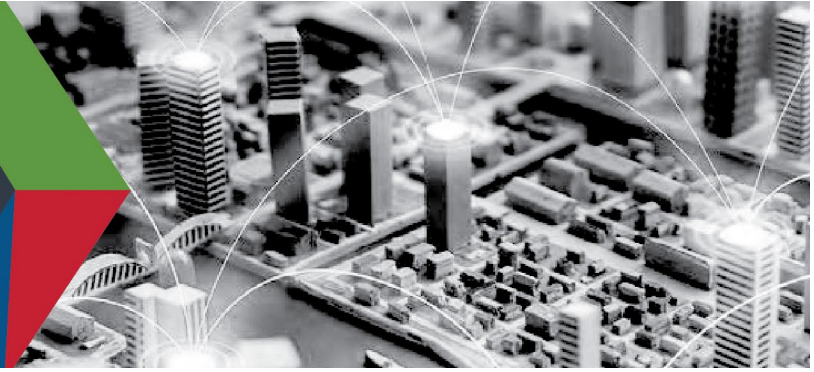
DEFEND TODAY, SECURE TOMORROW



IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT PILOT FOR PUBLIC SAFETY

As new technologies increase public safety's reliance on data, first responders face increasing cyber threats that require innovative techniques to manage risk and secure information exchange between operational partners. Federated identity, credential, and access management (ICAM)[1] is an important cybersecurity component that allows agencies to safely access resources across existing systems and emerging platforms like the nationwide public safety broadband network[2] and next generation 911. As such, partners are encouraged to develop guidance on how to implement federated ICAM in an effective and actionable way across the community.

FEDERATED ICAM: TRUSTMARK FRAMEWORK

TRUSTMARK FRAMEWORK KEY CONCEPTS[3]

- A **Trustmark** is a statement of conformance to a well-scoped set of identity or interoperability requirements
- The formal assessment process for a Trustmark is specified by a **Trustmark Definition** (TD). A group of TDs form an agency's **Trust Interoperability Profile** (TIP)
- A **Trustmark Provider** (TP) issues a Trustmark to a **Trustmark Recipient** (TR) based on a formal assessment process
- The Trustmark is issued under a **Trustmark Policy** and is subject to a **Trustmark Agreement**

Despite recent progress made in ICAM initiatives across the nation, disparities in current solutions make it difficult for public safety organizations to confidently and quickly access important information from systems outside of their domain(s).

In 2016, SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) established the ICAM Working Group to help address ICAM-related issues that impact public safety and national security/emergency preparedness information sharing.[4] In 2017, the Working Group issued a position paper encouraging public safety agencies to consider the Trustmark Framework, a Federated ICAM trust identity management concept developed by the Georgia Tech Research Institute (GTRI).[5]

The Trustmark Framework is a means to achieve interoperability and trust between various identity federations without the use of explicit, written bilateral agreements. The Framework seeks to enable agile, scalable, and rigorous trust management by providing a template for: (1) data owners to codify their security policies; and (2) data users (requestors) to show conformance with those policies. These statements of conformance, known as Trustmarks, can then be reused to achieve greater adaptability, interoperability, and potential cost savings for the public safety community.[6]

---

[1] Federated ICAM is a set of technologies which allows organizations to broker information on identities, identity attributes, and authentication that is used to provide secure access to applications and collaboration resources. This approach to identity management is typically used by large organizations or groups of organizations to establish a trusted information sharing environment known as an "identity federation."
[2] The NPSBN is administered by the First Responder Network Authority (FirstNet Authority). For more information, visit https://www.firstnet.gov/.
[3] Georgia Tech Research Institute (GTRI), "GTRI NSTIC Trustmark Pilot – the Technical Framework," last accessed on October 4, 2019.
[4] Department of Homeland Security (DHS) "SAFECOM and NCSWIC Encourage Public Safety to Adopt Trustmark Framework," May 16, 2017.
[5] SAFECOM and National Council of Statewide Interoperability Coordinators (NCSWIC), "Position Paper: Endorsing the Trustmark Framework," last accessed on October 4, 2019.
[6] GTRI, "GTRI NSTIC Trustmark Pilot," last accessed on October 4, 2019.

CONNECT WITH US
www.cisa.gov

For more information,
email PublicSafetyComms@cisa.dhs.gov

Linkedin.com/company/cybersecurity-and-infrastructure-security-agency

@CISAgov | @cyber | @uscert_gov

Facebook.com/CISA

TRUSTMARK FRAMEWORK PILOT

In 2019, the Cybersecurity and Infrastructure Security Agency (CISA) and the Office of the Director of National Intelligence (ODNI)—in collaboration with the SAFECOM and NCSWIC ICAM Working Group—conducted two ICAM pilot demonstrations. Personal Identity Verification-Interoperable (PIV-I) cards and Fast Identity Online (FIDO) credentials[7] were evaluated and used by federal, state, local, tribal, and regional public safety users in Texas and Tennessee to obtain user feedback. The overall purpose of the project was to advance the state of public safety ICAM by demonstrating the integration and application of the Trustmark Framework and the following technologies within the National Identity Exchange Federation (NIEF):[8]

Security Assertion Markup Language (SAML)	An open standard protocol for exchanging authentication and authorization data between parties—particularly between identity provider (IdP) and service provider (SP) systems—as part of federated ICAM transactions for information sharing (http://xml.coverpages.org/saml.html).
Personal Identity Verification-Interoperable (PIV-I)	A federal standard for strong multi-factor physical and logical user authentication credentials based on public key infrastructure (PKI) currently in use by a large subset of public safety personnel across the United States (https://doi.org/10.6028/NIST.FIPS.201-2).[9]
Fast Identity Online (FIDO)	A commercial standard for strong multi-factor user authentication credentials, developed by the FIDO Alliance industry group, based on PKI and targeted primarily towards mobile devices (https://fidoalliance.org/).

Figure 1. Federated ICAM Technologies

During the demonstrations, participants used the technologies defined in **Figure 1** to experience, first-hand, the following ICAM concepts commonly used by industry and the federal government:

- **Identity federation,** the ability of one organization to accept identity and credentials from another,
- **Strong authentication,** authentication using two or more factors as a replacement for passwords, and
- **Single sign-on (SSO),** the use of a single authentication to grant access to multiple resources.

CISA and ODNI accomplished three primary technical objectives during the project:

- **Issued** PIV-I and FIDO credentials based on identity assurance policies and procedures asserted by the Trustmark Framework;
- **Established** the use of SAML and the Trustmark Framework to enable public safety personnel's access to sensitive NIEF resources[10] using newly dispensed PIV-I and FIDO credentials; and
- **Developed** software tools, artifacts, and federated ICAM implementation guidance based on field tests, so that agencies can adopt their own solutions in accordance with well-accepted guidance.

The Texas Department of Public Safety and the Tennessee's Dangerous Drug Task Force hosted the pilot demonstrations and provided resources to support planning and demonstration-day activities.

[7] PIV-I and FIDO credentials were selected due to their wide-adoption and applicability for public safety.
[8] An operational identity federation for law enforcement and public safety communities that provides existing information sharing services and resources via federated ICAM. For more Information, visit https://nief.org/.
[9] The PIV-I standard was developed in response to Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors (2004). For more information, visit https://www.dhs.gov/homeland-security-presidential-directive-12.
[10] Subject to applicable access control policies.

KEY FINDINGS

The PIV-I and FIDO pilot demonstrations were conducted in July and August 2019, respectively. Key findings can be categorized as follows:[11]

Desire for strong identity management. Overall, pilot participants indicated a desire for stronger user credentials and authentication. As a result, the demonstrations received largely positive feedback from both participants and observers.

Viability of PIV-I and FIDO. PIV-I credentials are inherently more secure as they offer higher levels of identity proofing and are less prone to tampering. However, PIV-I smartcards are not compatible with mobile devices. While FIDO does not support the same level of high-end assurance, it is more easily integrated on mobile, which allows for the use of "bring your-own-device" policies. FIDO credentials are also available in a range of different form factors, as compared to the standard PIV-I card.

Accessibility and ease of use. Participants indicated that the pilot technologies were easier to use and more secure than traditional login methods (e.g., passwords). Some participants who were initially apprehensive about the technology changed their minds after undergoing the issuance process and using new credentials to access various systems.

Opportunities for cost savings. The pilot demonstrated that, when applicable, PIV-I or FIDO can provide strong multi-factor authentication. This means that these solutions could offer a certain level of affordability and product selection for large parts of the public safety community.

Requirements to scale. Increased adoption of the Trustmark Framework is not possible without additional entities providing technical expertise and being willing to serve as Trustmark Providers (issuers). As such, automated tools need to be developed to assist with Trustmark issuance and usage. CISA is continuing to define and engage on issues of scale.

FUTURE CONSIDERATIONS

As ICAM technologies continue to emerge and evolve, public safety organizations are encouraged to prepare for the incorporation of ICAM into their information sharing operations. Below are some steps to consider when developing technical, governance, and policy best practices for ICAM:

- **Review** lessons learned from the pilot demonstrations and discuss future ICAM applications across the larger public safety community;
- **Support** efforts to integrate PIV-I and FIDO IdPs and users into the NIEF;
- **Expand** ICAM outreach to other public safety groups, and organizations;
- **Determine** available local and regional application services for end users;
- **Identify** other public safety networks/federations that may wish to integrate with NIEF or have an interest in federated identity;
- **Connect** state, local, and tribal agencies to ICAM subject matter expertise and early adopters to support public safety information sharing initiatives; and
- **Train** personnel on the latest technologies, service offerings, and best practices.

Public safety partners could also work with CISA to: (1) implement consistent ICAM standards, policies, procedures; and (2) develop interoperability and implementation guidance for community-wide use.

FOR MORE INFORMATION

To find out more, visit https://www.cisa.gov/safecom/icam-resources, or email PublicSafetyComms@cisa.dhs.gov.

[11] This list is meant to provide a representative sampling of participant and observer feedback on the pilot, received in real-time/in response to survey questions. Detailed survey results, lessons learned, and technical findings are provided in GTRI and CISA after-action documentation.