Georgia Tech Research Institute

Problem. Solved.

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

Georgia Tech Research Institute

NASCIO
Representing Chief Information Officers of the States

In the Beginning…

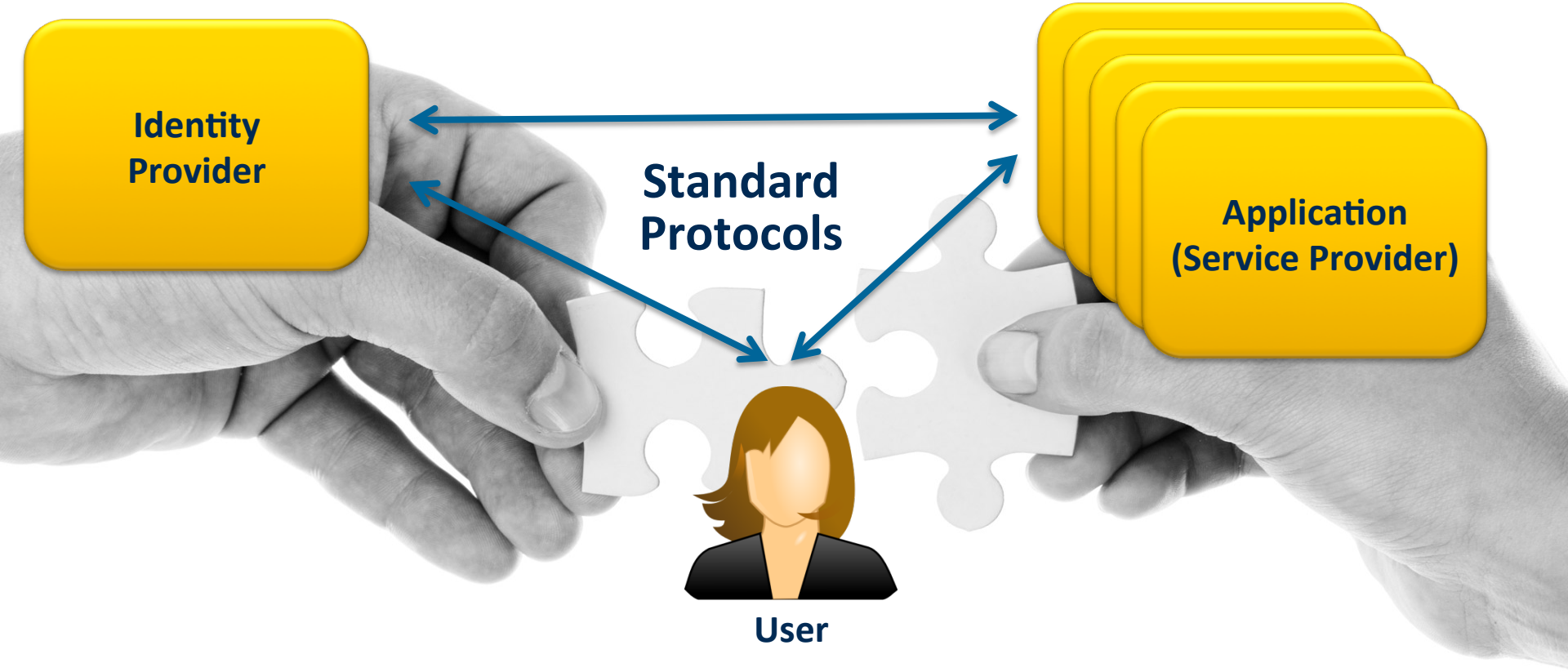
Georgia Tech Research Institute

Lots of Application-Specific Identity Silos

Along Came Federated Identity…

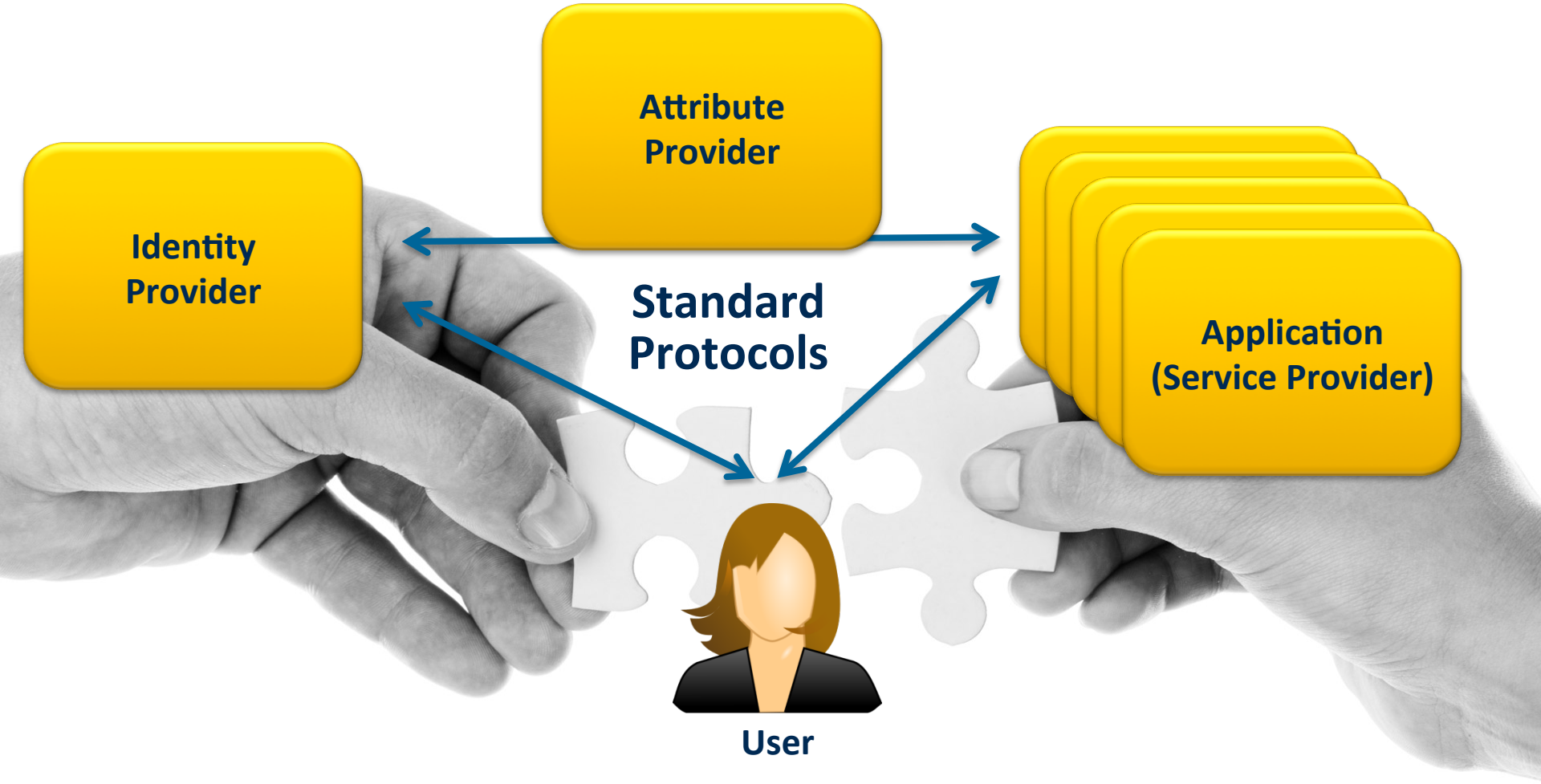
Georgia Tech Research Institute

Decouple Identities from Applications!



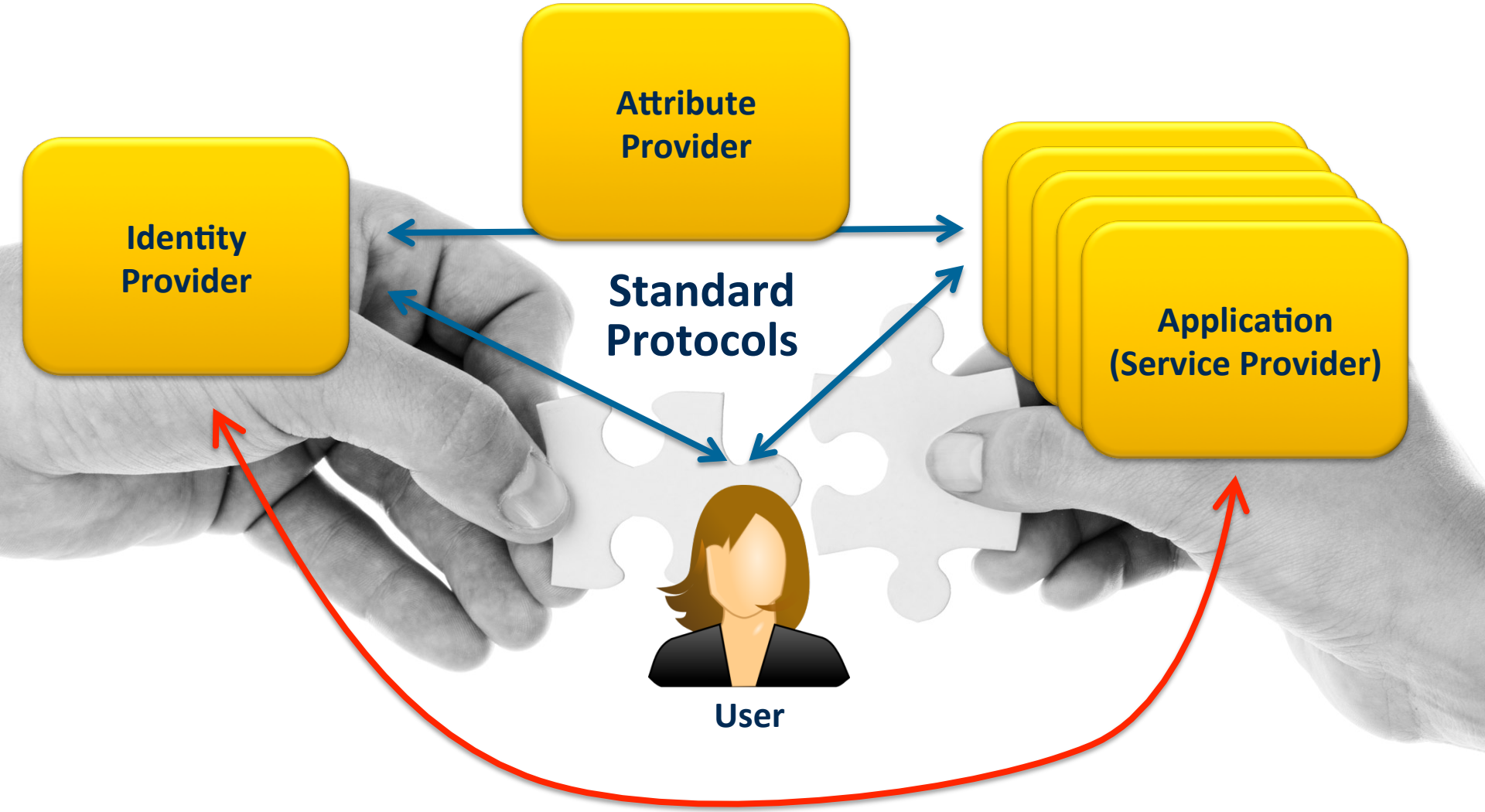
Along Came Federated Identity…

Georgia Tech Research Institute



Along Came Federated Identity…

Georgia Tech Research Institute



So what about Trust, Liability, Security?

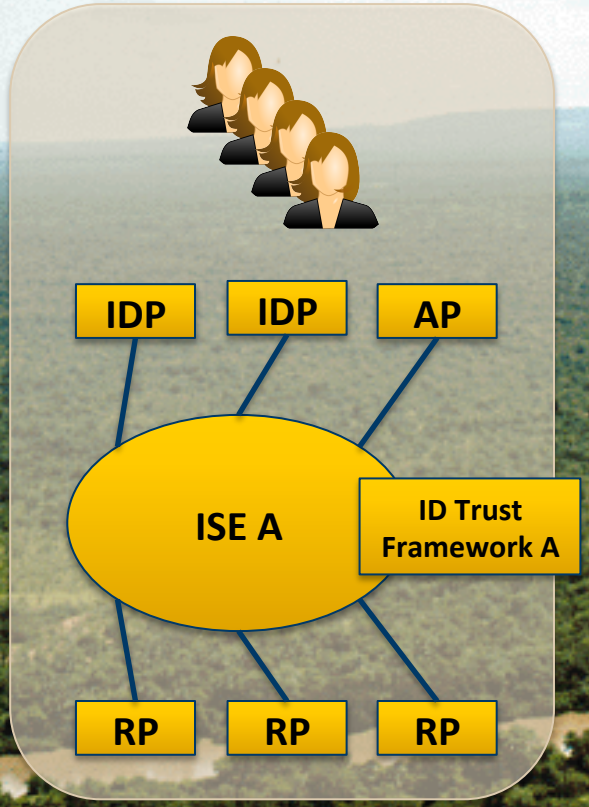
And Today…

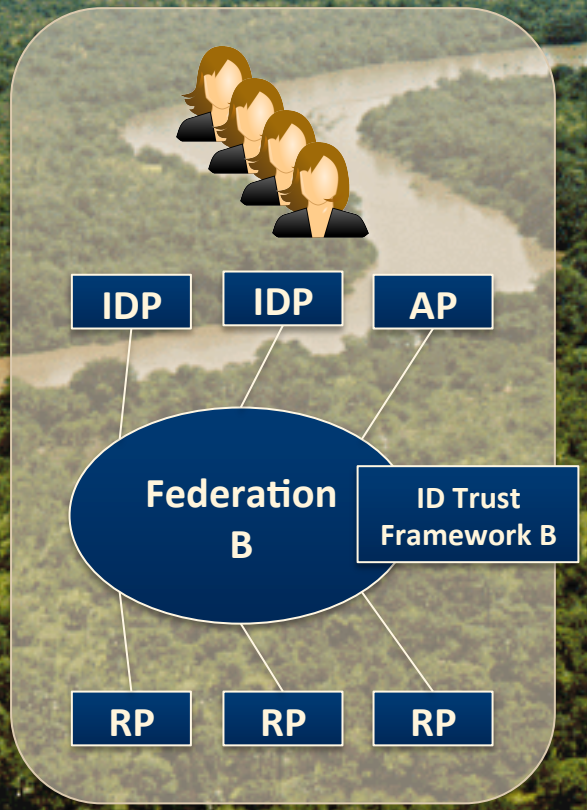
Georgia Tech Research Institute

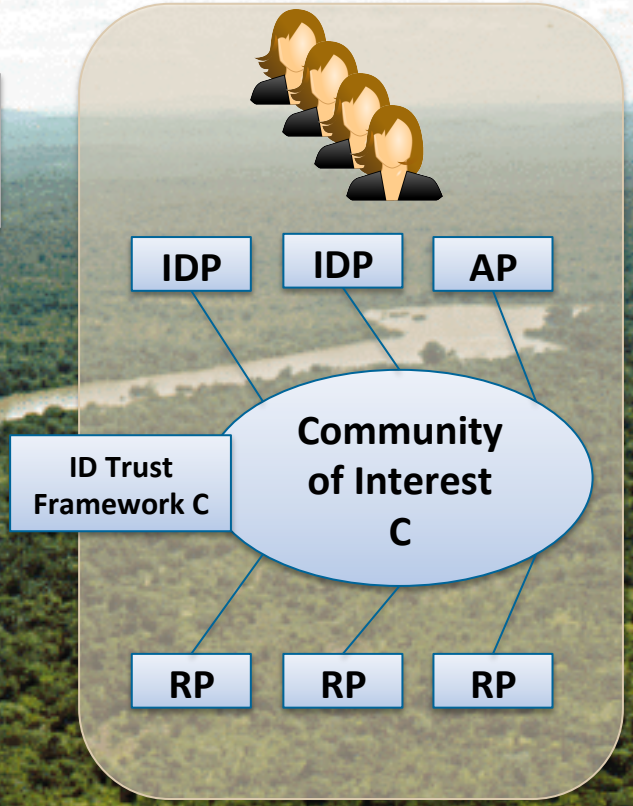
Current State of the Identity Ecosystem

Georgia Tech Research Institute

There exist many **Trust Frameworks**.



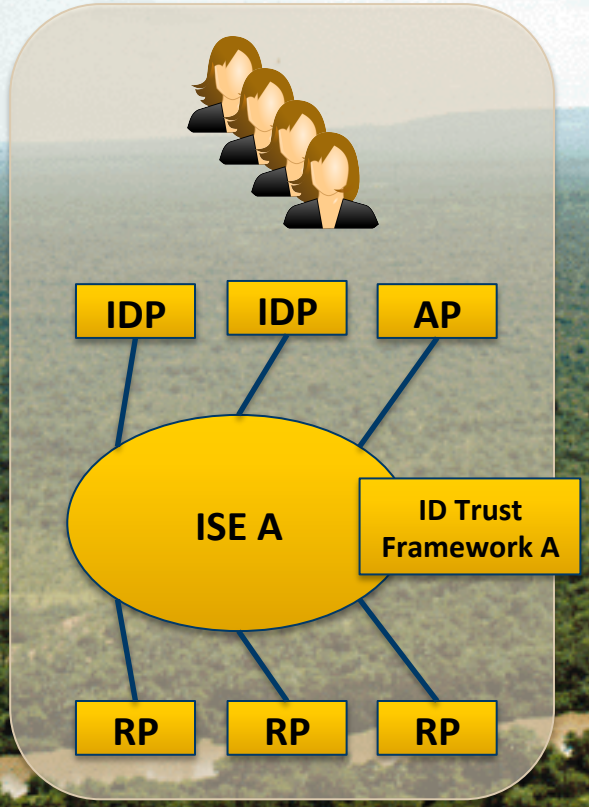


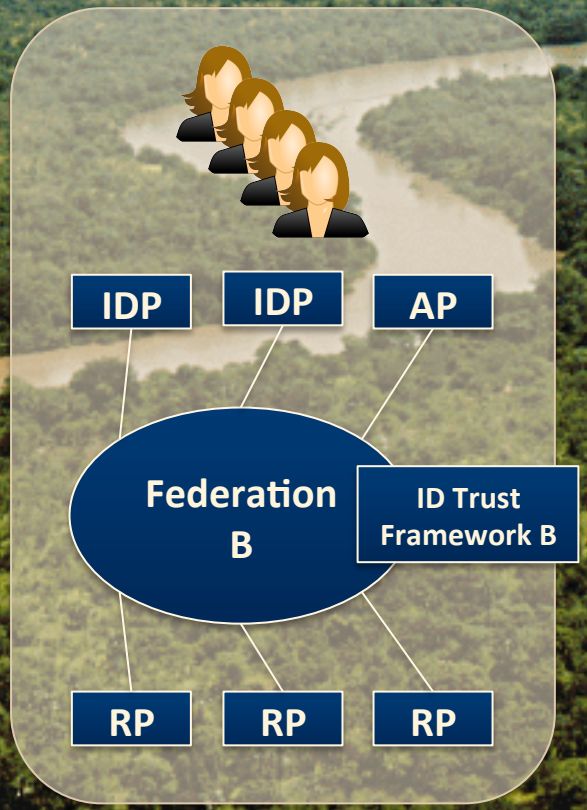


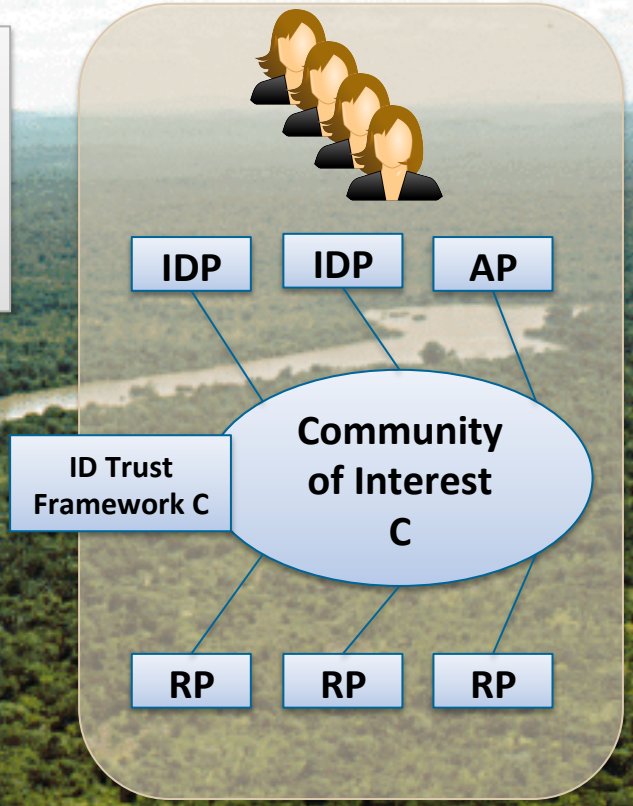
Current State of the Identity Ecosystem

Georgia Tech Research Institute

Each Trust Framework requires agreement across many dimensions.



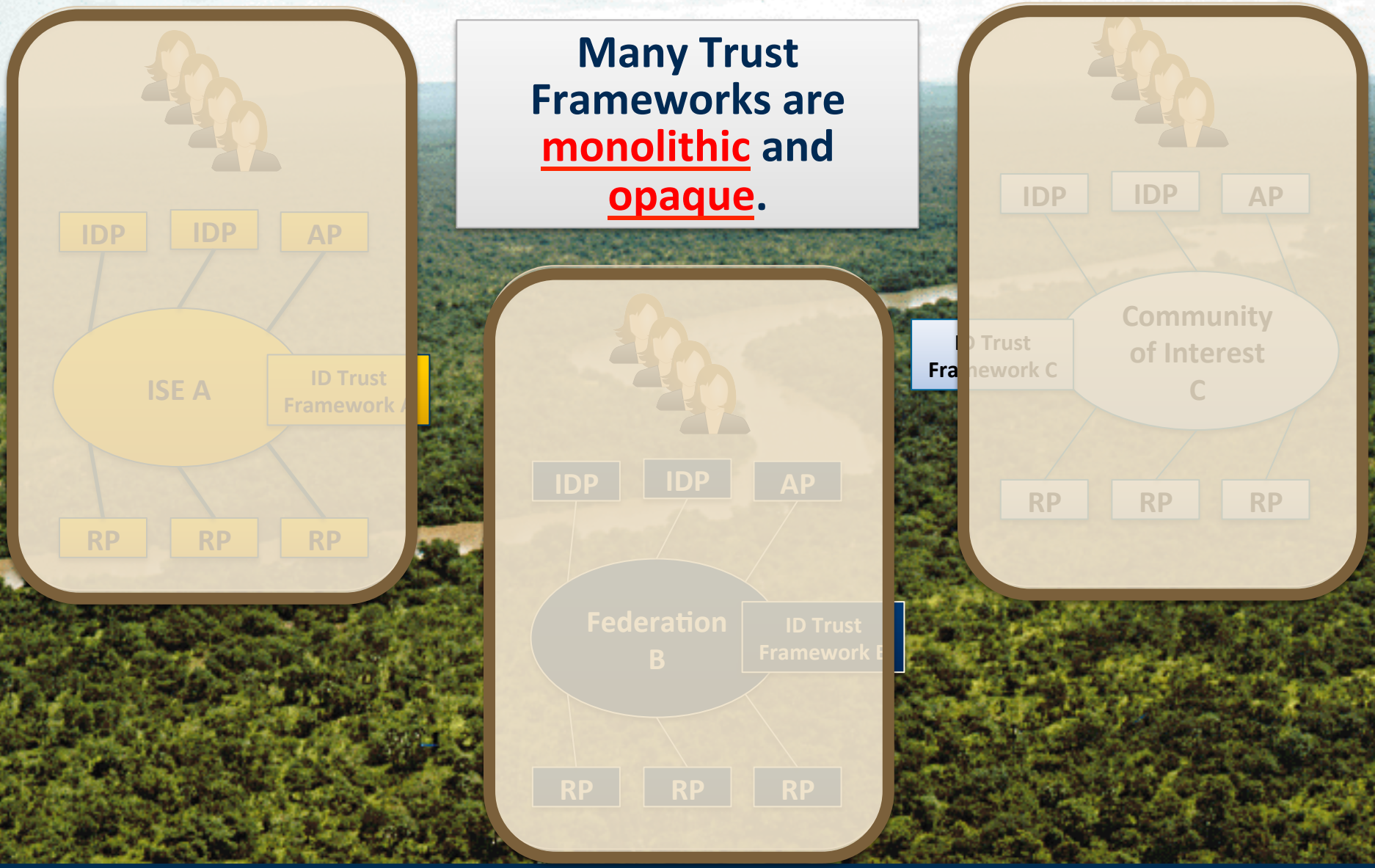




Current State of the Identity Ecosystem

Georgia Tech Research Institute

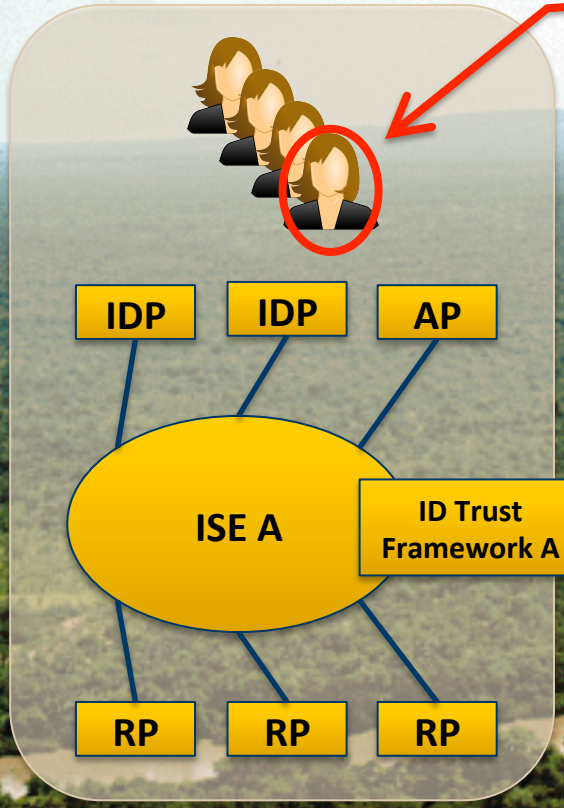
Many Trust Frameworks are monolithic and opaque.

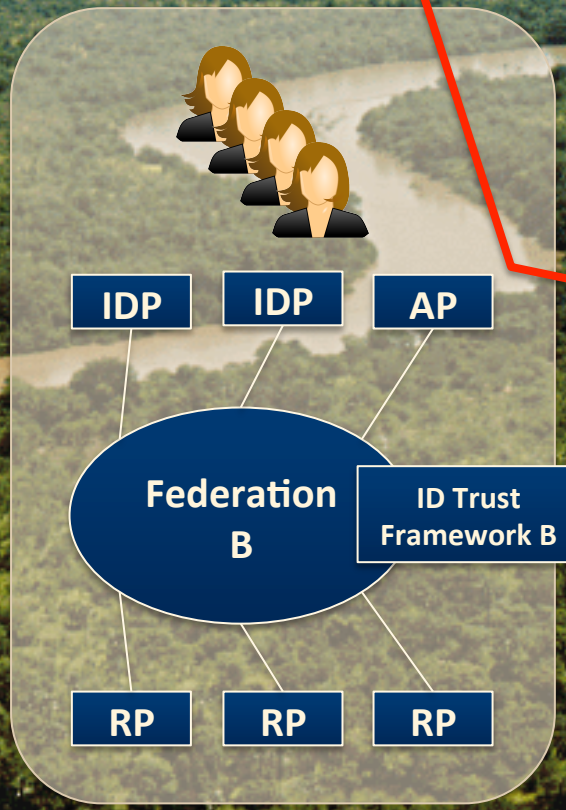


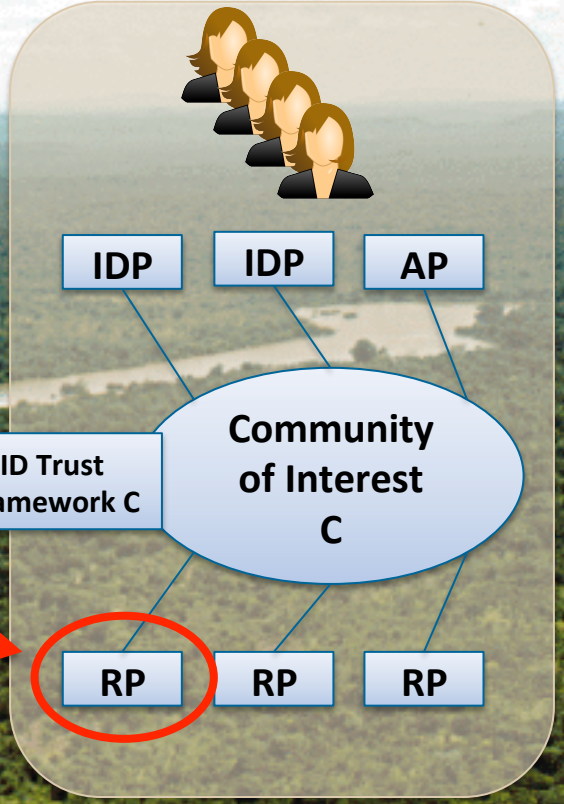
Achieving Cross-Framework Trust

Georgia Tech Research Institute

Suppose this user needs access to this RP.





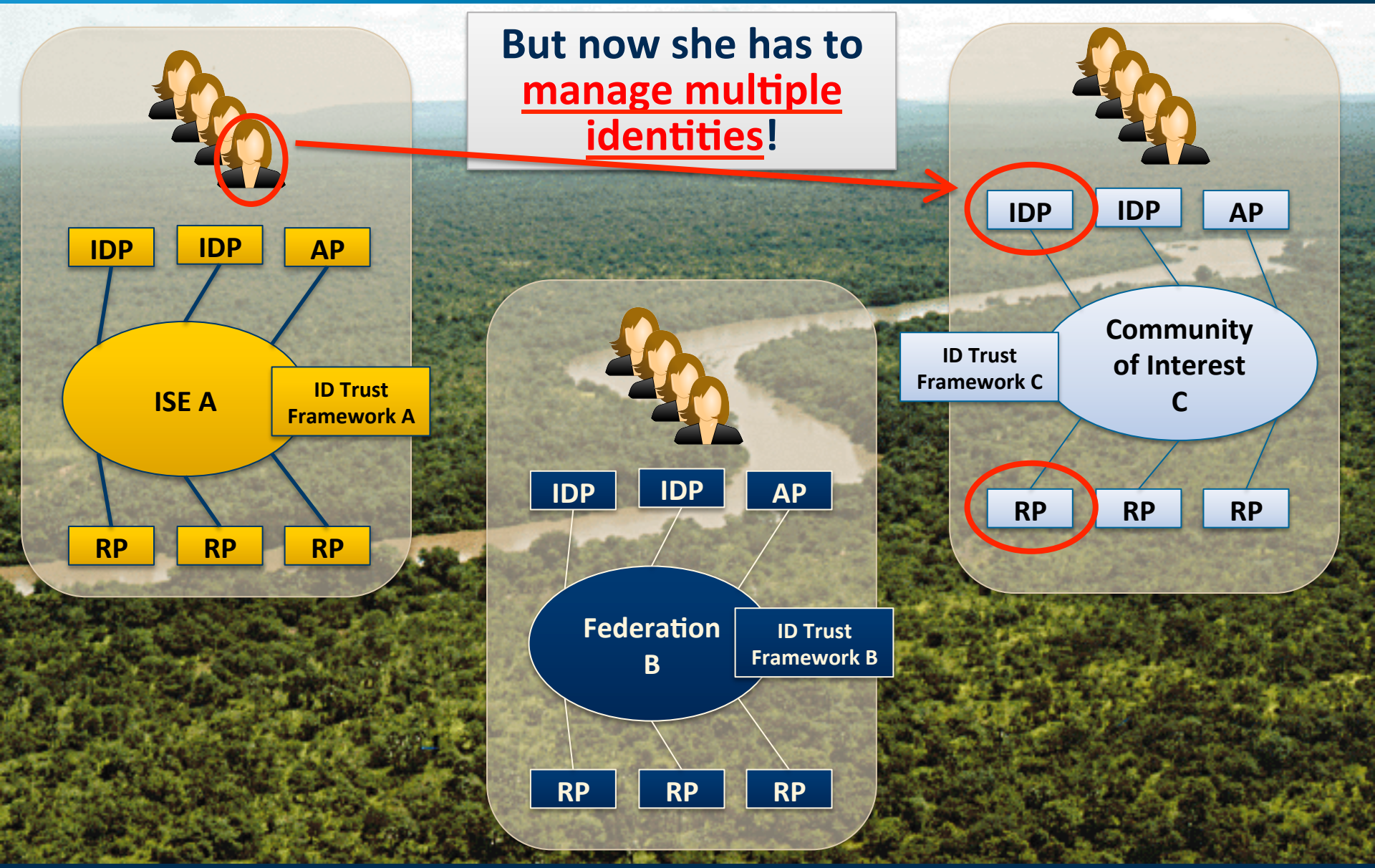


In today's ID Ecosystem, there are at least five ways to do it…

…and all of them face challenges.

Option #1: User Creates a New Identity

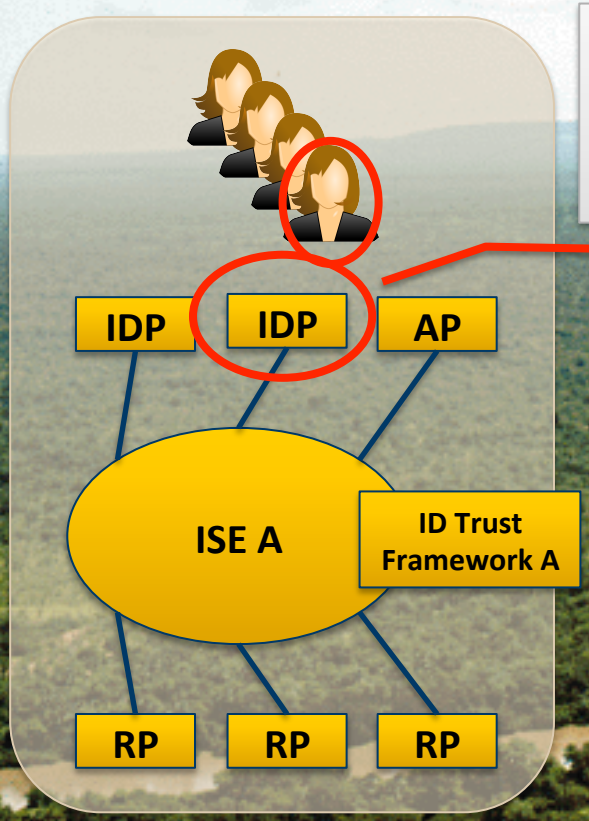
Georgia Tech Research Institute

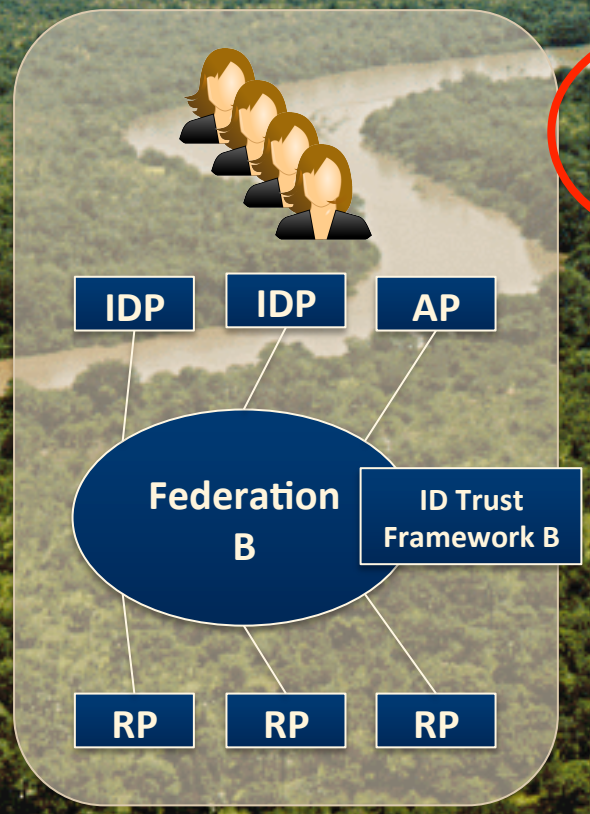


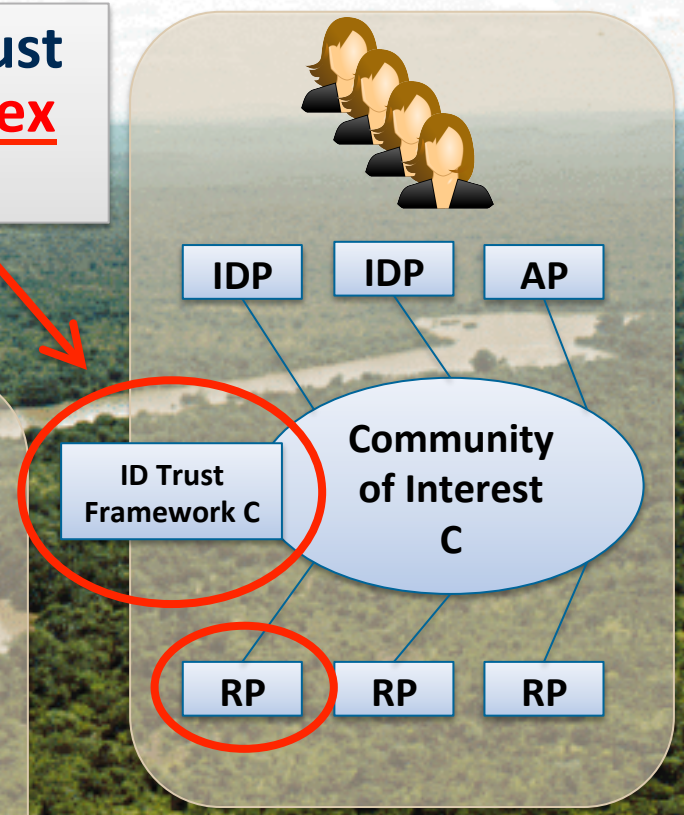
Option #2: IDP Joins New Trust Framework

Georgia Tech Research Institute

But joining a new Trust Framework is complex and expensive!



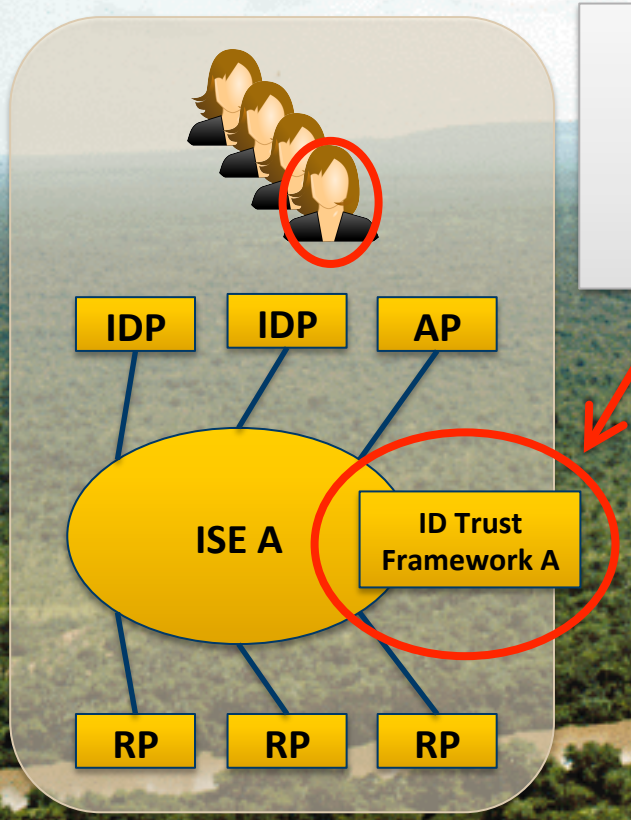


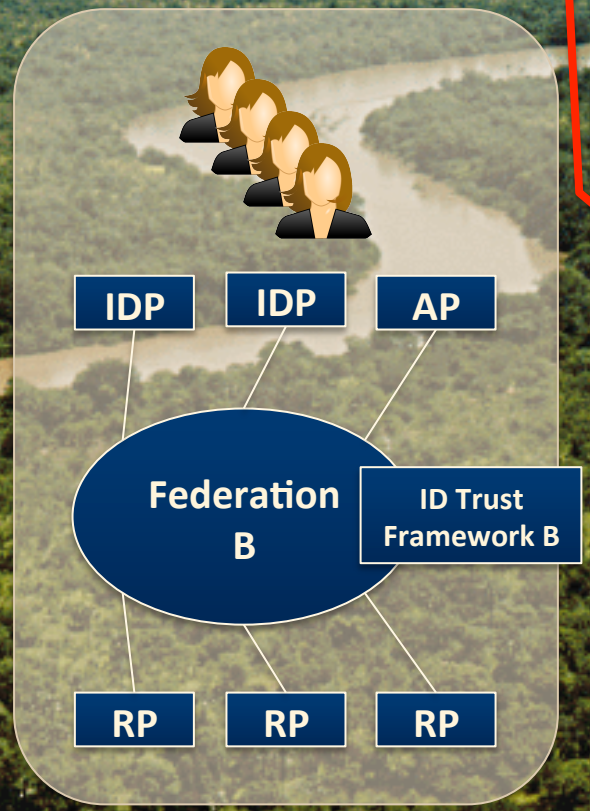


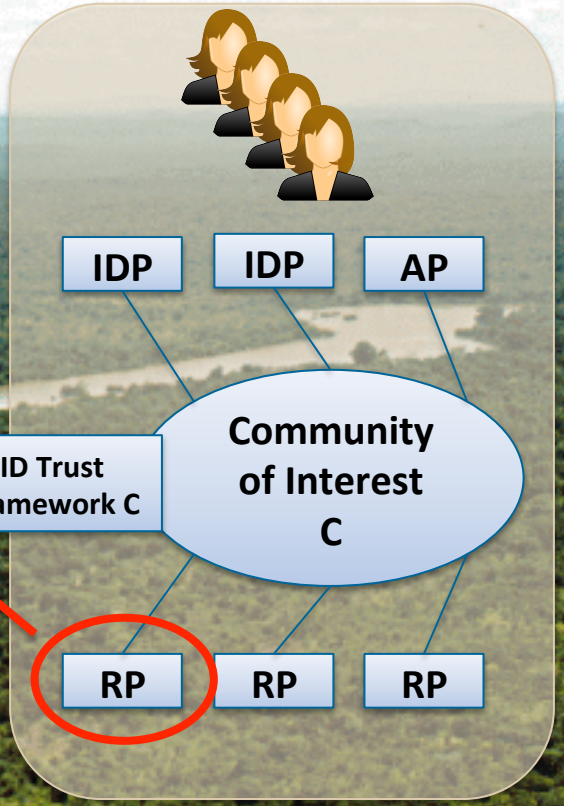
Option #3: RP Joins New Trust Framework

Georgia Tech Research Institute

Same problem here: Joining a new Trust Framework is complex and expensive!



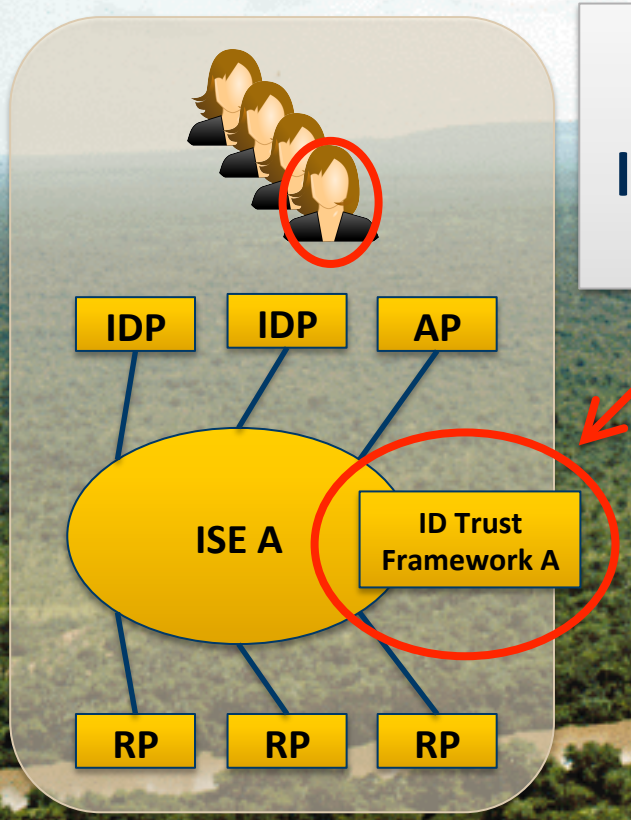


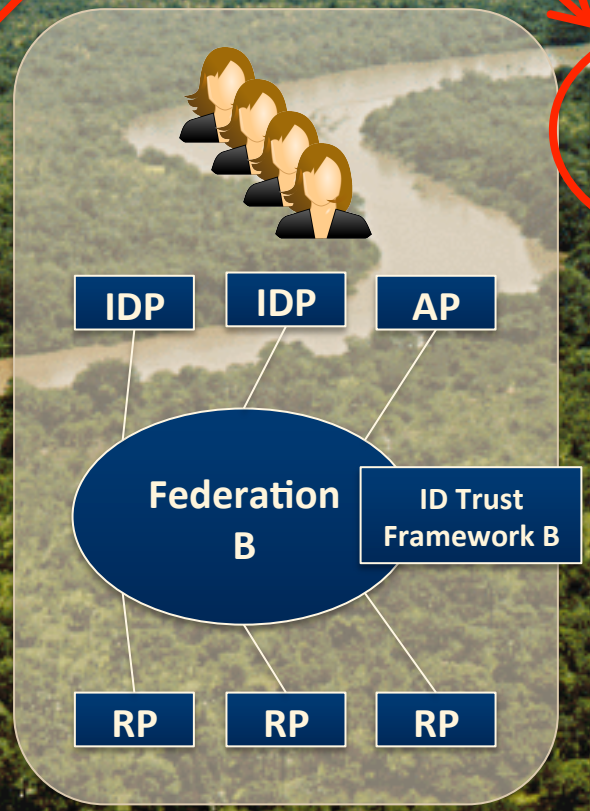


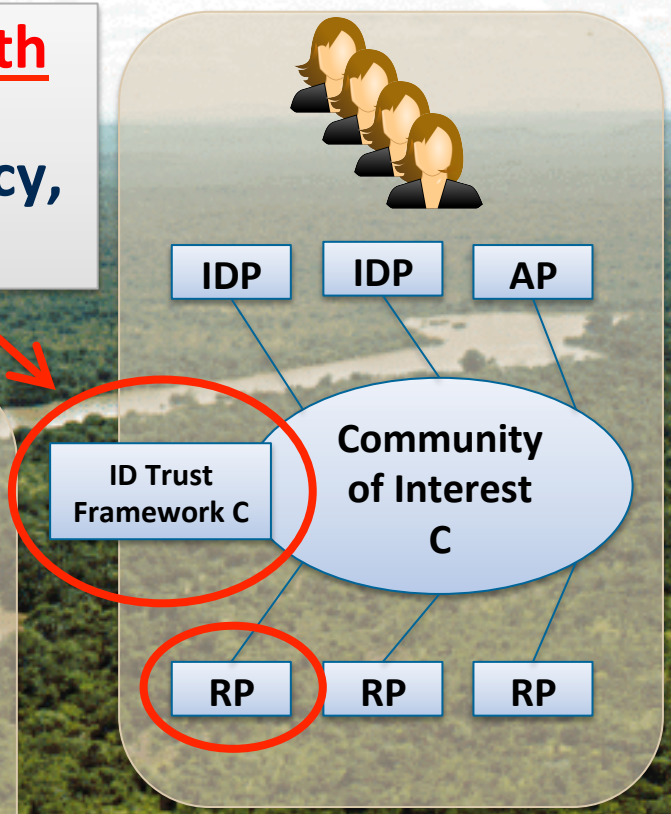
Option #4: Cross-Framework Relationship

Georgia Tech Research Institute

But this is fraught with challenges at many layers: technical, policy, legal, etc.



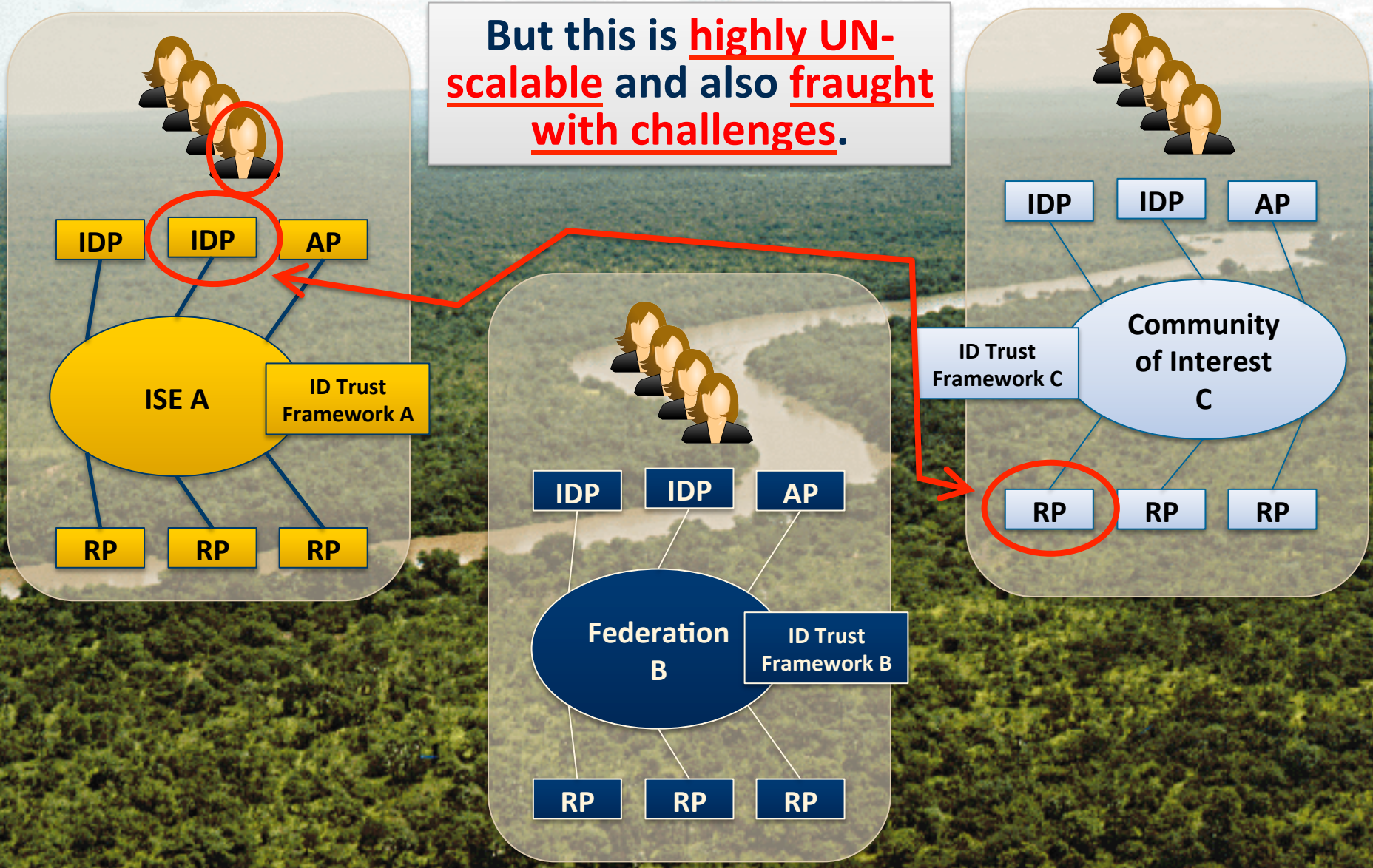




Option #5: Bilateral IDP-RP Relationship

Georgia Tech Research Institute

But this is highly UN-scalable and also fraught with challenges.



The Perspective from the LE Community

Georgia Tech Research Institute

Law Enforcement COI has over 1 million people in the US alone

Over 10,000 US LE agencies

Required to share data across jurisdictions

But must obey applicable access controls when sharing

LE agencies are autonomous (NOT centrally funded)

Trust between agencies is a fundamental requirement

3rd party trust is required due to COI size and complexity

Most users must have high-assurance credentials

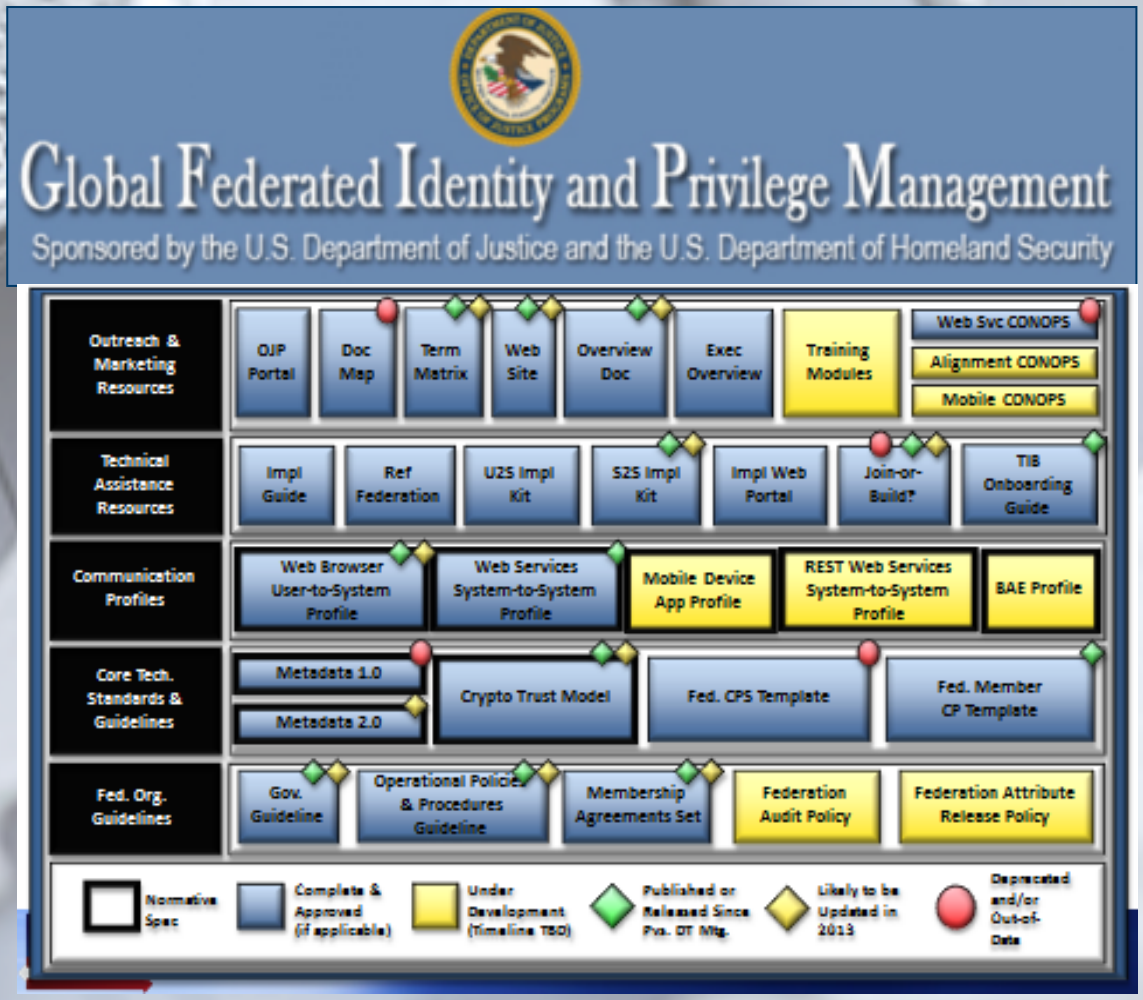
Legitimate business need to interact with many other COIs

LE agencies are highly heterogeneous

- Federal Agencies
- State Agencies
- Local Agencies
- Tribal Agencies
- Task Forces
- Fusion Centers

The Perspective from the LE Community

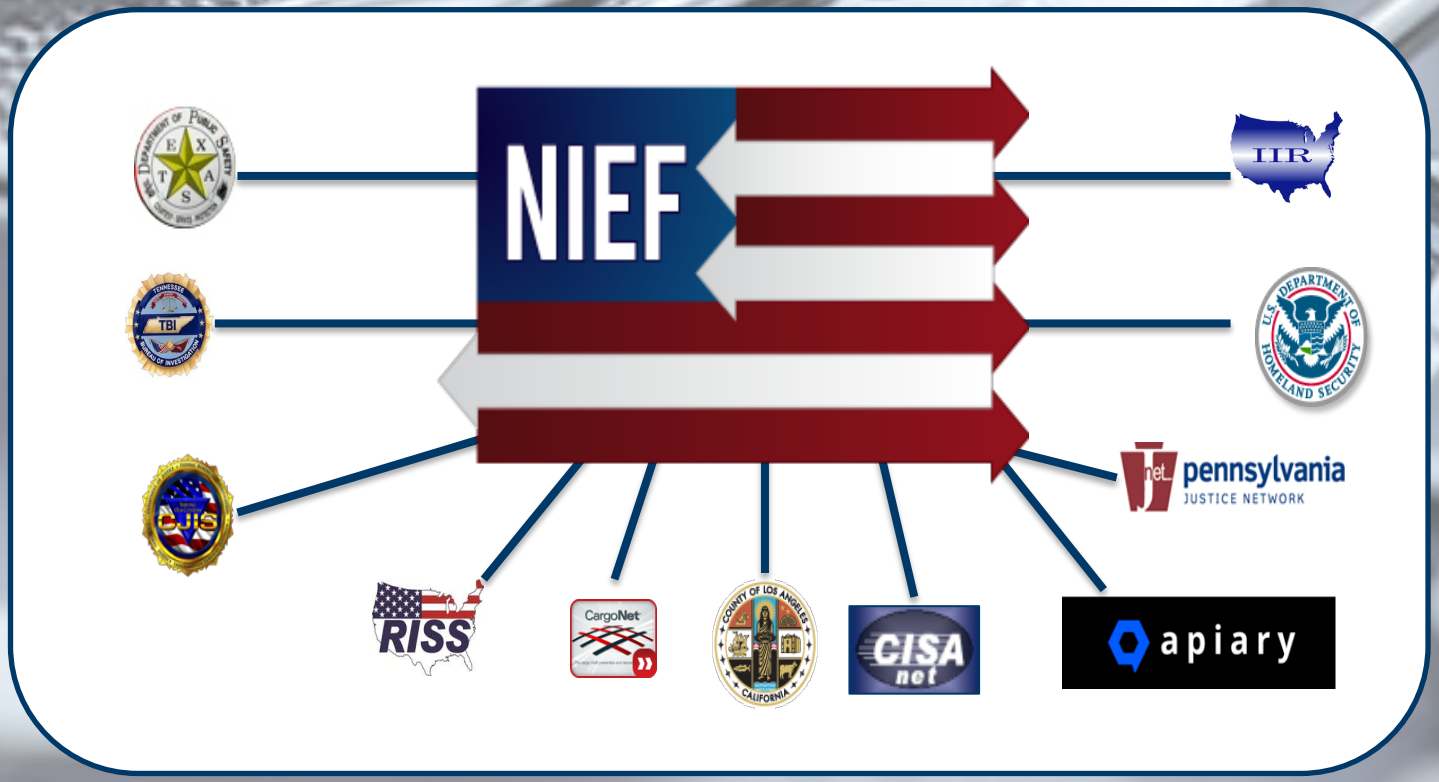
Georgia Tech Research Institute

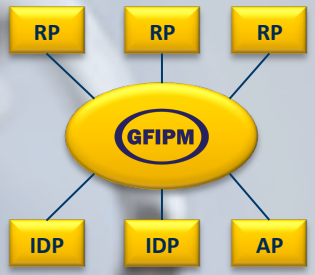


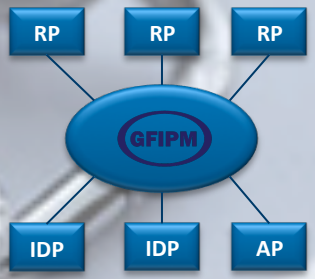
Global Justice Information Sharing Initiative

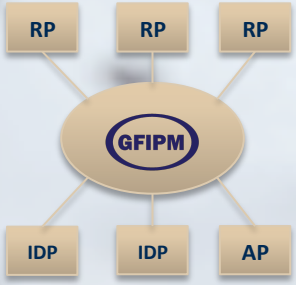
The Perspective from the LE Community

Georgia Tech Research Institute



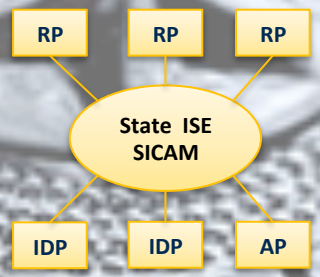


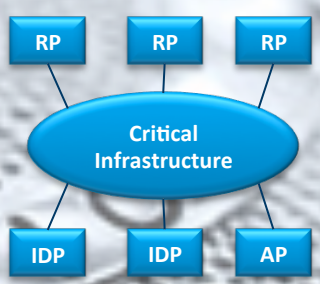


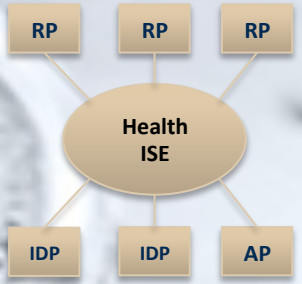


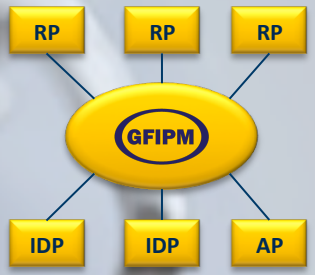
The Perspective from the LE Community

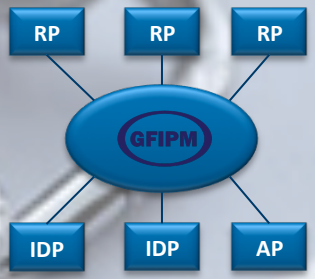
Georgia Tech Research Institute

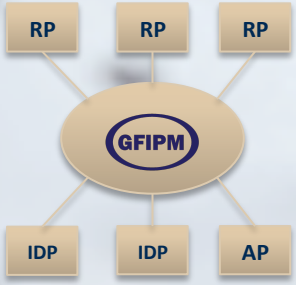


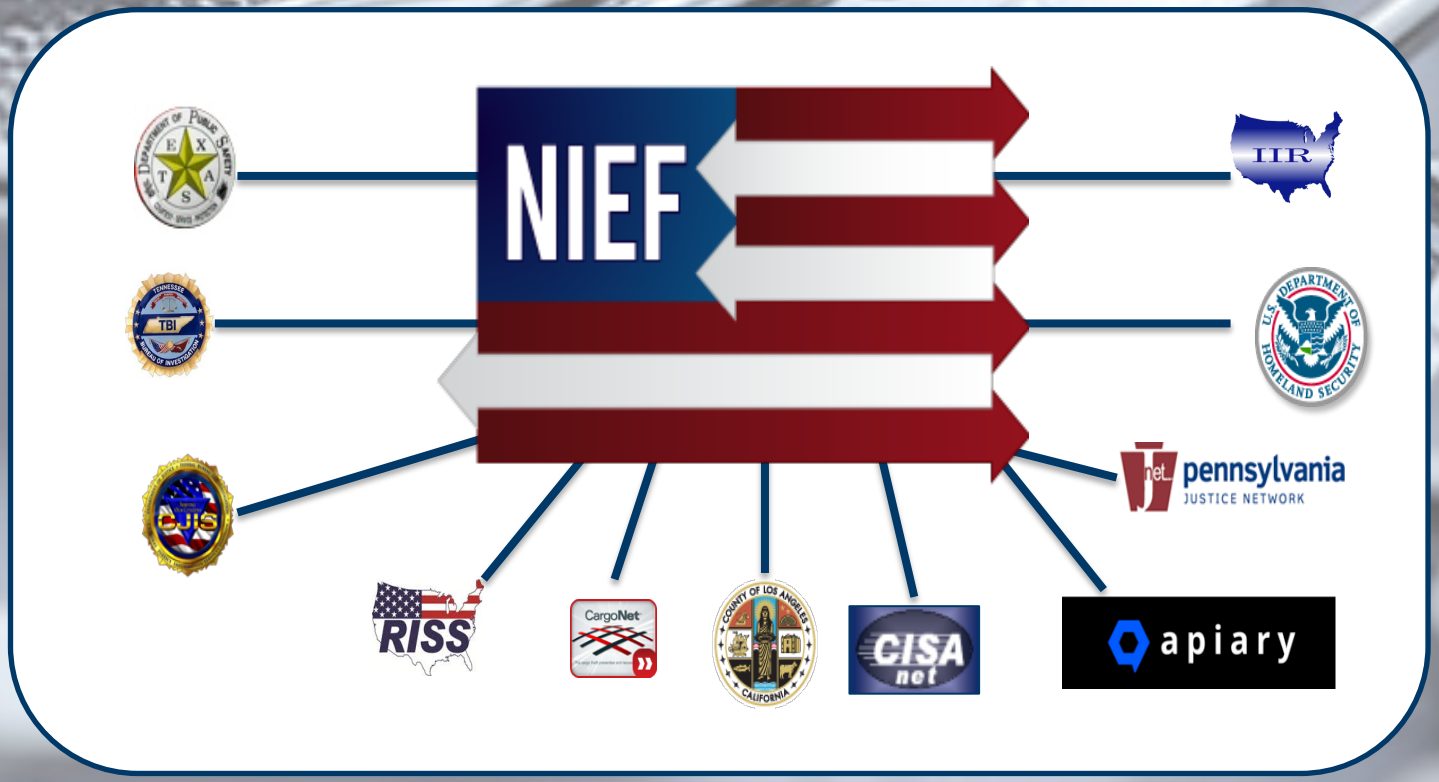












Some NIEF Members

Georgia Tech Research Institute

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 secure critical infrastructure and

IIR
Institute for Intergovernmental Research®

Post Office Box 12729
Tallahassee, FL 32317
(850) 385-0600
www.iir.com

CargoNet
The Cargo Theft Prevention and Recovery Network

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 theft victims, their business partners, and law enforcement. CargoNet offers A 24 hours a day, 7 days a week fusion center and cargo recovery network – staffed

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 (DOJ).

The RISSNET Portal currently provides secure access to services and resources to more than 9,000 federal, state, local, and tribal law member enforcement agencies as well as public safety and Critical Infrastructure / Key Resource (CI / KR) communities. In addition, RISS' participation in NIEF allows RISS to provide different levels of authorization to NIEF users based upon user attributes.

- RISS Resources available to all federated partner users:
  - RISS ATIX Website - RISS TechPage - Intelink-U
- RISS Resources available only to Sworn Law Enforcement Officers (SLEO) or those acting for SLEO:
  - RISS National Gang Program (RISSGang) Web Site - RISS Officer Safety Website - Cold Case Locator System, National Criminal Intelligence Resource Center (NCIRC) - National Motor Vehicle Title Information System (NMVTIS) - Nationwide SAR Initiative (NSI) Search Tool (must have SAR account) - Federal law Enforcement Training Center (FLETC) Electronic Learning Portal (ELP)

Contact: Larry Maloney
(lmaloney@rissnet.org/ria.net)

BJA Bureau of Justice Assistance U.S. Department of Justice

RISS – A Proven Resource for Law Enforcement™

Tennessee
Meth & Pharmaceutical Task Force

TENNESSEE Methamphetamine & Pharmaceutical Task Force

Homeland Security HSIN Homeland Security Information Network

HSIN is the nation's platform for sharing sensitive but unclassified information – enabling the Homeland Security Enterprise, its Federal, State, local, tribal, territorial

apiary
Apiary Threat Intelligence Framework

What is Apiary?

Apiary is an automated framework for malware analysis and threat intelligence. Members of our vetted community anonymously upload malware and benefit from the ongoing addition of in-depth malware correlation and behavior analysis. The results are delivered automatically within a secure sharing environm
for analysts, inve
protect their organ

Apiary processes
samples per day a
picture' relationshi
samples. Our ana
cutting edge resea
malware research
the Apiary commu
analysis process a
amongst a trusted
confidently make

Who uses Apiary

Apiary 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, Apiary is used by local, state, and federal government organizations including law enforcement and education. The

LA County Criminal History

Consolidated Criminal History Reporting System CCHRS Los Angeles County

Brought to you by ISD Los Angeles County

Powered by Java

Target Audience – Law Enforcement , Probation and Prosecution

CCHRS is the LA County Criminal History System used by Investigators and Prosecutors for filing criminal cases within LA County. It contains over 12,000,000 subjects with their record 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 CCHRS for their daily operations with 10,000+ transactions per day.

Status – Available Now (CCHRS-lite)

Sponsoring Agency – LA County Sheriff

Contact Rolf Embom at 562-403-6559 or rembom@isd.lacounty.gov

Where to from here?

A Variety of ID Ecosystem Perspectives

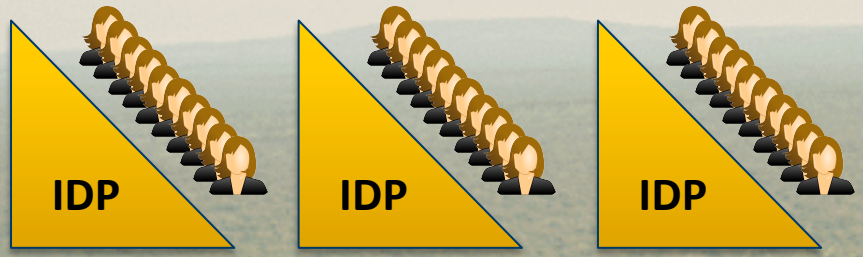
Georgia Tech Research Institute

Is the ID Ecosystem only about identification and authentication?

Or are attributes and authorization fundamental to it?

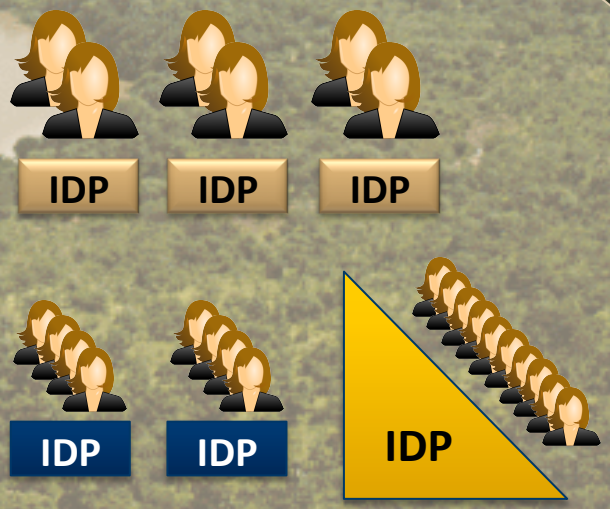
A Variety of ID Ecosystem Perspectives

Georgia Tech Research Institute



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

Georgia Tech Research Institute

Will Trust Frameworks **remain static** over time?

ID Trust Framework

Or must they constantly **evolve to meet new requirements**?

ID Ecosystem Vision

Georgia Tech Research Institute

Is it OK if the Trust Frameworks in the ID Ecosystem are mostly non-interoperable and non-trusting identity silos?

ID Ecosystem Vision

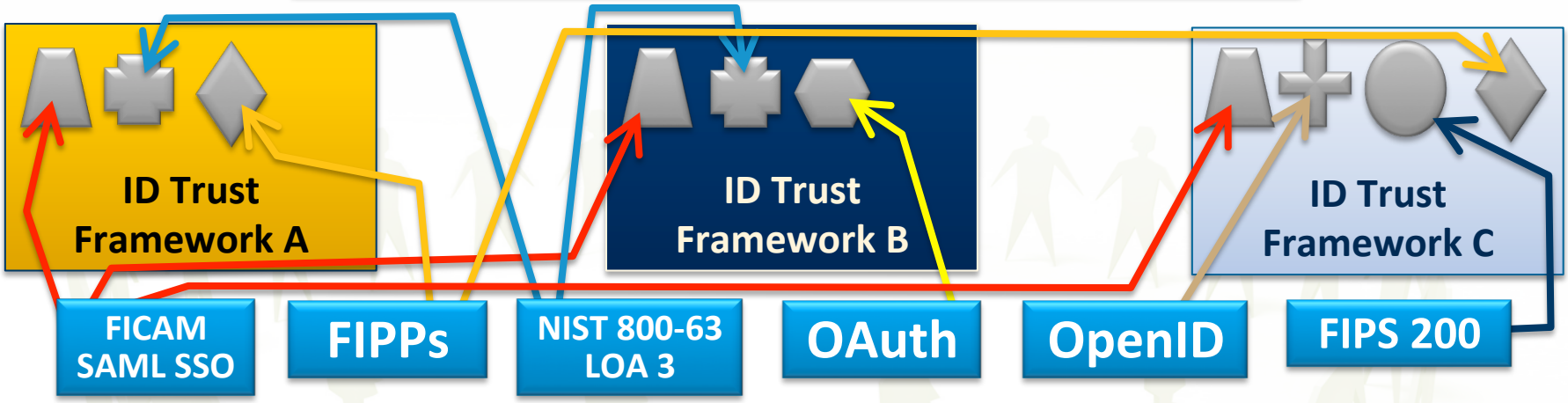
Georgia Tech Research Institute

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?

Georgia Tech Research Institute

If the frameworks were modular…



…then we get:

Greater transparency of trust framework requirements

Greater ease of comparability between frameworks

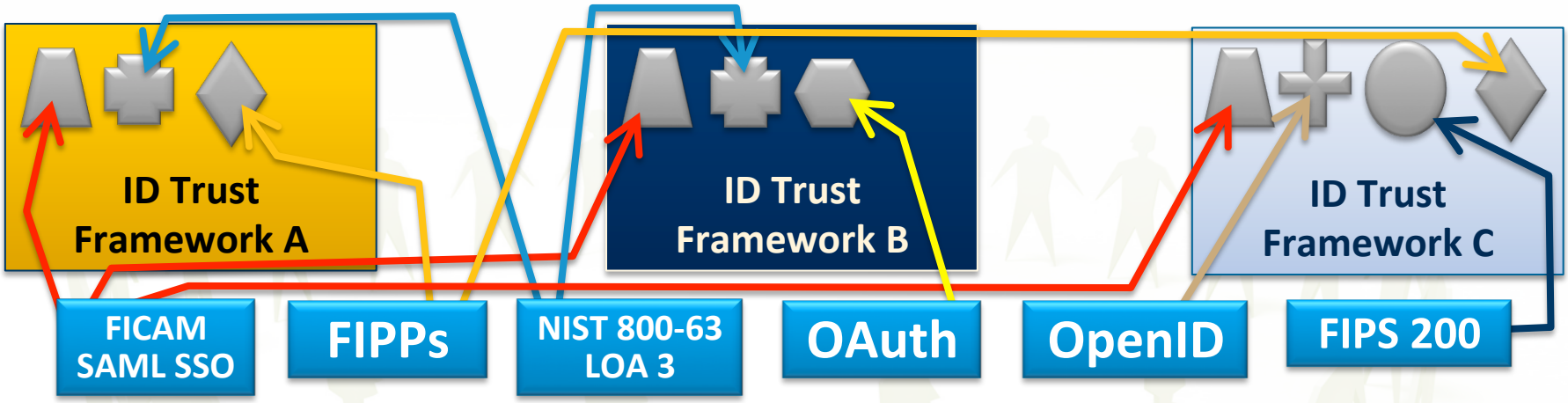
Greater potential for reusability of framework components

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?

Georgia Tech Research Institute



These modular components are called Trustmarks.

A Few Examples of Trustmarks

Georgia Tech Research Institute

- 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)

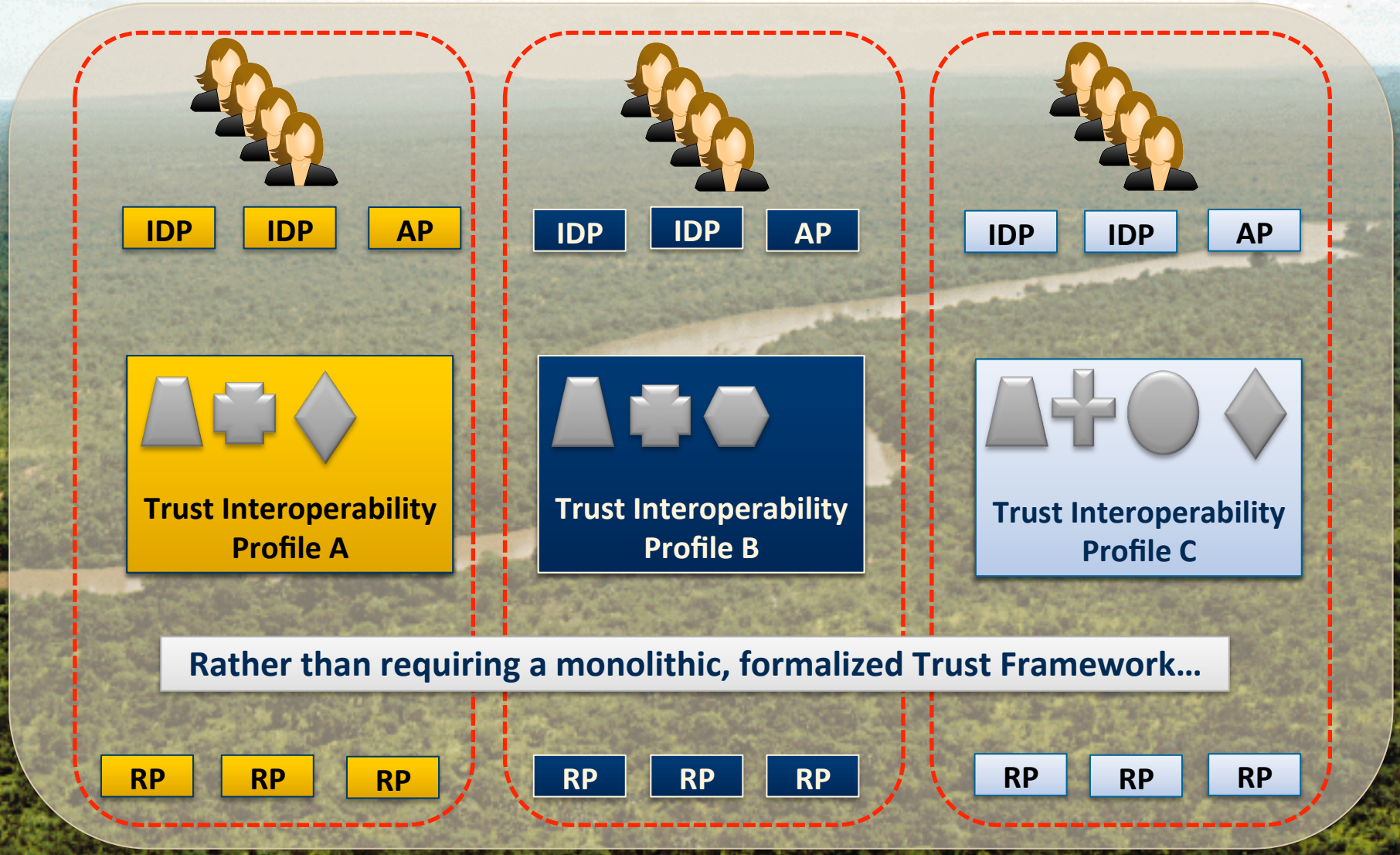
Technical
Trust
Privacy
Security
Business

Trustmark Policies & Trustmark Agreements

Legal

A Trustmark-Based ID Ecosystem

Georgia Tech Research Institute



A Trustmark-Based ID Ecosystem

Georgia Tech Research Institute

IDP IDP AP

Trust Interoperability Profile A

RP RP RP

IDP IDP AP

Trust Interoperability Profile B

RP RP RP

IDP IDP AP

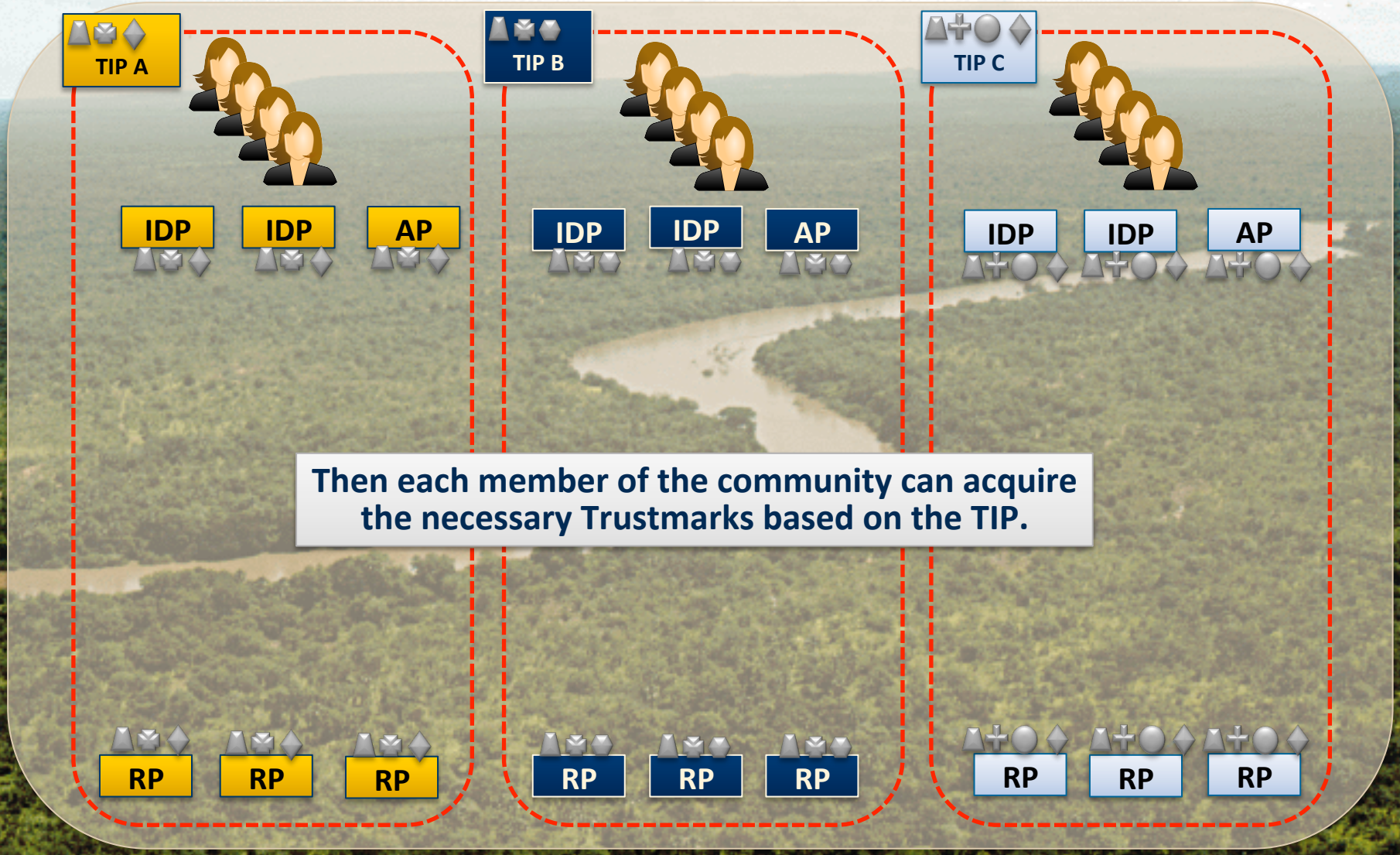
Trust Interoperability Profile C

RP RP RP

...each community can define a TIP.

A Trustmark-Based ID Ecosystem

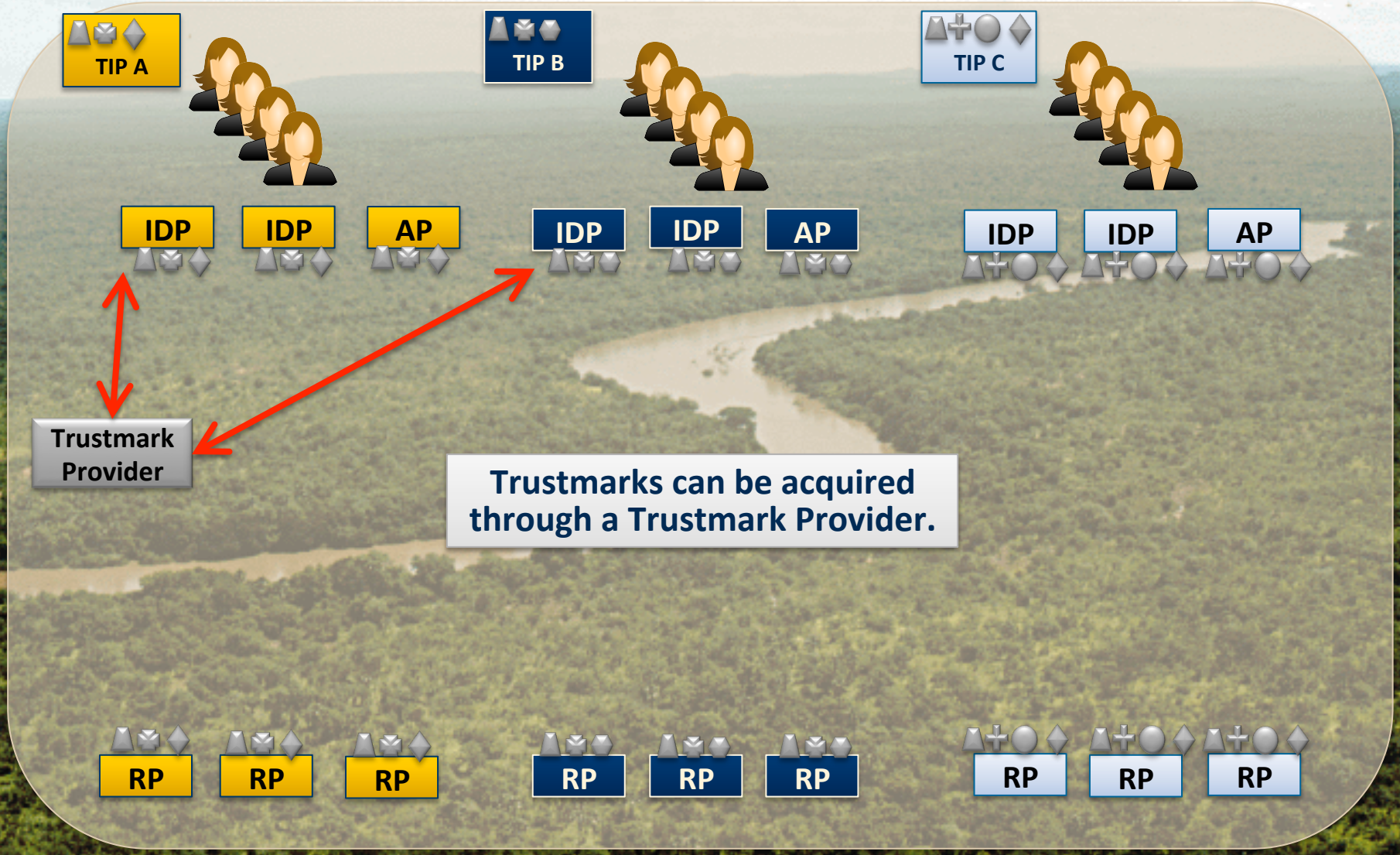
Georgia Tech Research Institute



Then each member of the community can acquire the necessary Trustmarks based on the TIP.

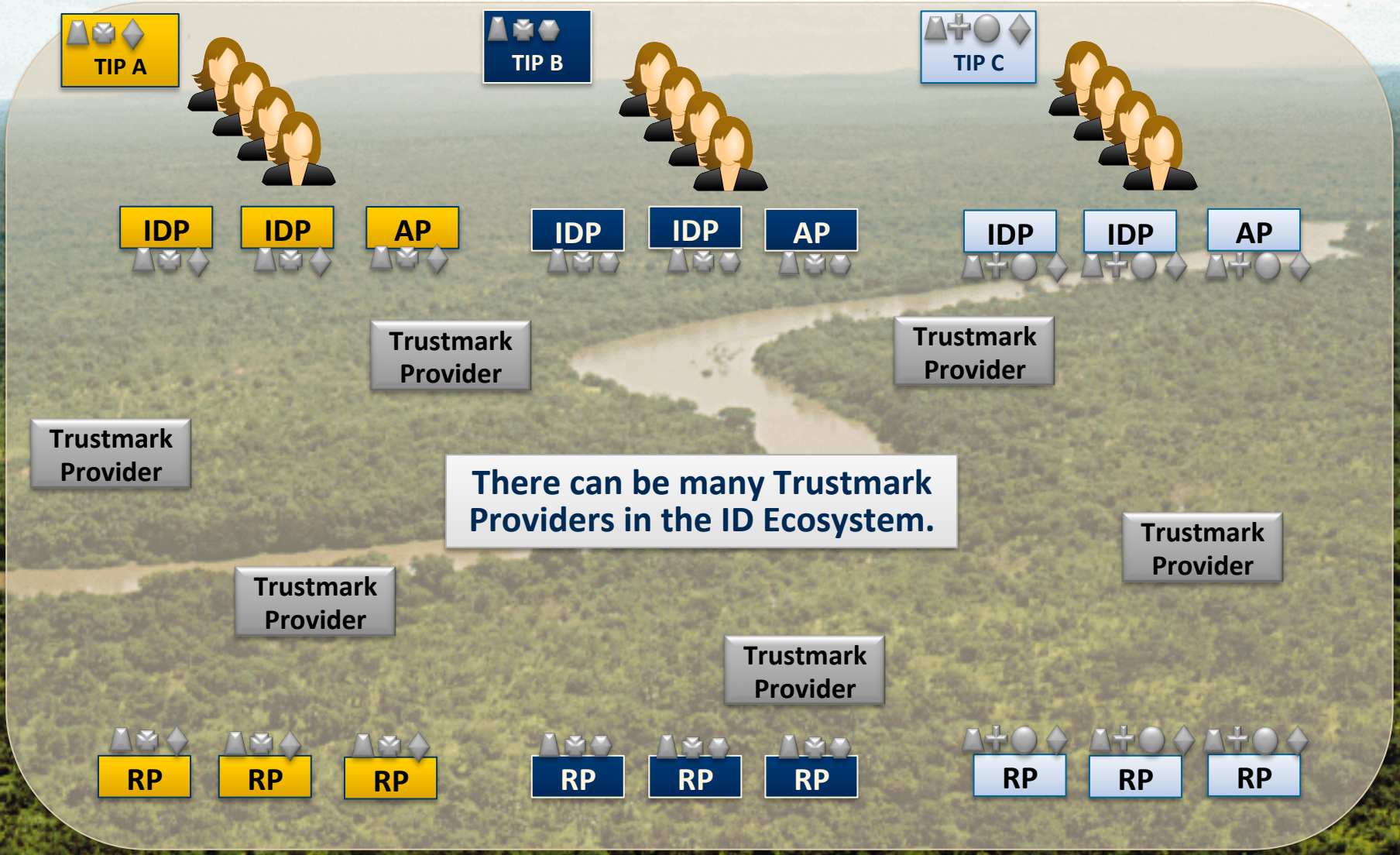
A Trustmark-Based ID Ecosystem

Georgia Tech Research Institute



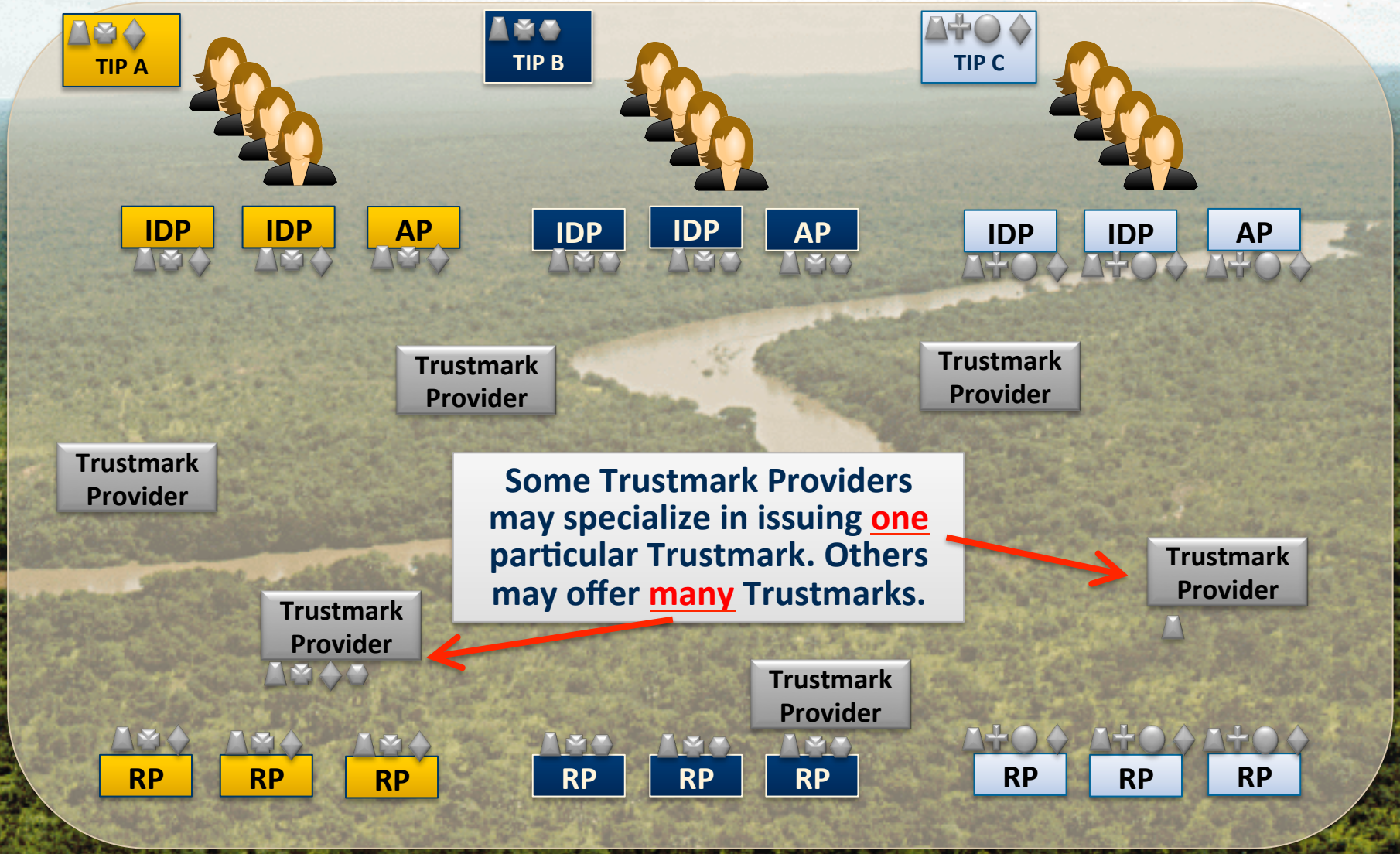
A Trustmark-Based ID Ecosystem

Georgia Tech Research Institute



A Trustmark-Based ID Ecosystem

Georgia Tech Research Institute

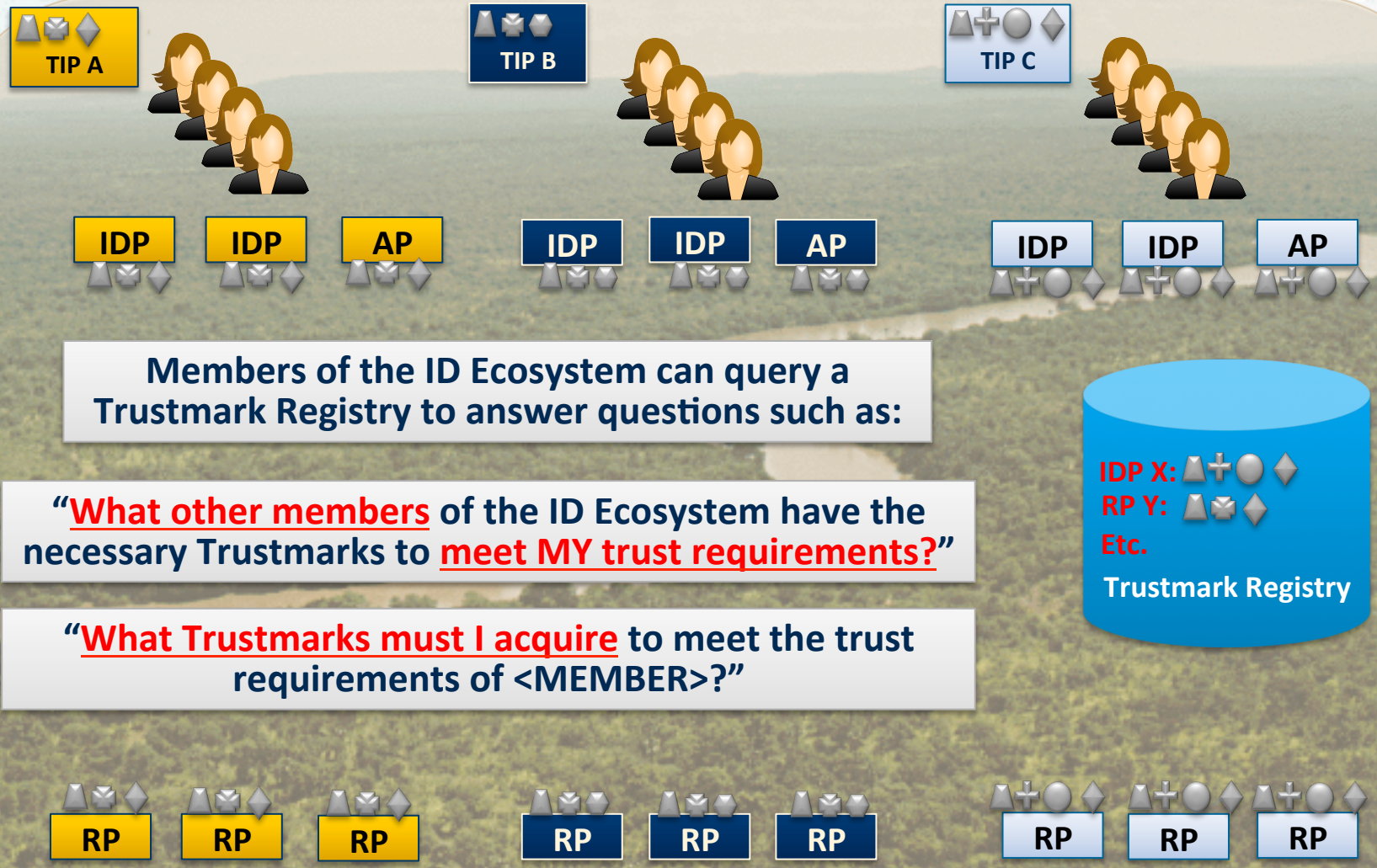


A Trustmark-Based ID Ecosystem

Georgia Tech Research Institute

A Trustmark-Based ID Ecosystem

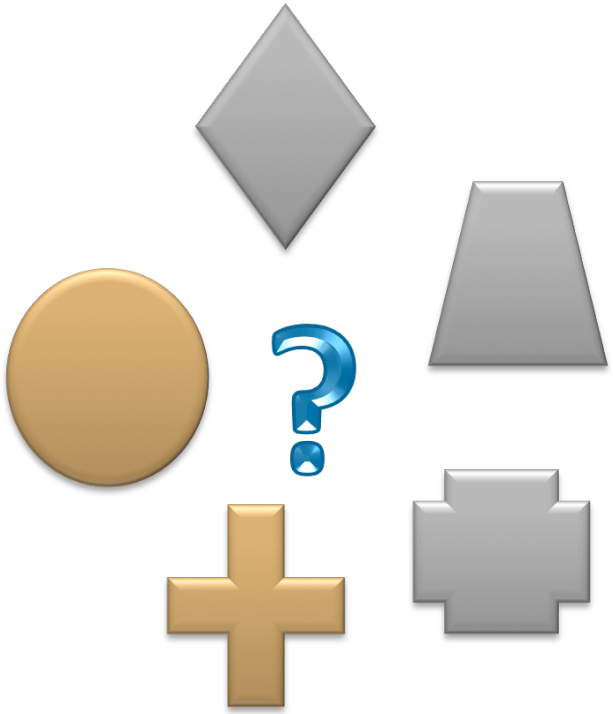
Georgia Tech Research Institute



A Trustmark-Based ID Ecosystem

Georgia Tech Research Institute

Trustmarks – What? Where?



Sources of Components

Georgia Tech Research Institute

GFIPM Trust & Interop Components

Georgia Tech Research Institute

NIEF Trust & Interop Components

Georgia Tech Research Institute

FICAM Trust & Interop Components

Georgia Tech Research Institute

AAMVA Trust & Interop Components

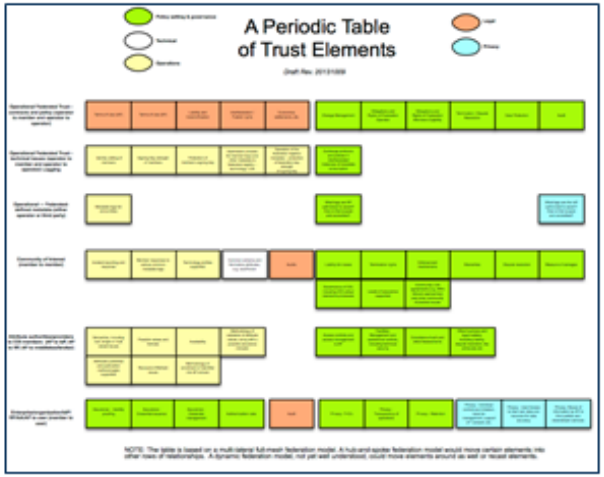
Georgia Tech Research Institute

Business Requirements	FDR Model Training Program	Internal Review of Document Issuing Systems
Business and Systems Integrity	Audit Pl	
Initial Customer Identification	Residency	Verify other
Record and Document Creation	Name collection use and maintenance	Use immigr docum
Record and Document Use	Minimum Penalties and Sanctions For Unlawful Use	

Requirement

Another Component Perspective

Georgia Tech Research Institute



Source: Ken Klingenstein, Internet 2

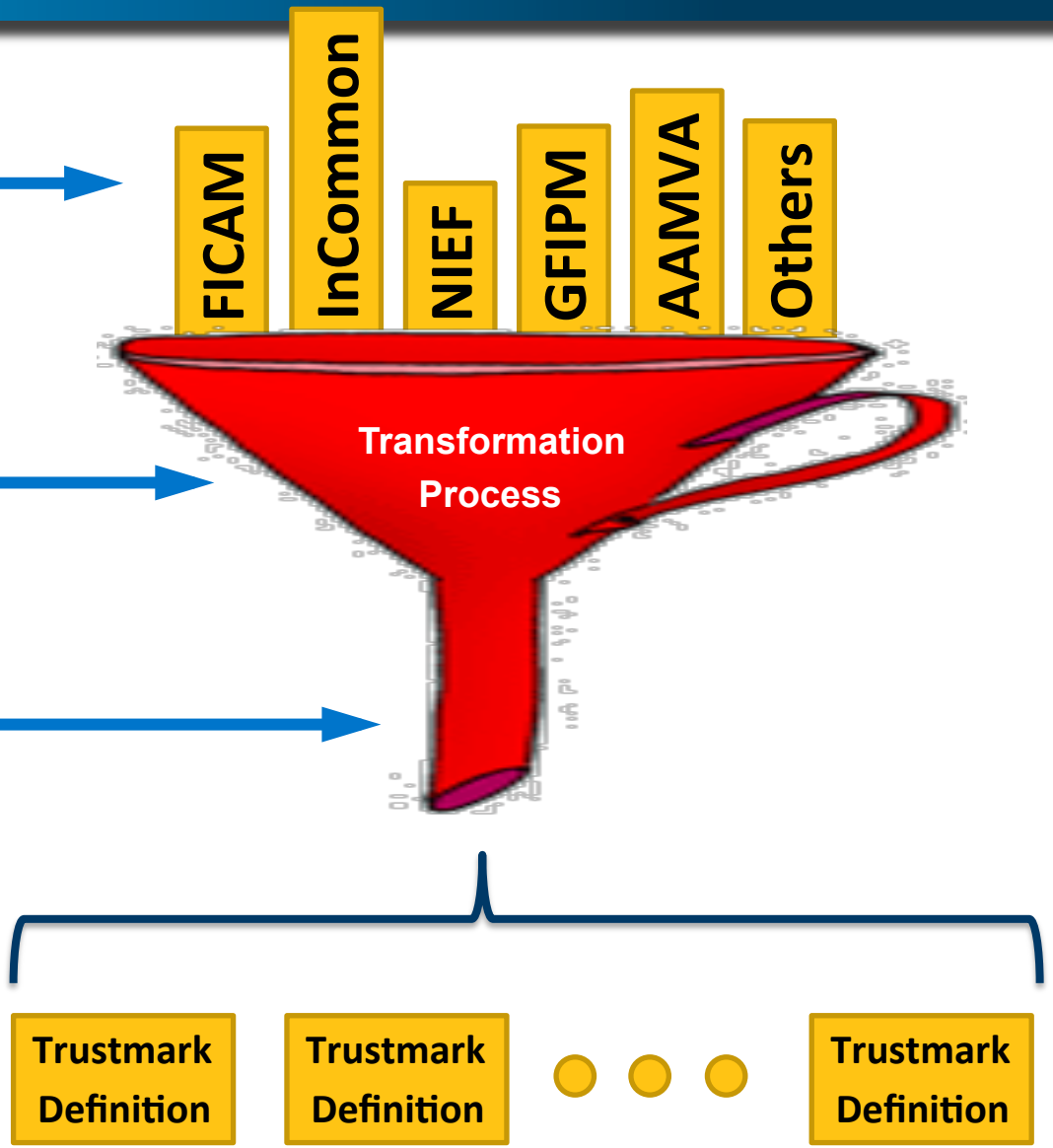
Creating Modular Common Components

Georgia Tech Research Institute

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

Georgia Tech Research Institute

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

122 distinct trustmarks identified (so far)

Covers FICAM, GFIPM, & NIEF communities

Also covers FIPPs (privacy) topics

Trustmarks By Category

Georgia Tech Research Institute

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

Security Policy
(18 Total, 18 Essential to Pilot)

Privacy Policy
(23 Total, 15 Essential to Pilot)

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

Technical Interoperability
(57 Total, 8 Essential to Pilot)

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

Technical Trust
(4 Total, 3 Essential to Pilot)

Usability
(2 Total, 0 Essential to Pilot)

Scope of the NSTIC Trustmark Pilot

Georgia Tech Research Institute

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

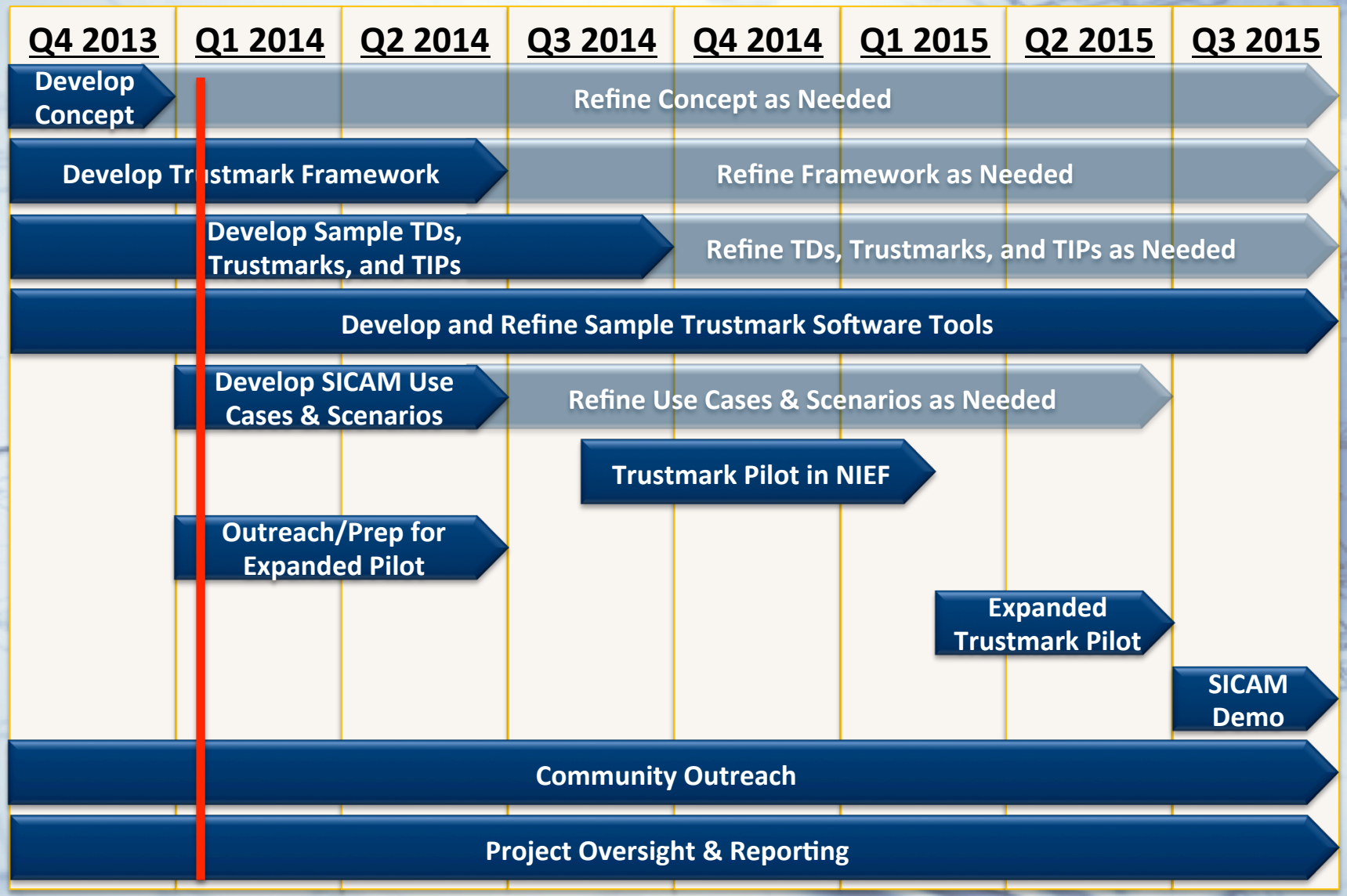
- Issue Trustmarks to Current NIEF Members
- Modify Tech Framework, Specs, TDs, TIPs, Policies, Agreements, and Tools as Needed

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

Georgia Tech Research Institute



How the IDESG Can Help

Georgia Tech Research Institute

- 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