Scaling Interoperable Trust through a Trustmark Marketplace

Georgia Tech Research Institute
December 2013

This work was performed under the following financial assistance award 70NANB13H189 from the U.S. Department of Commerce, National Institute of Standards and Technology.
The Trustmark Pilot Team

Georgia Tech Research Institute

NIEF

RISS

CISA

Pennsylvania Network

APIARY

NASCIO

Representing Chief Information Officers of the States
In the Beginning...

Lots of Application-Specific Identity Silos
Along Came Federated Identity…

Decouple Identities from Applications!

Identity Provider

Standard Protocols

Application (Service Provider)

User
Along Came Federated Identity…

Identity Provider

Attribute Provider

Standard Protocols

Application (Service Provider)

User
Along Came Federated Identity…

Identity Provider

Attribute Provider

Standard Protocols

Application (Service Provider)

User

So what about Trust, Liability, Security?
And Today...

Lots of **Federated** Identity Silos
There exist many Trust Frameworks.
Each Trust Framework requires agreement across many dimensions.
Many Trust Frameworks are **monolithic and opaque**.
Achieving Cross-Framework Trust

Suppose this user needs access to this RP.

In today’s ID Ecosystem, there are at least five ways to do it...

...and all of them face challenges.
Option #1: User Creates a New Identity

But now she has to manage multiple identities!
Option #2: IDP Joins New Trust Framework

But joining a new Trust Framework is **complex and expensive**!
Option #3: RP Joins New Trust Framework

Same problem here: Joining a new Trust Framework is **complex and expensive**!
Option #4: Cross-Framework Relationship

But this is **fraught with challenges** at many layers: technical, policy, legal, etc.
Option #5: Bilateral IDP-RP Relationship

But this is **highly UN-scalable and also fraught with challenges.**
The Perspective from the LE Community

- Law Enforcement COI has over 1 million people in the US alone
- Required to share data across jurisdictions
- But must obey applicable access controls when sharing
- Trust between agencies is a fundamental requirement
- Most users must have high-assurance credentials
- LE agencies are autonomous (NOT centrally funded)
- 3rd party trust is required due to COI size and complexity
- Legitimate business need to interact with many other COIs
- LE agencies are highly heterogeneous

Federal Agencies
State Agencies
Local Agencies
Tribal Agencies
Task Forces
Fusion Centers
The Perspective from the LE Community
The Perspective from the LE Community

State ISE SICAM

Critical Infrastructure

Health ISE

NIEF

GFIPM

RP RP RP
IDP IDP AP

RP RP RP
IDP IDP AP

RP RP RP
IDP IDP AP

RP RP RP
IDP IDP AP

RP RP RP
IDP IDP AP

RP RP RP
IDP IDP AP

RP RP RP
IDP IDP AP

RP RP RP
IDP IDP AP

RP RP RP
IDP IDP AP

RP RP RP
IDP IDP AP

RP RP RP
IDP IDP AP

RP RP RP
IDP IDP AP

RP RP RP
IDP IDP AP

RP RP RP
IDP IDP AP

RP RP RP
IDP IDP AP
Where to from here?
Is the ID Ecosystem only about identification and authentication?

Or are attributes and authorization fundamental to it?
A Variety of ID Ecosystem Perspectives

Will the ID Ecosystem have very few IDPs with consistent user bases and requirements?

Or a large number of IDPs with heterogeneous user bases and requirements?
A Variety of ID Ecosystem Perspectives

Will Trust Frameworks remain static over time?

Or must they constantly evolve to meet new requirements?
Is it OK if the Trust Frameworks in the ID Ecosystem are mostly non-interoperable and non-trusting identity silos?
Or does success demand that we at least provide a **viable strategy and framework for trust and interoperability** between various COIs, ISEs, and Federations?
What about a Trustmark Framework?

If the frameworks were modular...

If the frameworks were modular...

- Greater transparency of trust framework requirements
- Greater ease of comparability between frameworks
- Greater potential for reusability of framework components
- Greater potential for participation in multiple trust frameworks by ID Ecosystem members with incremental effort and cost

And, most importantly:
What about a Trustmark Framework?

These modular components are called **Trustmarks**.
A Few Examples of Trustmarks

- FICAM SAML SSO Profile
- NIST 800-63 / FICAM LOA 3 Identity
- Fair Information Practice Principles (FIPPs)
- FIPS 200 Security Practices
- GFIPM Metadata Registry (User Attributes)
A Trustmark-Based ID Ecosystem

Rather than requiring a monolithic, formalized Trust Framework...
A Trustmark-Based ID Ecosystem

...each community can define a TIP.
A Trustmark-Based ID Ecosystem

Then each member of the community can acquire the necessary Trustmarks based on the TIP.
A Trustmark-Based ID Ecosystem

Trustmarks can be acquired through a Trustmark Provider.
A Trustmark-Based ID Ecosystem

There can be many Trustmark Providers in the ID Ecosystem.
Some Trustmark Providers may specialize in issuing one particular Trustmark. Others may offer many Trustmarks.
A Trustmark-Based ID Ecosystem

Trustmarks can be stored in a searchable Trustmark Registry.
A Trustmark-Based ID Ecosystem

Members of the ID Ecosystem can query a Trustmark Registry to answer questions such as:

“What other members of the ID Ecosystem have the necessary Trustmarks to meet MY trust requirements?”

“What Trustmarks must I acquire to meet the trust requirements of <MEMBER>?”
This collection of actors and entities is the **Trustmark Marketplace**.
Trustmarks – What? Where?
Sources of Components

GFIPM Trust & Interop Components

NIEF Trust & Interop Components

FICAM Trust & Interop Components

AAMVA Trust & Interop Components

Another Component Perspective

Source: Ken Klingenstein, Internet 2
Creating Modular Common Components

Step 1: Gather trust and interop requirements from many frameworks

Step 2: Break down and reassemble requirements into modular, reusable components

Step 3: Express modularized requirements in a standard format to encourage broad reuse
# GTRI NSTIC Pilot Trustmark Analysis

<table>
<thead>
<tr>
<th>TD Name</th>
<th>Source</th>
<th>In Use in NIEF?</th>
<th>Essential to Pilot?</th>
<th>Type</th>
<th>Related Periodic Trust Elements</th>
<th>Related TDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>FICAM Bona Fides IDPO TD</td>
<td>FICAM TFAP, Section 3.3</td>
<td>n</td>
<td>y</td>
<td>bona fides</td>
<td>Identity vetting of</td>
<td>NIEF Bona Fides IDPO TD</td>
</tr>
<tr>
<td>FICAM LOA 2 Assertions TD</td>
<td>NIST SP 800-63-1, Chapter 9. FICAM TFAP, Appendix A-2, Assertions.</td>
<td>n</td>
<td>y</td>
<td>policy: ID assurance</td>
<td>Assurance - Authentication rules</td>
<td>GFIPM SAML SSO Profile IDP TD. FICAM SAML SSO Profile IDP TD.</td>
</tr>
<tr>
<td>FICAM LOA 2 Authentication Process TD</td>
<td>NIST SP 800-63-1, Chapter 8. FICAM TFAP, Appendix A-2, Authentication Process. NIEF Audit Policy, Section 4.1.4.</td>
<td>n</td>
<td>y</td>
<td>policy: ID assurance</td>
<td>Assurance - Identity proofing</td>
<td>Assurance - Authentication rules</td>
</tr>
<tr>
<td>FICAM LOA 2 Registration and Issuance TD</td>
<td>NIST SP 800-63-1, Chapter 5. FICAM TFAP, Appendix A-2, Registration and Issuance. NIEF Audit Policy, Section 4.1.1.</td>
<td>n</td>
<td>y</td>
<td>policy: ID assurance</td>
<td>Assurance - Credential management</td>
<td>Assurance - Credential management</td>
</tr>
<tr>
<td>FICAM LOA 2 Token and Credential Management TD</td>
<td>NIST SP 800-63-1, Chapter 7. FICAM TFAP, Appendix A-2, Token and Credential Management. NIEF Audit Policy, Section 4.1.3.</td>
<td>n</td>
<td>y</td>
<td>policy: ID assurance</td>
<td>Assurance - Credential management</td>
<td>Assurance - Credential management</td>
</tr>
<tr>
<td>ICAM BAE Metadata Consumption TD</td>
<td>ICAM BAE SAML Metadata Profile, Section 2</td>
<td>?</td>
<td>n</td>
<td>tech trust</td>
<td></td>
<td>GFIPM SAML Metadata Consumption TD</td>
</tr>
<tr>
<td>ICAM BAE SAML Protocol Requester TD</td>
<td>ICAM BAE SAML Profiles, Section 4</td>
<td>?</td>
<td>n</td>
<td>tech interop</td>
<td></td>
<td>GFIPM-WS Attribute Provider SIP AC TD</td>
</tr>
<tr>
<td>ICAM BAE SAML Protocol Responder TD</td>
<td>ICAM BAE SAML Profiles, Section 4</td>
<td>?</td>
<td>n</td>
<td>tech interop</td>
<td></td>
<td>GFIPM-WS Attribute Provider SIP AP TD</td>
</tr>
<tr>
<td>NIEF Bona Fides APO TD</td>
<td>NIEF Audit Policy, Section 4.5. NIEF Membership Agreement. NIEF APO Participation Agreement.</td>
<td>n</td>
<td>n</td>
<td>bona fides</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIEF Bona Fides SCO TD</td>
<td>NIEF Audit Policy, Section 4.5. NIEF Membership Agreement. NIEF SCO Participation Agreement.</td>
<td>n</td>
<td>n</td>
<td>bona fides</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIEF Bona Fides TIBO TD</td>
<td>NIEF Audit Policy, Section 4.5. NIEF Membership Agreement. NIEF TIBO Participation Agreement.</td>
<td>y</td>
<td>n</td>
<td>bona fides</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **122 distinct trustmarks identified (so far)**
- Covers FICAM, GFIPM, & NIEF communities
- Also covers FIPPs (privacy) topics
Trustmarks By Category

Identity Assurance Policy  
(10 Total, 10 Essential to Pilot)

Privacy Policy  
(23 Total, 15 Essential to Pilot)

Technical Interoperability  
(57 Total, 8 Essential to Pilot)

Technical Trust  
(4 Total, 3 Essential to Pilot)

Security Policy  
(18 Total, 18 Essential to Pilot)

Attribute Assurance Policy  
(2 Total, 2 Essential to Pilot)

Organizational Integrity / Bona Fides  
(6 Total, 3 Essential to Pilot)

Usability  
(2 Total, 0 Essential to Pilot)
**Scope of the NSTIC Trustmark Pilot**

1. **Concept Maturation**
   - Trustmark Concept Presentation
   - Trustmark Pilot Concept Website
   - Outreach to IDESG
   - Outreach to NIEF Membership
   - Outreach to SICAM Stakeholders
   - Outreach to Other Stakeholders

2. **Trustmark Framework**
   - Normative Trustmark Spec
   - Normative TD Spec
   - Normative TIP Spec
   - Trustmark Policy Template
   - Trustmark Agreement Template

3. **Sample TDs, TIPs, and Trustmarks**
   - Comm. Protocol TDs & Trustmarks
   - Identity LOA TDs & Trustmarks
   - End-User Privacy TDs & Trustmarks
   - Security Policy TDs & Trustmarks
   - Other TDs & Trustmarks
   - Sample TIPs for NIEF Community

4. **Sample Tools**
   - Trustmark Assessment Tool for Trustmark Providers
   - Trustmark Generating & Publishing Tool for Trustmark Providers
   - Trustmark Registry Query Tool

5. **NIEF Pilot**
   - Issue Trustmarks to Current NIEF Members
   - Modify Tech Framework, Specs, TDs, TIPs, Policies, Agreements, and Tools as Needed

6. **Expanded Pilot via NASCIO/SICAM**
   - Identify SICAM Use Cases
   - Issue Trustmarks to More IDPs, APs, and RPs via a New Trustmark Provider
   - Demonstrate SICAM Use Cases in a Multiple-Trustmark-Provider Marketplace
High-Level Project Plan & Timeline

- **Refine Concept as Needed**
- **Develop Concept**
- **Refine Framework as Needed**
- **Develop Trustmark Framework**
- **Refine TDs, Trustmarks, and TIPs as Needed**
- **Develop Sample TDs, Trustmarks, and TIPs**
- **Develop and Refine Sample Trustmark Software Tools**
- **Refine Use Cases & Scenarios as Needed**
- **Develop SICAM Use Cases & Scenarios**
- **Trustmark Pilot in NIEF**
- **Outreach/Prep for Expanded Pilot**
- **Expanded Trustmark Pilot**
- **Community Outreach**
- **Project Oversight & Reporting**
- **SICAM Demo**
How the IDESG Can Help

- Review the trustmark framework
  - Is the framework structured properly?
  - Who should review it to help make this determination?

- Review the TDs developed through the pilot
  - Do we have the right set of TDs?
  - What TDs are missing?
  - How well do existing TDs capture requirements from other existing trust frameworks in the ID Ecosystem?

- Facilitate participation by the “right” TDOs
  - What group is best suited to maintain each TD over time?
    - E.g., NIST, FICAM, industry groups and SDOs, etc.
Visit us at
https://trustmark.gtri.gatech.edu