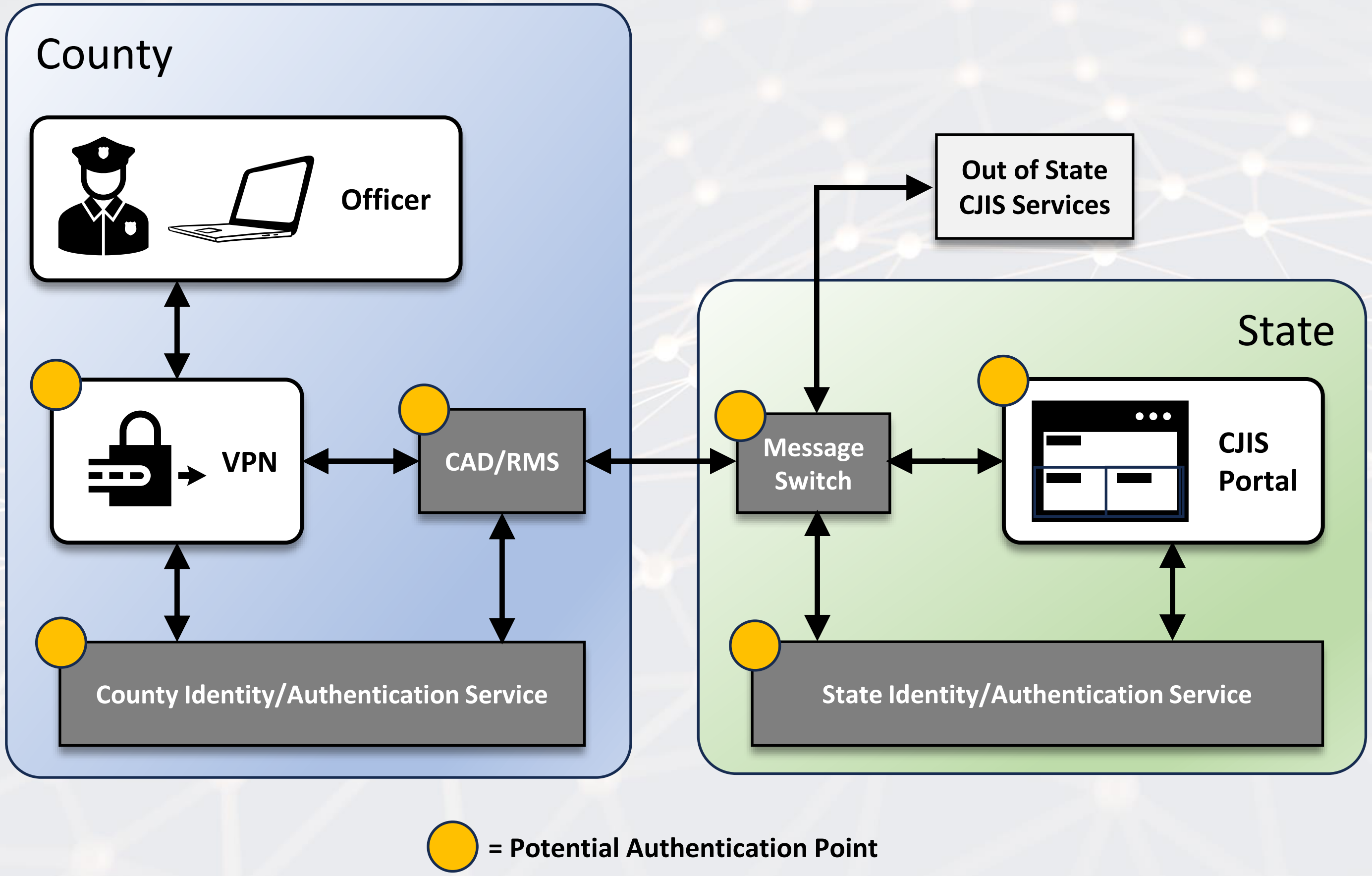
- Common architectural components
- Common ways of accessing CJI
  - State portal
  - CAD/RMS
- Interconnectivity between state and local systems
- MFA likely at state portal
- Local agencies required to have MFA before accessing CAD/RMS


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

MFA Design Principles

Design Principles Overview

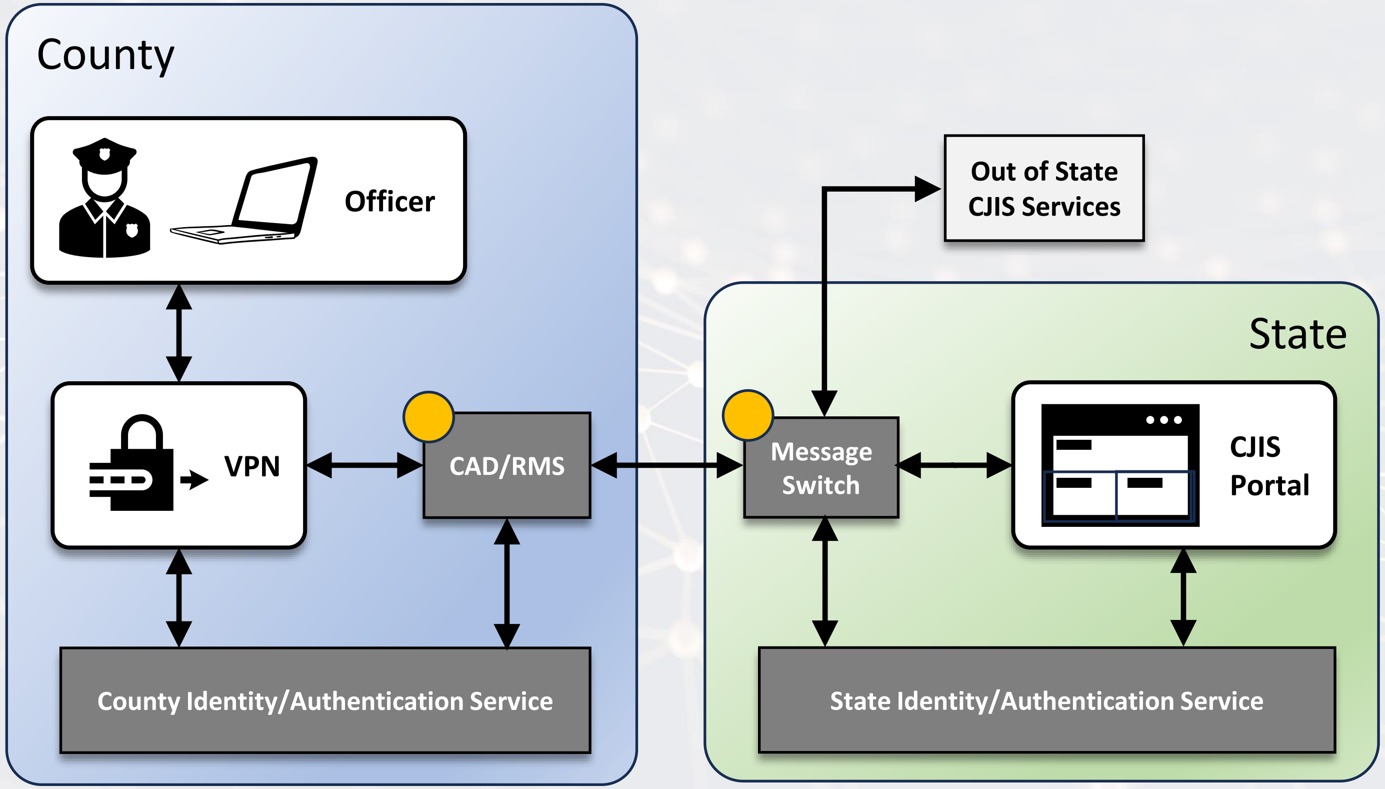
Agencies should consider a few key principles when implementing MFA:


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

1. **Authenticator re-usability**
2. **Authenticator optionality**
3. **Avoid passing memorized shared secrets**
4. **Ensure MFA is protecting your CJI**

Principle #1: Authenticator Re-Usability

- Minimize the number of credentials users have to manage
- Save money by leveraging pre-existing MFA or identity services which may exist at the state, county or local level, inside or outside of public safety departments
- Challenge: User is required to maintain 2 sets of MFA credentials, one locally for CAD/RMS and another when accessing the state CJIS portal

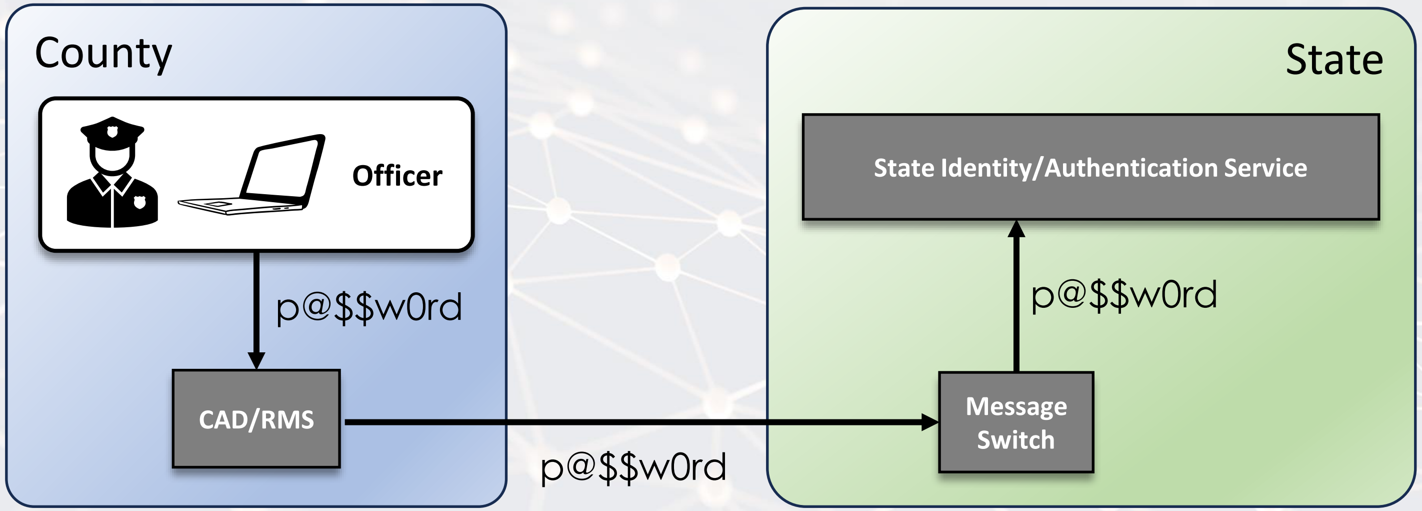

County
Officer
VPN
CAD/RMS
County Identity/Authentication Service
Out of State CJIS Services
State
Message Switch
CJIS Portal
State Identity/Authentication Service

Principle #2: Authenticator Optionality

- Agencies have a diverse set of user authentication requirements.
- Giving agencies authenticator optionality allows them to meet the user needs and use cases.
- Challenge - Department of corrections:
  - Phone not allowed in facility
  - No biometrics available
  - Tokens too costly
  - Users are not assigned to specific devices

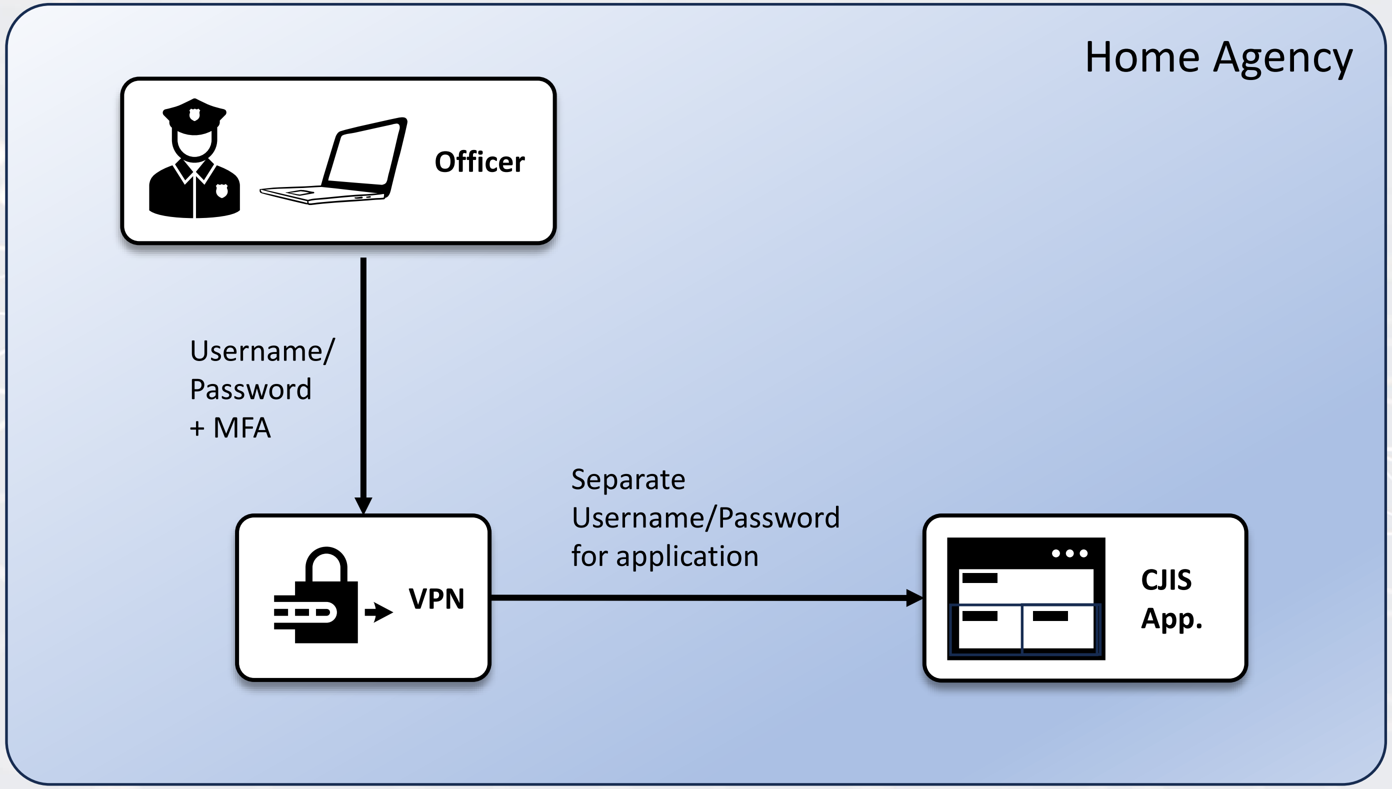
Principle #3: Avoid Passing Memorized Shared Secrets

- The passing of shared memorized secrets, such as passwords, between public safety 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.
- Security concerns exist with this model. Passing of memorized shared secrets should be avoided to the greatest extend possible.



Principle #4: Ensuring MFA protects CJI

- Just because MFA is “in front” of a CJIS application does not mean it’s providing the intended level of security.
- MFA does not need to be at the application, but it should be integrated with the application.
- Challenge: User authenticates with MFA at a VPN service, but when accessing a CJI application needs a separate username and password.



Because most states have multiple ways to access CJI and access to CJI often requires cross-jurisdictional (across state, local, tribal and territorial) connection between IT systems, implementing these MFA principles can be a challenge.

Supporting Technology

Standards & Best Practices that support MFA

"It Depends" still applies, but in general there are some standards and best practices that if supported by vendors could help agencies implement MFA. Specifically:

1. Identity Federation & other token-based protocols
2. Integration with Identity Services
3. Single Sign-On

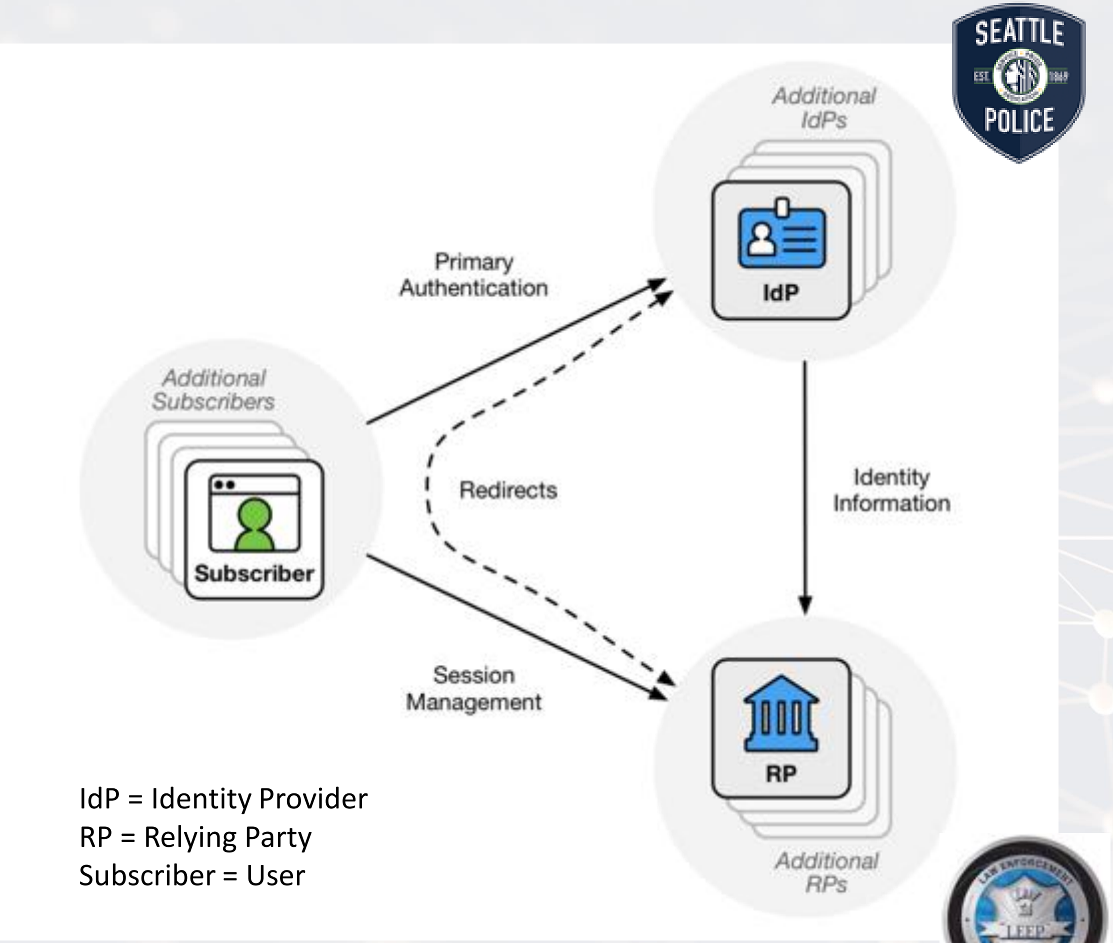
OpenID Connect

SAML v2.0
Security Assertion Markup Language

Identity Federation

- Identity Federation allows for the conveyance of identity and authentication information across a set of networked systems.
- Designed to alleviate the need to pass memorized shared secrets across networks.
- Supports integration between Identity services and applications that need to consume identity information such as authentication success/failure and attributes about the user.
- Two common protocols: OpenID Connect 1.0 and SAML 2.0

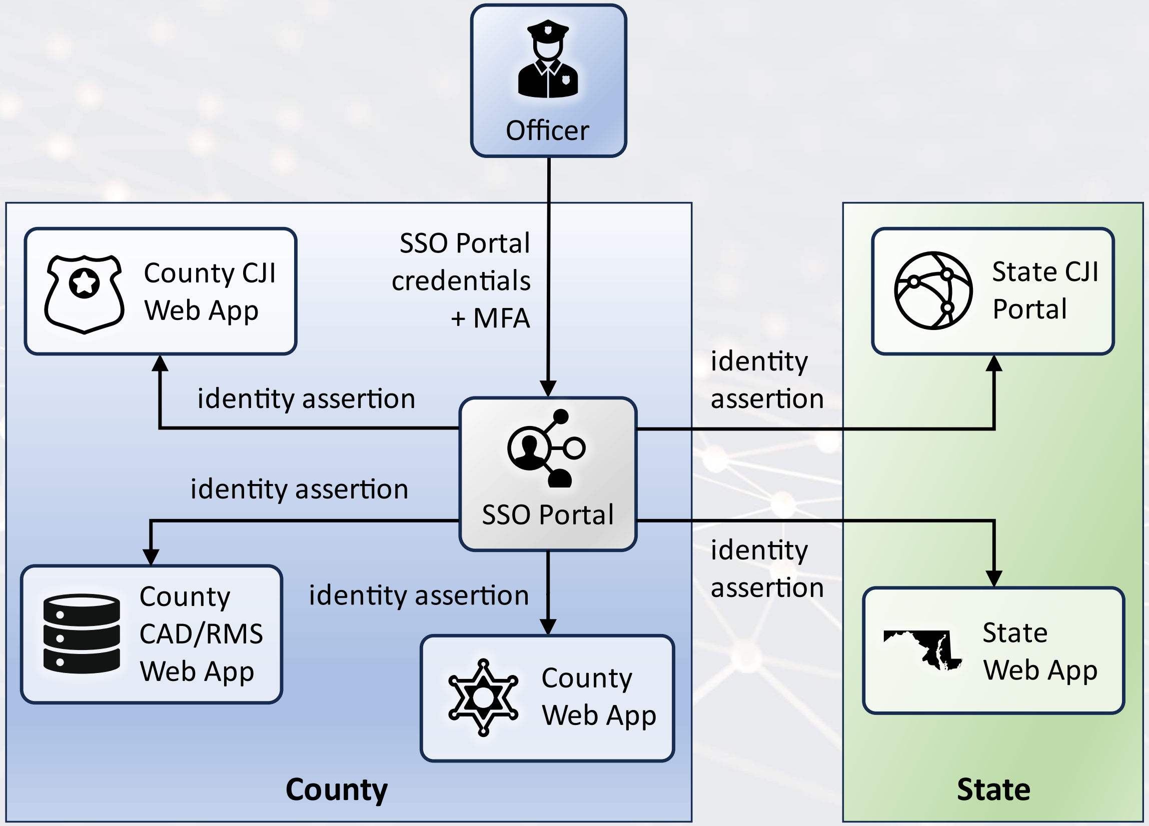
NOTE: Identity Federation is the primary way to support the passing of attributes under the AC-2 control.



IdP = Identity Provider
RP = Relying Party
Subscriber = User

Integration with Identity Services

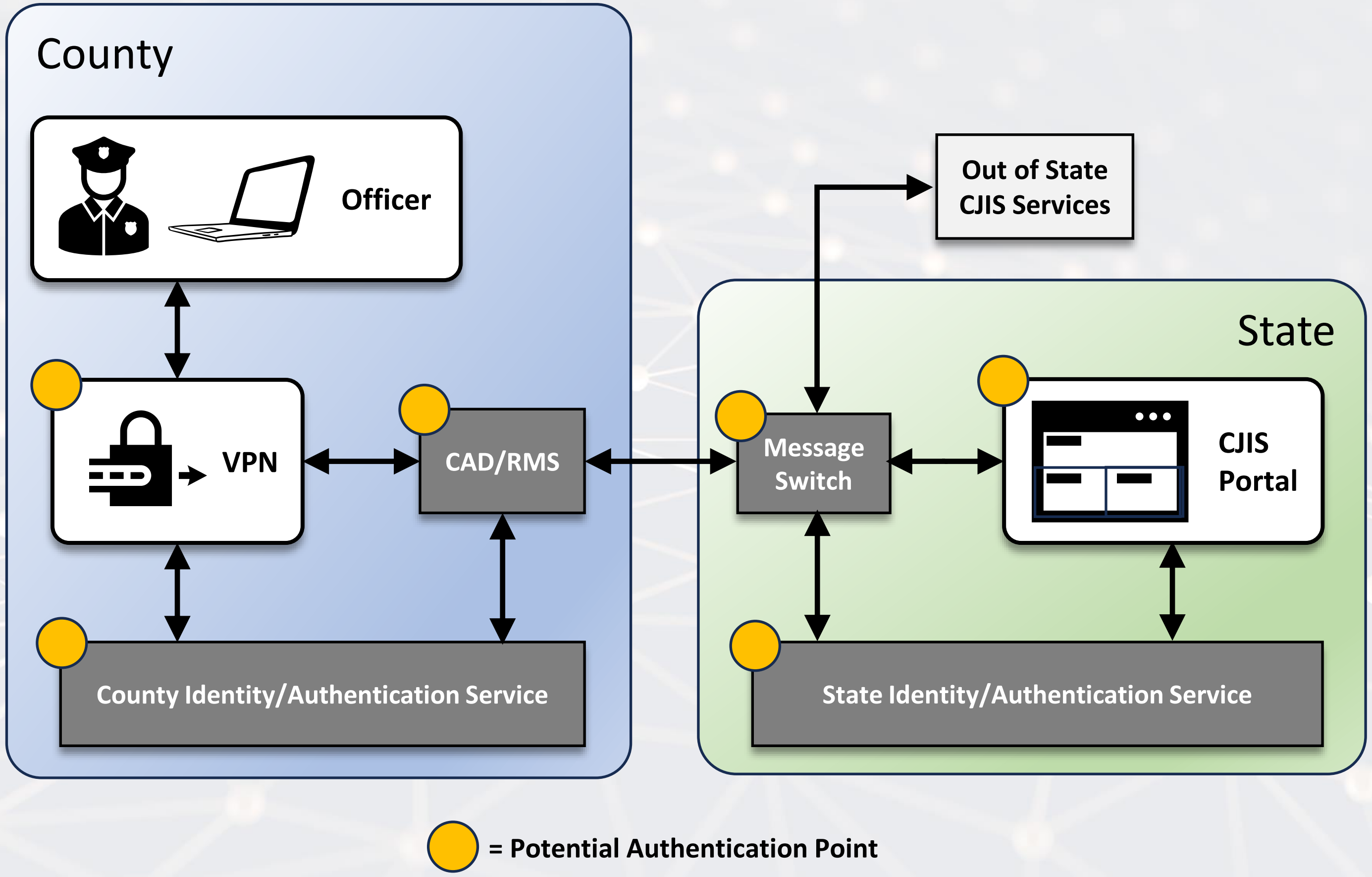
- Dedicated identity services provide several potential benefits:
  - Alleviate the need for other applications to manage user IDs and credentials
  - Identity services often support all major identity protocols and authentication methods
  - Can enable SSO models to reduce the number of credential users need to manage
  - Identity services can be centralized and enable shared service models and/or cost savings



Example of CJIS application behind an SSO service

Example Use Cases

Commonly seen State and Local CJI Architecture

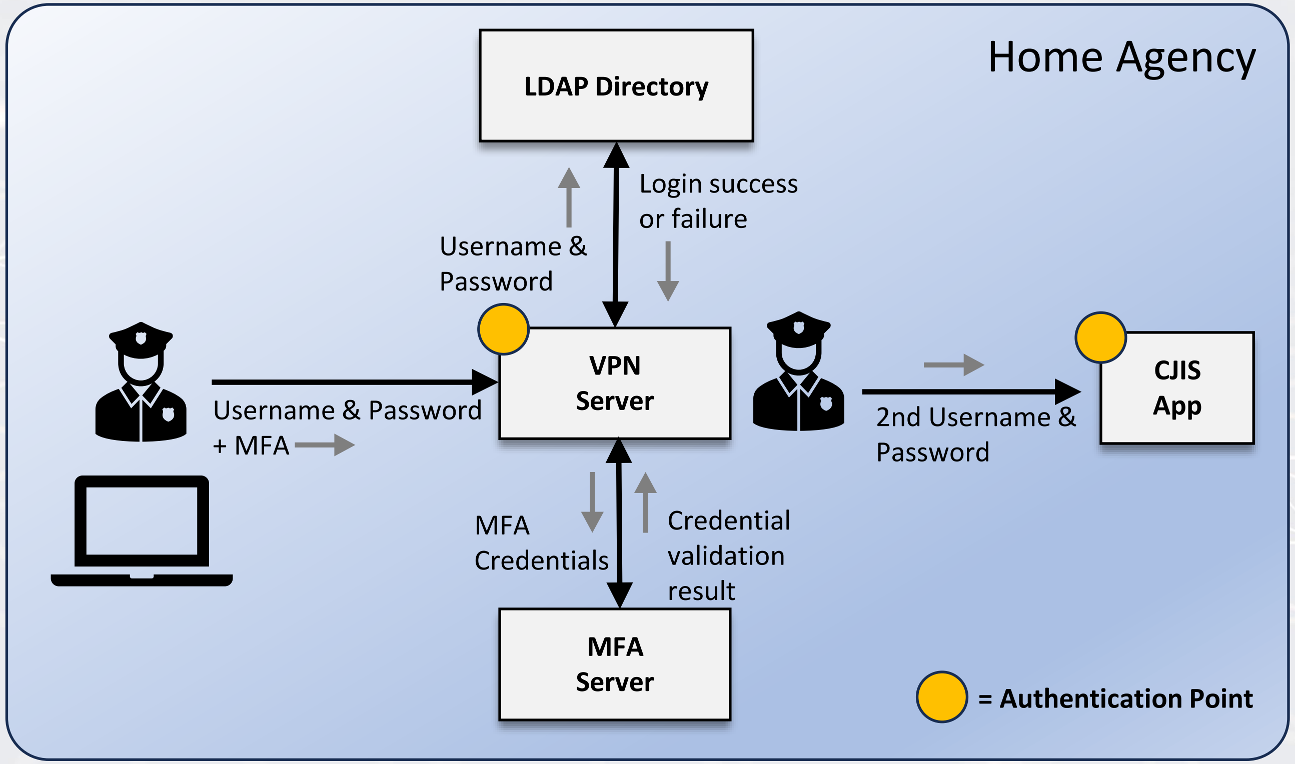

County
Officer
VPN
CAD/RMS
County Identity/Authentication Service
Out of State
CJIS Services
State
Message
Switch
CJIS
Portal
State Identity/Authentication Service
= Potential Authentication Point

Any of the orange dots are reasonable places to implement MFA. However, each comes with potential trade offs against the 4 MFA principles. The tradeoffs chosen will depend on the requirements of individual organizations. The following slides highlight use cases we have seen and ways to implement MFA for those use cases using standards and best practices.

VPN Use Case

VPN Use Case

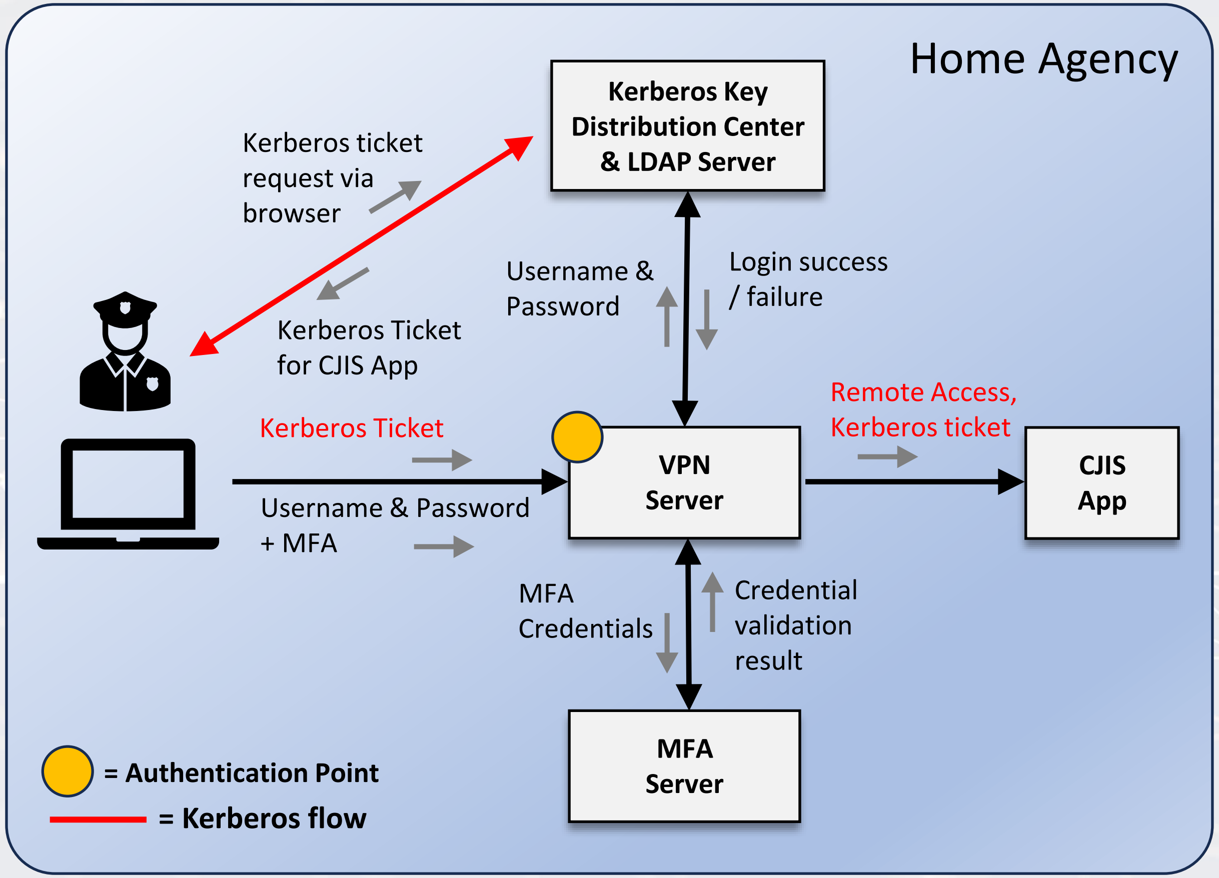
- Implementing MFA at the VPN is a very viable option, but not all implementations are equal.
- In this example, the user authenticates with MFA at a VPN service, but when accessing a CJI application they need a separate username and password.
- In this design MFA is "in front" of the CJIS application, yet the application is still left open to Phishing or Password database breaches.
- Plus, the user has to input and manage a second credential.
- Recall principles #1 and #4



Example when MFA is not integrated with the CJIS application

VPN Use Case with Kerberos

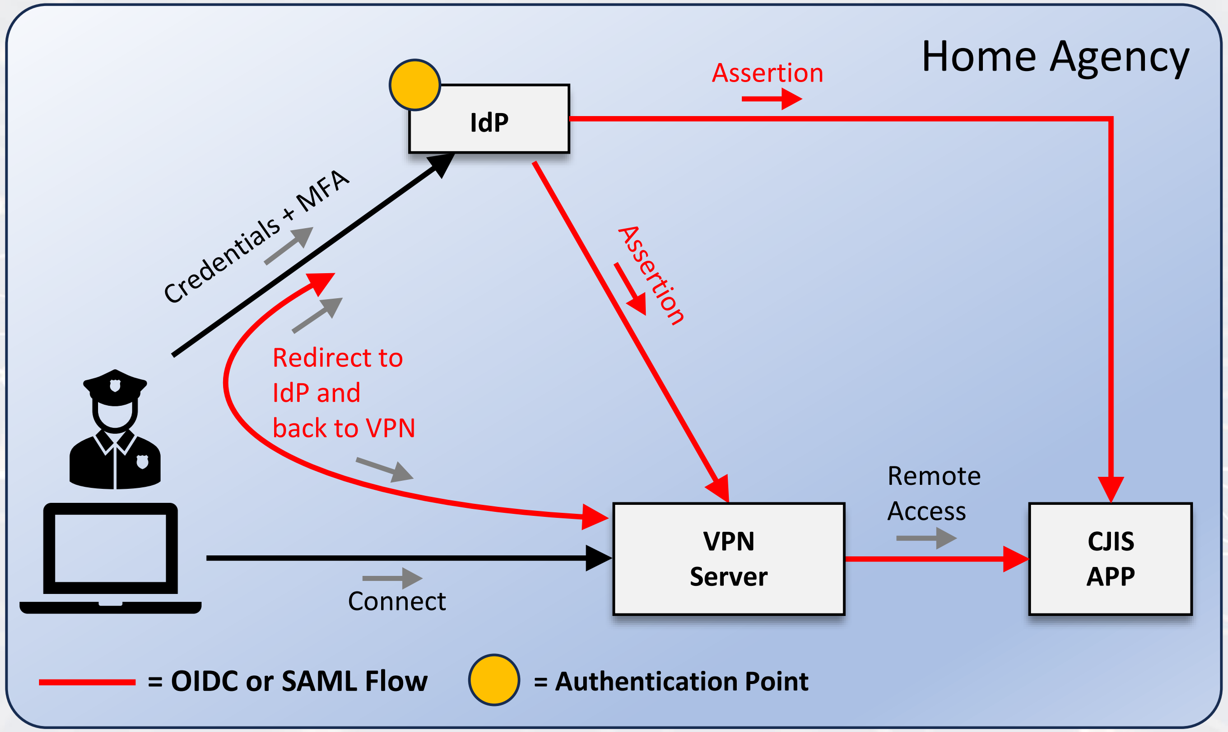
- As mentioned previously a token-based system could help alleviate this. This example shows a Kerberos-centric architecture.
- Once the user successfully authenticates to the VPN service with their MFA credentials, rather than providing a second username and password to the CJIS application, the user's browser gets redirected back to the LDAP service and is given a Kerberos ticket that can be presented by the browser to access the CJIS application.
- Benefits:
  - User no longer needs to manage a second credential
  - Kerberos tickets are not phishable
  - No need for a password database associated with the CJIS app.


Home Agency
Kerberos Key Distribution Center & LDAP Server
Kerberos ticket request via browser
Kerberos Ticket for CJIS App
Username & Password
Login success / failure
Remote Access, Kerberos ticket
Kerberos Ticket
Username & Password + MFA
VPN Server
CJIS App
MFA Credentials
Credential validation result
MFA Server
● = Authentication Point
= Kerberos flow

Example of how MFA at the VPN could be integrated using Kerberos

VPN Use Case with Federation

- Similar to Kerberos, federation protocols like OIDC and SAML can be used.
- In this scenario the user authenticates at the IDP and is given an assertion, an OpenID or SAML token, that can be given both to the VPN service and the CJIS App.
- Benefits:
  - User no longer need to manage a second credential
  - SAML/OIDC tickets are not phishable
  - No need for a password database associated with the CJIS app.

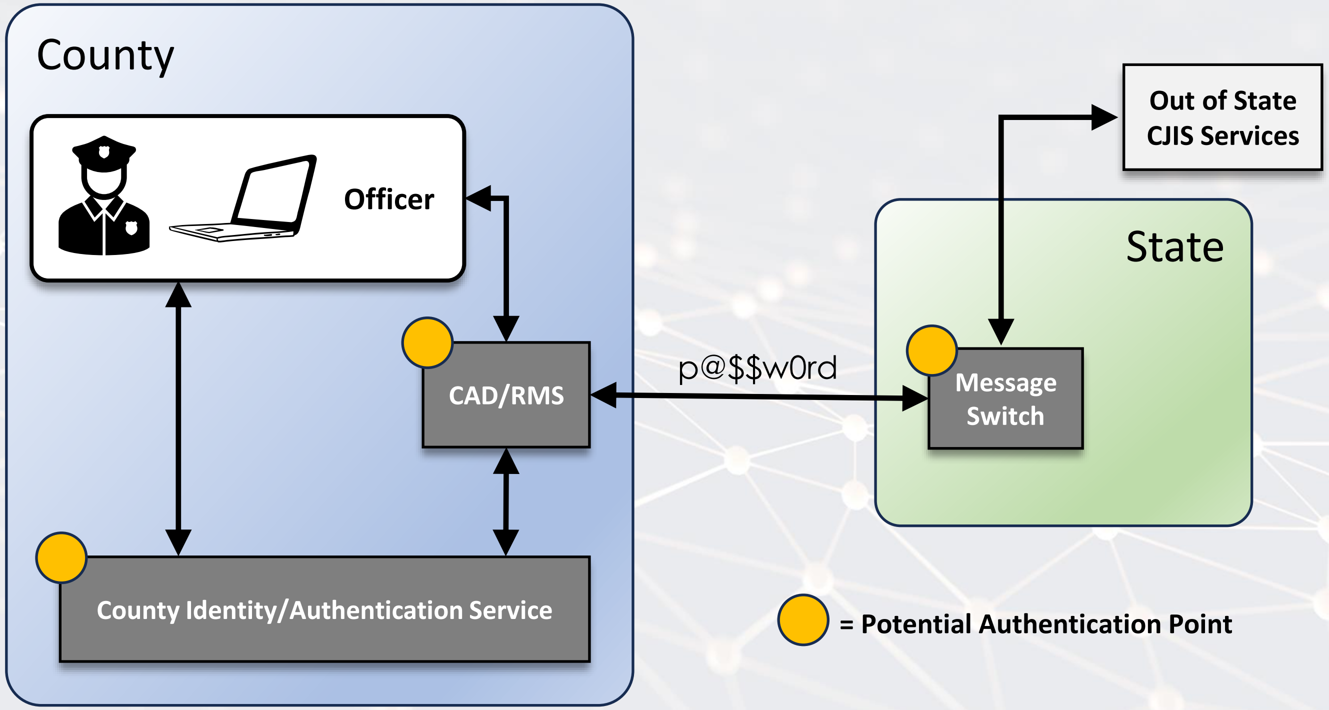


Example of how MFA at the VPN could be integrated using SAML or OIDC

Local Agency Use Case

Common MFA implementations for Local Agency

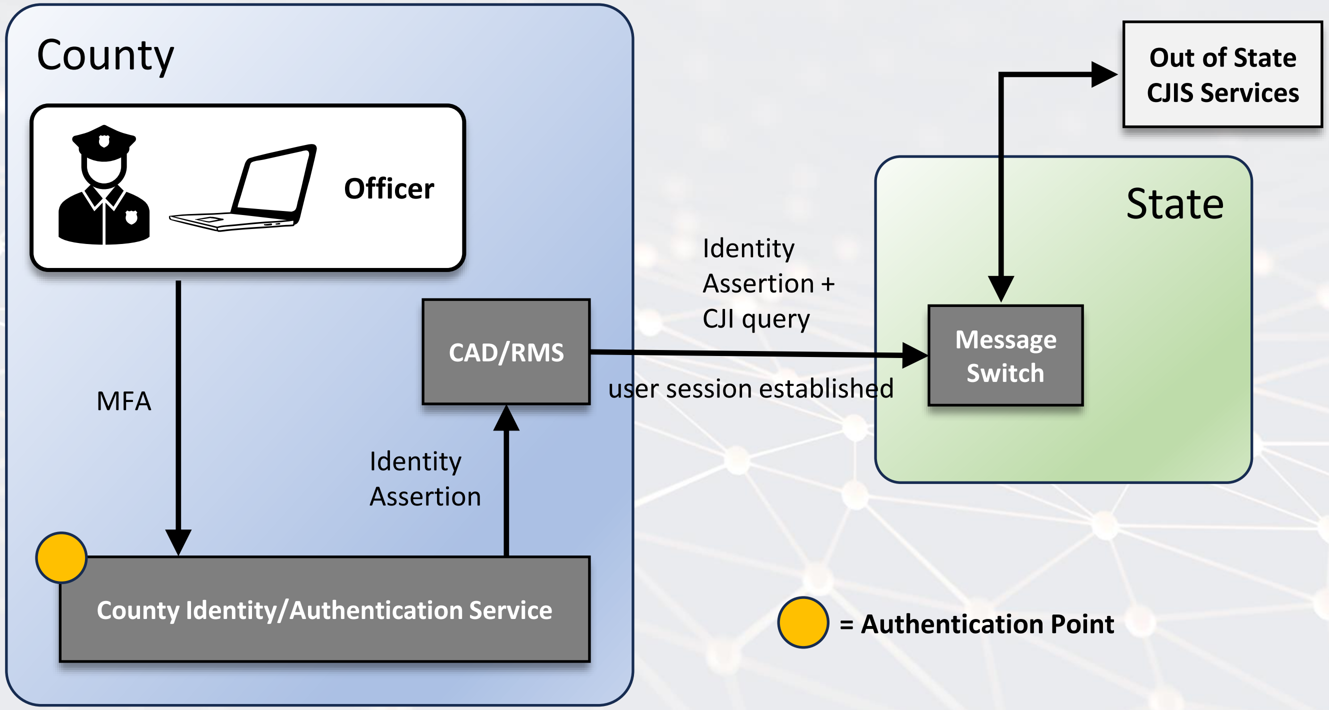
- MFA integrated at message switch:
  - May not have MFA optionality
  - MFA likely cannot be reused
- MFA integrated at the CAD/RMS
  - May not have MFA optionality
  - MFA likely cannot be reused
  - Identity information needs to be passed between CAD/RMS and Message Switch
- MFA at local Identity service
  - Likely to have more MFA optionality
  - MFA can likely be reused
  - Identity information still need to be passed to other applications


County
Officer
CAD/RMS
County Identity/Authentication Service
p@$$w0rd
Out of State CJIS Services
State
Message Switch
● = Potential Authentication Point

Simple but common architecture of how local agencies access CJI

Potential MFA implementations for Local Agency

- MFA integrated at local agency identity service to maximize authenticator optionality and re-useability
- Federation protocols use to integrate MFA with CAD/RMS
- Federation protocols allow for the sharing of identity information between CAD/RMS and message switch without sharing passwords.

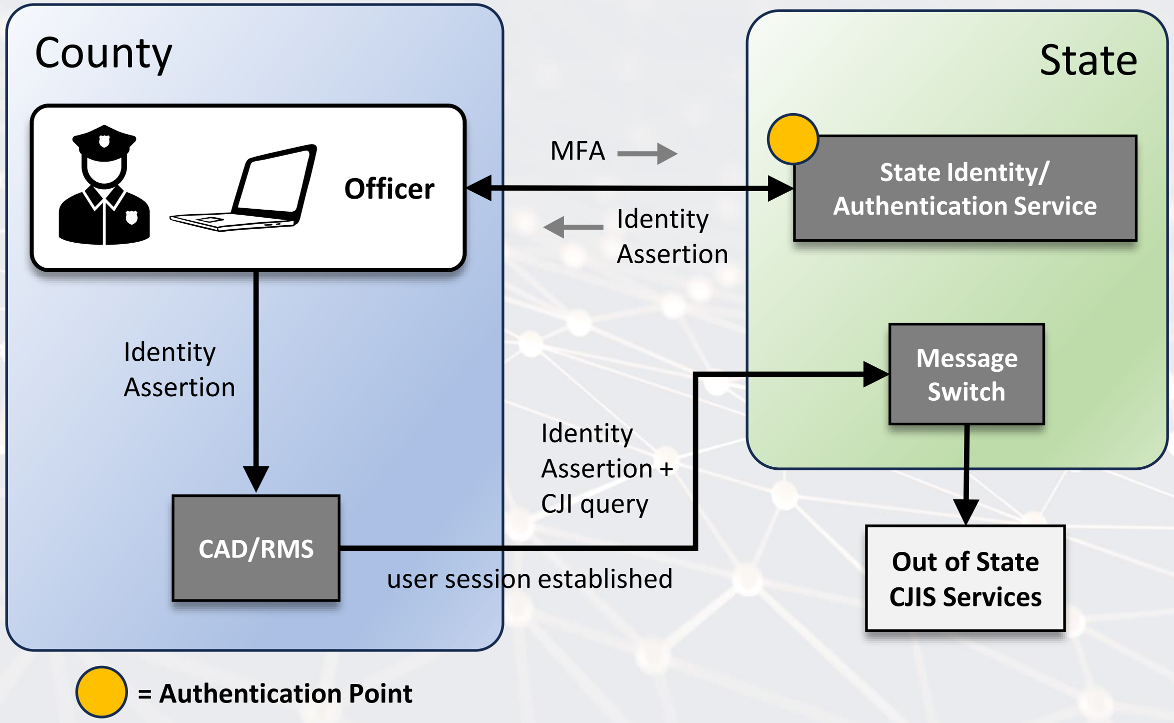


County IDP integrated with CAD and RMS using Identity Federation

NOTE: This requires CAD/RMS and Message switch vendors to support federation protocols.

Potential State IDP for Local Agency

- In this model the state agency IDP is an identity service that can offer local agencies MFA capabilities
- Similar to the last model integrating with identity service typically offers maximum MFA optionality and re-usability
- This model could be good for small and rural agencies who cannot implement their own MFA
- This could also enable a shared service model where the state acting as IDP could save on costs and MFA implementation variation across the state



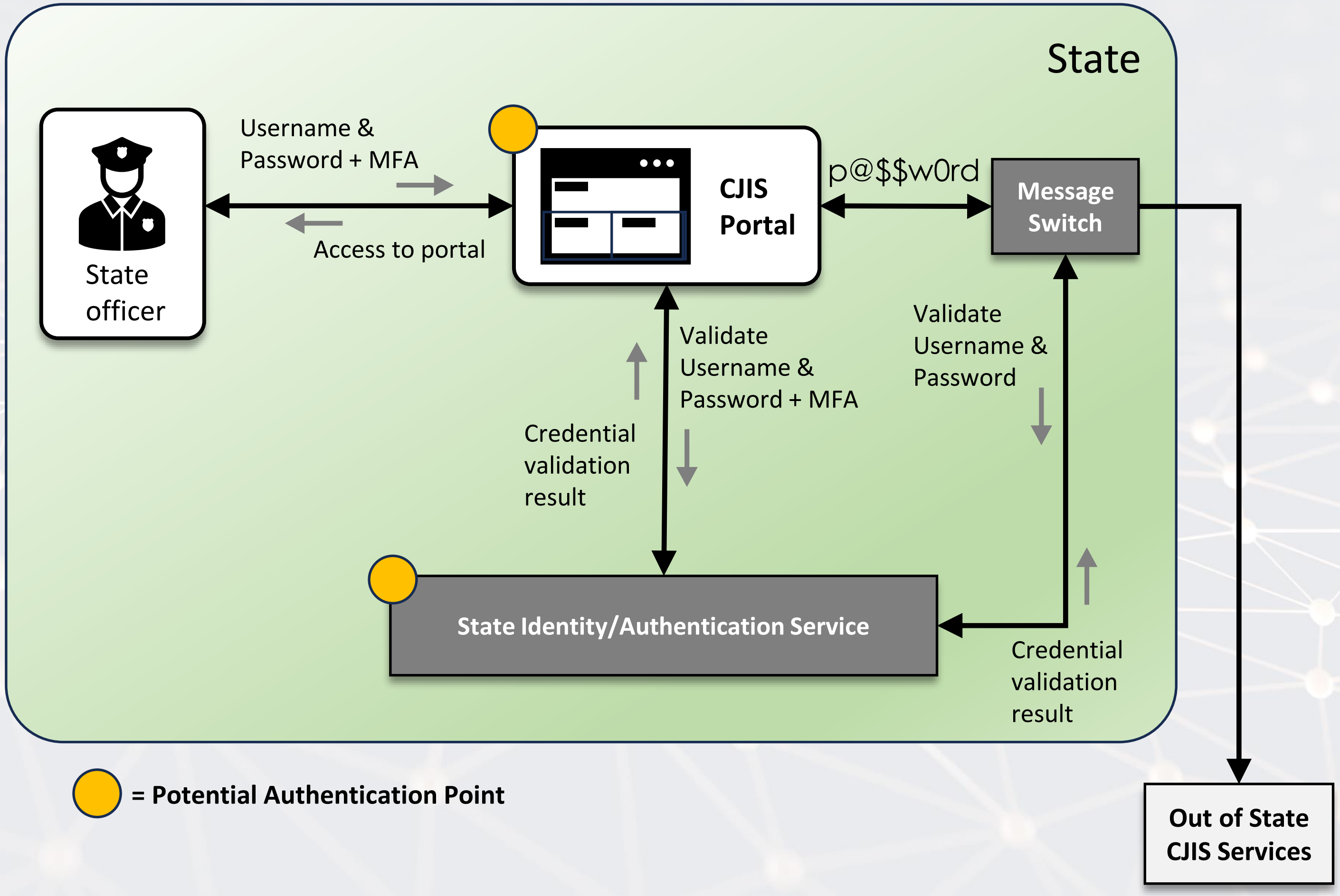
State IDP integrated with Local CAD and RMS using Identity Federation

NOTE: This requires CAD/RMS and Message switch vendors to support federation protocols.

State Agency Use Case

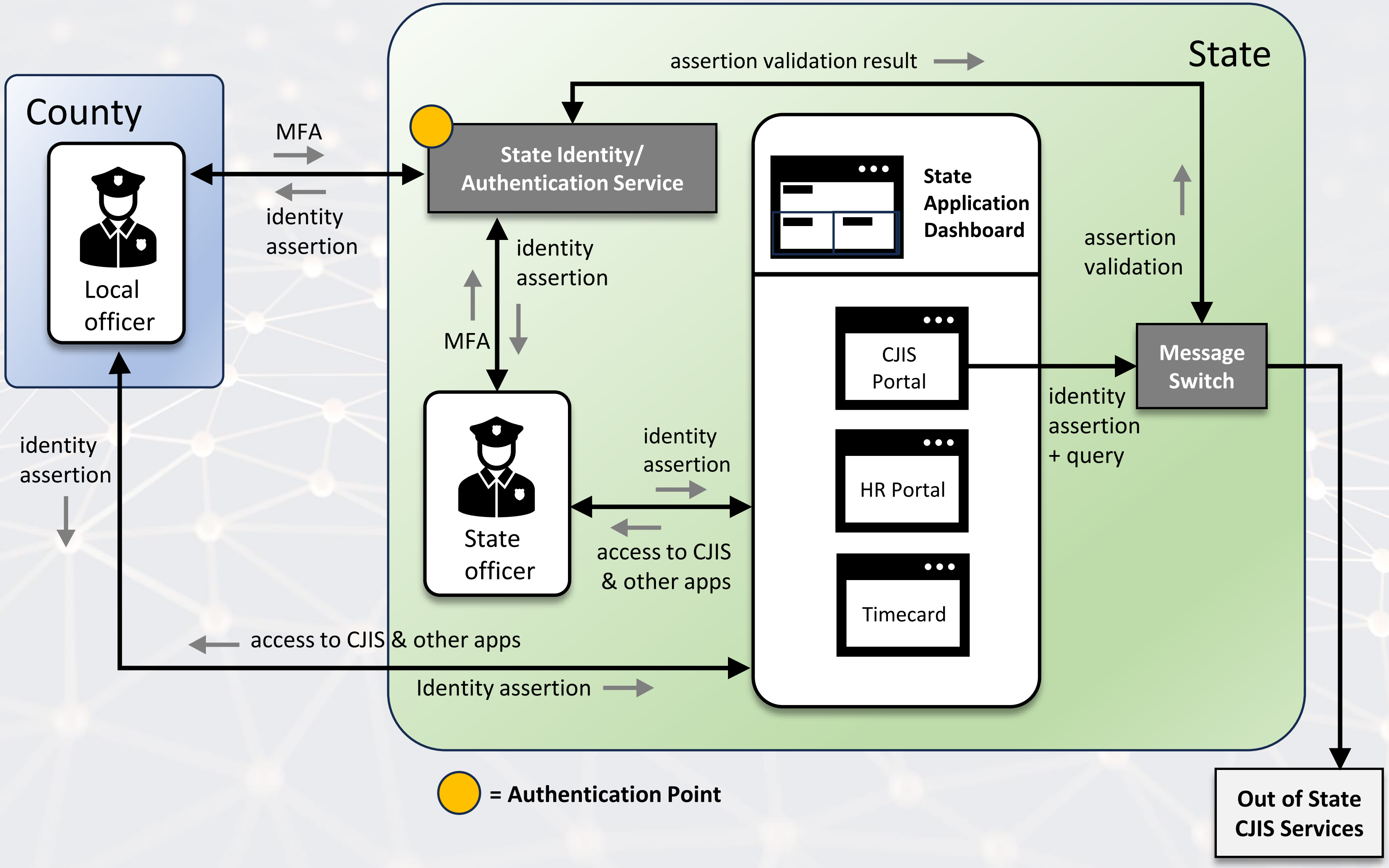
Common State Portal Deployment

- MFA integrated at the state portal:
  - May not have MFA optionality
  - MFA likely cannot be reused
- MFA integrated at the state identity service:
  - Likely to have more MFA optionality
  - MFA can likely be reused
  - Identity information still need to be passed to other applications
- With this model we've still seen the need to pass a password to the state switch for verification.


State
State officer
Username & Password + MFA
Access to portal
CJIS Portal
p@$$w0rd
Message Switch
Validate Username & Password + MFA
Credential validation result
Validate Username & Password
State Identity/Authentication Service
Credential validation result
Out of State CJIS Services
= Potential Authentication Point

Potential State Portal Deployment

- Diagram shows state CJIS portal integrated with an application dashboard accessible via state and local users authenticating at the state identity service
- Many organizations have this type of dashboard. It could be leveraged for CJIS applications
- The dashboard vendors are usually also identity service vendors that support federation protocols and many different types of authentication
- Putting multiple applications, both CJI and Non-CJI enables single sign-on and minimizes the number of credentials users need to manage



NOTE: This requires CAD/RMS and Message switch vendors to support federation protocols.

Questions & Discussion

Call to Action

- Whether you're a vendor or agency consider the MFA implementation principles.
- We would love to see more support amongst public safety technology for the protocols we've talk about in this presentation.
- This mission space is important and we all have a role to play in MFA implementation.
- There is business value to be had by vendors and agencies alike.

PULLING THE FUTURE **FORWARD**

Contact Us

✉ Email us: psfr-nccoe@nist.gov

Join our community of interest and get updates on our work:
https://www.nccoe.nist.gov/public-safety-first-responder