Trustmark Framework for Public Safety

SAFECOM NCSWIC

What is the Trustmark Framework?

The Trustmark Framework, currently in use by many law enforcement organizations around the country, establishes a mechanism for codifying and reusing components of different identity, credential, and access management (ICAM) solutions.

What role does the Trustmark Framework play in ICAM?

The Trustmark Framework can help achieve interoperability between various communities of interest (COI) and identity federations without requiring explicit bilateral agreements. While different COIs often have their own specific rules to enable trust, there are also certain requirements that are consistent across communities. Trustmarks are a means to codify those rules in a machine-readable format.

What are the benefits of the Trustmark Framework?

A significant barrier to ICAM adoption is the difficulty in enabling trust and interoperability across multiple COIs and trust frameworks. By codifying and reusing components of different trust frameworks, the Trustmark Framework promotes mutual trust and interoperability in a manner that is scalable, standardized, reliable, modular, decentralized, secure, affordable, and sustainable.

Trustmark Framework Terms

Trust Framework – any structure that builds trust among organizations or users for the purpose of sharing information and reusing identities.

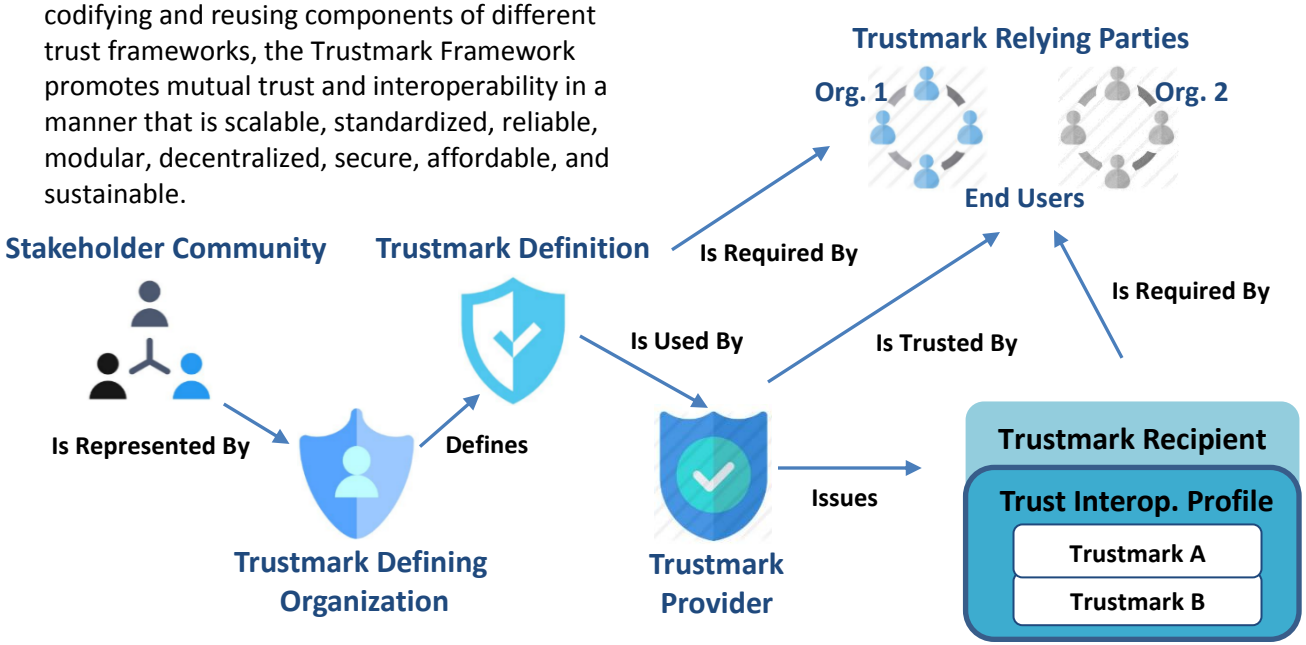
Trustmark –a set of machine-readable trust and/or interoperability criteria that can be used by one or more federations.

Trustmark Provider – an organization authorized to develop and issue trustmarks.

Trustmark Relying Party – a service, site or entity that relies on a third -party identity provider to authenticate users.

Trustmark Framework Concept Map

ICAM policies from different identity federations are identified and codified in a "Trustmark Definition." Approved trustmark providers use these definitions to issue trustmarks that can be used by multiple entities. The Trustmark Framework is emerging as a viable paradigm for enabling scalable and agile trust for many organizations and communities.



Who Developed the Trustmark Framework?

The Trustmark Framework was developed by the Georgia Tech Research Institute (GTRI) under funding from the National Strategy for Trusted Identities in Cyberspace (NSTIC) as one of the pilot programs for "catalyzing the identity ecosystem."

What is the current progress of the Trustmark Framework?

The National Identity Exchange Federation (NIEF) is the largest organization leveraging the Trustmark Framework. Trustmarks are currently in use by NIEF partners such as the Department of Justice and reviewed by other trust framework providers.

NIEF is also aligned with the Federal Identity, Credential, and Access Management (FICAM) program, and has been recognized as one of FICAM's five approved "trust framework providers."

Public Safety ICAM Initiatives Related to the Trustmark Framework

Federal Identity, Credential, and Access Management (FICAM) – created in 2008, FICAM coordinates the US Federal agencies on execution of the related policy, standards, implementation guidance, and information technology architectures.

Global Federated Identity and Privilege Management (GFIPM) Program – initiated in2005, the GFIPM program is part of the Global Justice Information Sharing Initiative. GFIPM seeks to develop secure, scalable, and cost-effective technologies for information sharing within the law enforcement and criminal justice communities.

National Identity Exchange Federation (NIEF) – NIEF is a collection of federal agencies that share sensitive law enforcement information. NIEF leverages existing GFIPM work products and also serves as a source of real-world feedback to drive the development of new GFIPM work products.

State Identity, Credential, and Access Management (SICAM) – the SICAM architecture enables states and their partners to share and audit identification, authentication, and authorization across state enterprise boundaries.

National Strategy for Trusted Identities in Cyberspace (NSTIC) – administered through NIST, NSTIC charts a course for the public and private sectors to collaborate to raise the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions.

The following resources provide additional information about the Trustmark Framework and other related ICAM initiatives:

2014 National ICAM Strategy Summit: After Action Report – the *2014 ICAM National Strategy Summit: After Action Report* provides foundational information on ICAM, identifies key ICAM principles and recommended actions.

GTRI NSTIC Trustmark Pilot – GTRI maintains a website with general information, technical specifications, and artifacts for the Trustmark Framework.

Policies for NIEF Trustmarks - NIEF offers a wide range of trustmarks to its members and other agencies that wish to participate in the emerging Trustmark ecosystem.

ISE Article – an ISE story on the NIEF Trustmark Pilot for Federated ICAM and its goals.

ISE Blog Post – blog post on the Trust Framework and its inclusion as a FICAM Trust Framework Provider.

NSTIC Pilots: Catalyzing the Identity Ecosystem (NISTIR 8054) – summaries and outcomes of NSTIC pilots, including the Trustmark Framework.

List of FICAM's "Adopted Trust Framework Providers" – the Trust Framework Solutions (TFS) program assesses the Trust Frameworks of commercial and non-profit organizations to determine if the polices, processes and technologies are comparable to the US Federal Standards for identity assurance, authentication assurance and privacy protections.

Visit the SAFECOM website to learn more about ICAM and the Trustmark Framework:
https://www.dhs.gov/safecom/icam-resources