Scaling Interoperable Trust through a Trustmark Marketplace

John Wandelt
Georgia Tech Research Institute
NASCIO Survey on ID Management

CIOs say that the most significant barriers to adoption of an enterprise IAM strategy are:

• The decentralized environment of the state
• The cost of doing so
• The complexity of legacy systems
• The lack of governance
Scope of FICAM & SICAM

Enable Trust and Interoperability
- Internal to the Federal Community (IEE)
  - Intra-Agency
  - Inter-Agency
- With Other Governments (G2G)
  - State
  - Local
  - Tribal
  - Allied Partners
- With External Organizations (G2B)
  - Industry
  - Financial Institutions
  - Healthcare Providers
- With the American People (G2C)
  - Taxpayers
  - Grant Recipients
  - Medicare/Medicaid Beneficiaries

Credential Types
- PIV Credentials
- PIV-Interoperable Credentials
- Open Solutions
  - OpenID
  - iCard
  - SAML
  - WSFed
  - Etc.

4 Levels of Identity Assurance
(No confidence through full confidence)
- Persons
- Non-Persons

Logical Access
Physical Access
Need to Defy Gravity

Scale

Privacy
Security
Interop
Trust
Id&AM Frameworks Need to Evolve

- Cross Sector Information Sharing
- Regulatory Requirements
- Specialization
- Mobile
- Population Mobility
- New Business Models
- Partnerships
- Outsourcing
- Virtualization
- Cloud
- Economic
- Services

NEED TO SHARE
Past, Present, and Future

Legacy
Application

State of Practice
Enterprise

State of Technology
Federation

State of Need
Ecosystem

Application
Organization
Community of Interest
Cross Sector Marketplace

Application Specific
VPN, Virtual Directories, etc.
PKI, SAML, Trust Frameworks, etc.
Trustmark Framework

Access Control Lists
Role Based Access Control
Attribute Based Access Control
Policy Based Access Control

Scale and Governance
Enabling Technology
Authorization
In the Beginning...

Lots of **Application-Specific** Identity Silos

Application A  Application B  Application C  Application D  Application E
Along Came Federated Identity…

Decouple Identities from Applications!

Identity Provider

Attribute Provider

Standard Protocols

Application (Service Provider)

User

So what about **Trust, Liability, Security?**
And Today…

Lots of **Federated** Identity Silos

- Trust Framework X
- Info Sharing Environment Y
- Federation Z
- Community of Interest ABC
- Other Federation
There exist many Trust Frameworks. Each Trust Framework requires agreement across many dimensions. Many Trust Frameworks are monolithic and opaque.
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.
Challenges with “Inter-federation”

1. No two TFs are the same, so mapping trust and interop requirements between them is hard. Think protocols, attributes, policies, etc.

2. TFs are moving targets, which further complicates the mapping process.

3. Transitive trust is diluted trust, so inter-federation trust cannot be as strong as intra-federation trust.

4. Contractual obligations usually cannot be transferred or assigned to 3rd parties, which makes inter-federation legal agreements difficult or impossible to execute.

(Many other issues exist.)
The Perspective from the LE Community

- Law Enforcement COI has over 1 million people in the US alone
- Over 10,000 US LE agencies
- Required to share data across jurisdictions
- LE agencies are autonomous (NOT centrally funded)
- But must obey applicable access controls when sharing
- 3rd party trust is required due to COI size and complexity
- Trust between agencies is a fundamental requirement
- Legitimate business need to interact with many other COIs
- Most users must have high-assurance credentials
- LE agencies are highly heterogeneous

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

Global Justice Information Sharing Initiative

Global Federated Identity and Privilege Management
Sponsored by the U.S. Department of Justice and the U.S. Department of Homeland Security
The Perspective from the LE Community
Many Other Relevant Initiatives

**FICAM – Federal Identity, Credential, and Access Management**
- NIEF Technical specs and policies are aligned with FICAM
- NIEF has submitted formal application to be approved as a FICAM Trust Framework Provider @ LOA 2 and non-PKI LOA 3

**SICAM – State Identity, Credential, and Access Management**
- SICAM currently only provides high-level guidance
- Leverages FICAM and FICAM TFP initiatives
- NIEF working with NASCIO to further mature SICAM through NIEF Quick Start program and NIEF NSTIC pilots

**BAE – Backend Attribute Exchange**
- NIEF one of first operational BAE pilots in partnership with GSA, PM-ISE, TX DPS, RISS, IIR
- NIEF has adopted BAE profile for Attribute Providers

**PIV/PIV-I – Personal Identity Verification**
- Under the sponsorship of DHS S&T and in partnership with JHAPL, GTRI developed a proof of concept Gateway between the PIV-I community and NIEF.
- Also Leverages the BAE to collect additional attributes not on the PIV-I card

**NSTIC – National Strategy for Trusted Identities in Cyberspace**
- NIEF selected by NIST to be a NSTIC pilot to demonstrate *Scalable Trust and Interoperability through a Trustmark Marketplace*
- Scope is broader than FICAM but leverages FICAM
Where to from here?
Is it OK if the Trust Frameworks in the ID Ecosystem are mostly non-interoperable and non-trusting identity silos?
Or is there 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...

ID Trust Framework A
- FICAM
- SAML
- SSO

ID Trust Framework B
- NIST 800-63
- LOA 3

ID Trust Framework C
- OAuth
- OpenID
- FIPS 200

...then we get:

Greater **transparency** of trust framework requirements

Greater **ease of comparability** between frameworks

Greater **potential for reusability** of framework components

And, most importantly:

Greater **potential for participation in multiple trust frameworks** by ID Ecosystem members with incremental effort and cost
What about a Trustmark Framework?

These modular components are called Trustmarks.
Scope 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)

MACHINE READABLE

Technical
Trust
Privacy
Security
Business

Legal

Trustmark Policies & Trustmark Agreements
A Trustmark-Based ID Ecosystem

Rather than requiring a monolithic, formalized Trust Framework...

...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. Trustmarks can be acquired through a Trustmark Provider. 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.
Trustmarks can be stored in a searchable Trustmark Registry. Members of the ID Ecosystem can query the 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.
What is a trustmark framework?

- **Stakeholder Community**
  - Is Represented By: Trustmark Defining Organization

- **Trustmark Defining Organization**
  - Defines: Trustmark Definition

- **Trustmark Definition**
  - Is Required By: Trustmark Provider, Trustmark Recipient, Org. 1, Org. 2, End User

- **Trustmark Provider**
  - Issues: Trust Interop Profile
    - Trustmark A
    - Trustmark B
    - Trustmark C

- **Trustmark Recipient**
  - Is Used By: Trustmark Provider
  - Is Trusted By: Org. 1

- **Org. 1**
  - Is Required By: Trustmark Provider
  - Is Trusted By: Trustmark Recipient

- **Org. 2**
  - Is Required By: Trustmark Provider

- **End User**
  - Is Required By: Trustmark Provider
<table>
<thead>
<tr>
<th>Trustmark Framework Concept</th>
<th>Analogous Concept from PKI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustmark</td>
<td>Certificate</td>
</tr>
<tr>
<td>Trustmark Provider</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>Trustmark Recipient</td>
<td>Subscriber</td>
</tr>
<tr>
<td>Trustmark Relying Party</td>
<td>Certificate Relying Party / Audience</td>
</tr>
<tr>
<td>Trustmark Policy</td>
<td>Certificate Policy</td>
</tr>
<tr>
<td>Trustmark Agreement</td>
<td>Subscriber Agreement</td>
</tr>
<tr>
<td>Trustmark Defining Organization</td>
<td>ITU (Agency that defined X.509)</td>
</tr>
<tr>
<td>Trustmark Definition</td>
<td>IETF RFC 5280 (X.509 Spec)</td>
</tr>
<tr>
<td>Trust Interoperability Profile</td>
<td>List of Trusted Certificate Authorities</td>
</tr>
</tbody>
</table>
The Trustmark Framework in More Detail

Trustmark Spec

Trustmark Definition Spec

Trust Interoperability Profile Spec

Trustmark Instance

Trustmark Definition Instance

Is used by...

Defines basic structure of...

Conforms to...

Defines extensions to...

Defines structure of...

Conforms to...

Defines structure of...

Conforms to...

Defines structure of...

Conforms to...

 Defines assessment criteria for...
Trustmark Definitions

Conformance Criteria:
Conformance to the Identity Provider Organization (IDPO) conformance target of this TD requires the following.

1. The IDPO MUST ...
2. The IDPO MUST ...
3. The IDPO MAY ...
4. ...

Assessment Process:
Before issuing a trustmark subject to this TD, a Trustmark Provider MUST complete the following assessment steps.

1. The TP MUST ...
2. The TP MUST ...
3. The TP MUST ...

Trustmark Extension Schema:
Trustmarks issued subject to this TD MUST conform to the Trustmark Base Schema, and MUST also conform to the following Trustmark Extension Schema.

Metadata:
- Publisher: U.S. General Services Administration
- Name: NIST/FICAM LOA 2 IDPO TD
- URL: <URL>
- Description and Intended Purpose: ...
- Target Stakeholder Audience: ...
- Date of Publication: 15 Apr 2014
- Version: 1.0
- Visual Icon: 🌐

Certification as a Trustmark Provider:
Before an entity may issue trustmarks subject to this TD, it MUST complete the following certification process.

1. The entity MUST ...
2. The entity MUST ...
3. The entity MUST ...
Trust and Interoperability Criteria:

Identity Provider Organization (IDPO) Trustmark Requirements:

<table>
<thead>
<tr>
<th>Trustmark</th>
<th>Requirement</th>
<th>Approved Trustmark Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>FICAM SAML SSO IDP</td>
<td>MUST HAVE</td>
<td>NIEF</td>
</tr>
<tr>
<td>NIEF/FICAM LOA 2 IDPO</td>
<td>MUST HAVE</td>
<td>NIEF or Deloitte</td>
</tr>
<tr>
<td>NIEF Attribute Profile IDPO</td>
<td>MUST HAVE</td>
<td>(ANY)</td>
</tr>
<tr>
<td>XYZ Privacy Policy IDPO</td>
<td>SHOULD HAVE</td>
<td>(ANY)</td>
</tr>
</tbody>
</table>

Service Provider Organization (SPO) Trustmark Requirements:

<table>
<thead>
<tr>
<th>Trustmark</th>
<th>Requirement</th>
<th>Approved Trustmark Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>FICAM SAML SSO SP</td>
<td>MUST HAVE</td>
<td>NIEF</td>
</tr>
<tr>
<td>NIEF Attribute Profile SPO</td>
<td>MUST HAVE</td>
<td>(ANY)</td>
</tr>
<tr>
<td>XYZ Privacy Policy SPO</td>
<td>MUST HAVE</td>
<td>(ANY)</td>
</tr>
</tbody>
</table>

Metadata:

- **Publisher**: U.S. Dept. of Justice
- **URL**: <URL>
- **Name**: U.S. Law Enforcement Community Info Sharing TIP
- **Description and Intended Purpose**: ...
- **Date of Publication**: 15 Jun 2014
- **Version**: 1.0
- **Digital Signature of Issuer**: <SIGNATURE>
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

| A | Trustmark Definition (TD) Name                                      | B | C | D | E | F | G | H | I | J | K | L |
|---|-------------------------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Trustmark Definition (TD) Name                  |   |   |   |   |   |   |   |   |   |   |   |   |
| 2 | FICAM Bona Fides Reqs for IDPs                  | YES| YES| YES|   |   |   |   |   | YES|   | GTRI|   |
| 3 | NIEF Bona Fides Reqs for IDPOs                  | YES| YES|   |   |   |   |   |   | YES|   | GTRI|   |
| 4 | NIEF Bona Fides Reqs for SPOs                   | YES| YES|   |   |   |   |   |   | YES|   | GTRI|   |
| 5 | NIEF Bona Fides Reqs for APOs                   | YES| YES|   |   |   |   |   |   | YES|   | GTRI|   |
| 6 | NIEF Bona Fides Reqs for SCOIs                  | YES| YES|   |   |   |   |   |   | YES|   | GTRI|   |
| 7 | FICAM LOA 1 Security Reqs                      |   |   |   |   |   |   | YES|   |   |   |   |   |
| 8 | FICAM LOA 2 Registration and Issuance Reqs      | YES| YES| YES|   |   |   | YES|   | YES| YES|   |
| 9 | FICAM LOA 2 Authentication Process Reqs         | YES| YES| YES|   |   |   | YES|   | YES| YES|   |
| 10| FICAM LOA 2 Token and Credential Management Reqs| YES| YES| YES|   |   |   | YES|   | YES| YES|   |
| 11| FICAM LOA 2 Tokens Reqs                        | YES| YES| YES|   |   |   | YES|   | YES| YES|   |
| 12| FICAM LOA 2 Assertions Reqs                    | YES| YES| YES|   |   |   | YES|   | YES| YES|   |
| 13| FICAM LOA 3 and LOA 3 Ongoing Verification Reqs|   |   |   |   |   | YES|   | YES| YES|   |   |
| 84| FIPPs Accountability and Auditing Reqs          | YES|   |   |   |   |   |   | YES|   |   |   |
| 85| FIPPs Data Minimization Reqs                    | YES|   |   |   |   |   |   | YES|   |   |   |
| 86| FIPPs Data Quality and Integrity Reqs           | YES|   |   |   |   |   |   | YES|   |   |   |
| 87| FIPPs Individual Participation Reqs             | YES|   |   |   |   |   |   | YES| TDB|   |   |
| 88| FIPPs Purpose Specification Reqs                | YES|   |   |   |   |   |   | YES| TDB|   |   |
| 89| FIPPs Security Reqs                            | YES|   |   |   |   |   |   | YES| TDB|   |   |
| 90| FIPPs Transparency Reqs                        | YES|   |   |   |   |   |   | YES| TDB|   |   |
| 91| FIPPs Use Limitation Reqs                       | YES|   |   |   |   |   |   | YES| TDB|   |   |
| 92| InCommon Research & Scholarship Reqs            | YES|   |   |   |   |   | YES| TDB|   |   | InCommon |
| 93| Children's Online Privacy Protection Act (COPPA) Reqs | YES|   |   |   |   | YES| TDB|   |   |   | PRIVO |
| 94| Knowledge-Based Authentication (KBA) Reqs        | YES|   |   |   |   | YES| TDB|   |   |   |   |
| 95| Accessibility Reqs                              | YES|   |   |   |   | YES| TDB|   |   |   |   |
| 96|                                                |   |   |   |   |   |   |   |   |   |   |   |
| 97| **TOTALS**                                      | 50| 71| 39| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

- **94 distinct trustmarks identified (so far)**
- **Covers FICAM, NIEF, and Other NSTIC Pilots**
- **Also covers FIPPs (privacy) topics**
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
NIEF Moving Forward

Legacy
- Application

State of Practice
- Enterprise

State of Technology
- Federation
- NIEF
- Ecosystem

State of Need
- NIEF
- Ecosystem

Scale and Governance
- Authorization

Enabling Technology
- Authentication
- Authorization

Application
- Application
- Specific

Organization
- VPN, Virtual Directories, etc.
- PKI, SAML, OpenID, etc.

Community of Interest
- Policy Based Access Control

Cross Sector Marketplace
- Trustmark Framework

Access Control Lists
- Attribute Based Access Control

Role Based Access Control
- Policy Based Access Control
The NIEF QuickStart Program

Drive broader adoption and implementation of GFIPM, FICAM, and NIEF standards among state agencies.

Streamline the onboarding process to lower cost and barriers to adoption.

Demonstrate the NIEF Trustmark Framework as a viable approach to cross sector interoperable security, privacy, and trust.

NASCIO to Partner with Georgia Tech Research Institute on NIEF QuickStart Program

FOR IMMEDIATE RELEASE

NASCIO to Partner with Georgia Tech Research Institute on NIEF QuickStart Program

LEXINGTON, Ky., Tuesday, October 22, 2013 — Building on the adoption of the National Identity Exchange Federation (NIEF), the National Association of State Chief Information Officers (NASCIO) has partnered with the Georgia Tech Research Institute (GTRI) to pilot the NIEF QuickStart Program in multiple states to provide data exchange among law enforcement, public safety, and emergency management agencies.

The goal of the pilot is to provide a standardized, domain-agnostic capability to trusted identity and attribute sharing. NASCIO member agencies can leverage this capability to achieve identity reuse, single sign-on (SSO), and policy compliant control access to the broadest set of public safety-related information across all levels of government. The program promises to deliver a marked improvement in the efficiency and automation of policy-based access control decisions on information resources. The underlying goal is to strategically jump-start key states’ information exchange capabilities, improve awareness of NIEF’s strategic vision, and drive an increased value proposition for all NIEF participants.

“States have struggled to develop identity trust frameworks, but the NIEF QuickStart Program will demonstrate the value proposition of a robust framework,” stated NASCIO Executive Director, Doug Peterson. “The value of any federation or information sharing environment increases with the number of participants, and the pilot participants will be seeds that will grow.”

GTRI will assist selected participants by facilitating and shepherding them through NIEF’s formal on-boarding process. It is expected that the selected on-boarding projects will be completed in approximately twelve (12) months.

“Over time, the NIEF QuickStart Program will create a way for state, local, tribal, and territorial governments to create an affordable, fast and repeatable process for on-boarding into a common trusted environment for identity and attribute exchange,” said John Wambolt, who is a GTRI Research Engineer in the Cybersecurity and Intelligence Division at Georgia Tech. “By the end of the project, all of the states will be able to see the proof of concept, and the pilot will demonstrate the practicality of rapid NIEF on-boarding for partners of any size.”

It is expected that the NIEF QuickStart Program will eventually grow to accommodate and facilitate adoption of agencies at all levels of government, but the pilot phase of the program is targeted primarily towards U.S. state and state-level agencies. NASCIO and GTRI seek to quickly engage with interested states and begin executing on the selection process. States interested in submitting a readiness assessment profile for the NIEF QuickStart Program can go to www.nief.org and submit an assessment profile online. For more details on NIEF, please visit https://www.gtrinst.org.

About NASCIO

The National Association of State Chief Information Officers is the premier network and resource for state CIOs and a leading advocate for technology policy at all levels of government. NASCIO represents state chief information officers and information technology executives from the states, territories, and the District of Columbia. The primary state government members are senior officials who have executive level and statewide responsibility for information technology leadership. State officials who are involved in agency level information technology management may participate as state members. Representatives from other public sector and non-profit organizations may also participate as associate members. For more information about NASCIO visit www.nascio.org.

About GTRI

The Georgia Tech Research Institute (GTRI) is a highly regarded applied research and development organization that is part of the Georgia Institute of Technology, one of the world’s top research universities. With more than 1,700 scientists, engineers and other professionals, GTRI helps solve some of the most difficult problems facing government and industry across the nation and around the world. For more information on GTRI visit www.gtrinst.org.

Media Contact

For immediate release from GTRI

Doug Peterson, GTRI
(404) 385-4608
doug.petersen@gtrinst.org
Learn More Here

https://trustmark.gtri.gatech.edu

Welcome!

Welcome to the project website for the GTRI NSTIC Trustmark Pilot!

In early 2013, GTRI submitted a proposal to NIST in response to the 2013 NSTIC Pilots Cooperative Agreement Program. In our proposal, we claimed that "the trust and interoperability scaling problem is the single most significant barrier to the wide adoption of an Identity Ecosystem", and our proposal described a concept called a Trustmark Framework, which we believe may help to overcome this barrier. Since being selected by the NSTIC NPO as a grant recipient by NIST in September 2013, we have begun to develop this concept from idea into reality.

This website serves as the public face of our pilot. Please take the time to look around and get familiar with our work. Also, please subscribe to our blog via RSS for occasional updates.

Note that this website is undergoing continual updates and improvements, so some pages may not yet be complete. Much of the content on this site will evolve over time as we execute the pilot and report
Some NIEF Members

Texas Department of Public Safety
TXMAP Web Mapping Application

What is it?
The TXMAP application is a multi-faceted data mapping and reporting tool created by the Texas Department of Public Safety. TXMAP provides users access to a variety of data ranging from state critical infrastructure and regional information sharing systems (RISS) to the CargoNet - The Cargo Theft Prevention and Recovery Network.

Regional Information Sharing Systems (RISS)

The RISS Program is funded by Congress and administered by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice (OJP). The RISS Program provides secure access to services and resources to more than 6000 federal, state, local, and tribal law enforcement agencies as well as public safety and critical infrastructure/key resources (CI/KR) communities. In addition, RISS participation in NIEF allows RISS providers different levels of authorization to NIFL users based upon their roles.

- RISS Resources available to all federal partners
- RISS AXX - Website - RISS TechPage - RISSU
- Most resources available to state and local law enforcement agencies/units and those acting for the RISS.
- Texas National Data Program (TNDP) - Related to the NDI Statewide Criminal Information System (NCIC) - National Crime Information System (NCIC).
- Texas Jailer System - National Criminal Intelligence Center (NCIC) - National Law Enforcement Training Center (NLETC) - Electronic Learning Portal (ELP).

CargoNet

What is it?
CargoNet provides a multi-layered solution to the cargo theft problem. CargoNet helps prevent cargo theft and increases recovery rates by facilitating secure information sharing among truckers, their business partners, and law enforcement. CargoNet offers 24/7 access to data.

Apiary

What is Apairy?
Apairy is an automated framework for malware analysis and threat intelligence. Members of our extended community anonymously upload malware samples from the ongoing position of in-depth malware correlation and behavior analysis. The results are delivered automatically within a secure data analysis process for analysts. Apairy protects our organization.

Who uses Apairy?
Apairy is currently being used in both the private and public sector. The community includes organizations from many industries including finance, oil and gas, utilities, retail, and more. Additionally, Apairy is used by local, state, and federal government organizations including law enforcement and education.

LA County Criminal History

Target Audience - Law Enforcement, Probation and Parole

LCCHR is the LA County Criminal History System used by investigators and prosecutors for filing criminal cases within LA County. It contains over 12,800,000 subjects with records of arrests, convictions, sentences, custody status, probation status, demographics and biometric identifiers. Over 44 local police agencies, LA Sheriff, LA District Attorney and LA Probation utilize LCCHR for their daily operations with 10,000 transactions per day.

Status - Available Now (CCHR IC)

Sponsoring Agency - LA County Sheriff

Contact: Kellie Embron at 3102-463-8899 or kbourne@ladj.security.org

Georgia Tech Research Institute
High-Level Project Plan & Timeline

Q4 2013
- Develop Concept

Q1 2014
- Refine Concept as Needed

Q2 2014
- Develop Trustmark Framework
  - Refine Framework as Needed
  - Develop Sample TDs, Trustmarks, and TIPs
  - Refine TDs, Trustmarks, and TIPs as Needed

Q3 2014
- Develop and Refine Sample Trustmark Software Tools

Q4 2014
- Develop SICAM Use Cases & Scenarios
  - Refine Use Cases & Scenarios

Q1 2015
- Trustmark Pilot in NIEF

Q2 2015
- Outreach/Prep for Expanded Pilot
  - Expanded Trustmark Pilot

Q3 2015
- Community Outreach
- Project Oversight & Reporting
- SICAM Demo