resilient
network systems

Kantara Initiative
NSTIC Pilots in Motion

30 January 2013

Work described in this presentation was supported by the National Strategy for Trusted Identities in Cyberspace (NSTIC) National Program Office and the National Institute of Standards and Technology (NIST).

Resilient Network Systems Kantara NSTIC Agenda

The Resilient Network Systems NSTIC Pilots
- Overview and Challenges

Defining a Trust Network
- What is a Trust Network
- What does a Trust Network offer
- How does a Trust Network work

NSTIC Pilot Status and Demo

Trust Framework Activity Review

Commercialization Efforts
- Incremental Solutions
- Framework for Implementation

Q&A

Resilient Network Systems NSTIC Pilots

Purpose:

Deliver national scale, secure, privacy-enhancing, on-demand, authentication and compliant authorization for online transactions and access control in Healthcare (HIPPA / HITECH) and Education (FERPA / COPPA)

NSTIC NIST National Institute of Standards and Technology U.S. Department of Commerce

Healthcare

Participants in Patient Centered Coordination of Care (PCC) Pilot

kantara INITIATIVE
Gorge Health Connect, Inc.
SAN DIEGO HEALTH CONNECT Better Information • Better Care
AUTHENTIFY
LexisNexis
AMA AMERICAN MEDICAL ASSOCIATION
MEDICITY
mirth
National eHealth Collaborative

Education

Participants in Zero-knowledge Identity and Privacy Protection Service (ZIPPS) Pilot

KnowledgeFactor
LexisNexis
NLET
neustar
WARNER BROS. ONLINE
RUSD
accenture
Clever
SUNGARD
Santa Cruz County Office of Education
kantara INITIATIVE

resilient network systems

Challenges in Education and Healthcare Information Exchange

Roadblocks in Education:

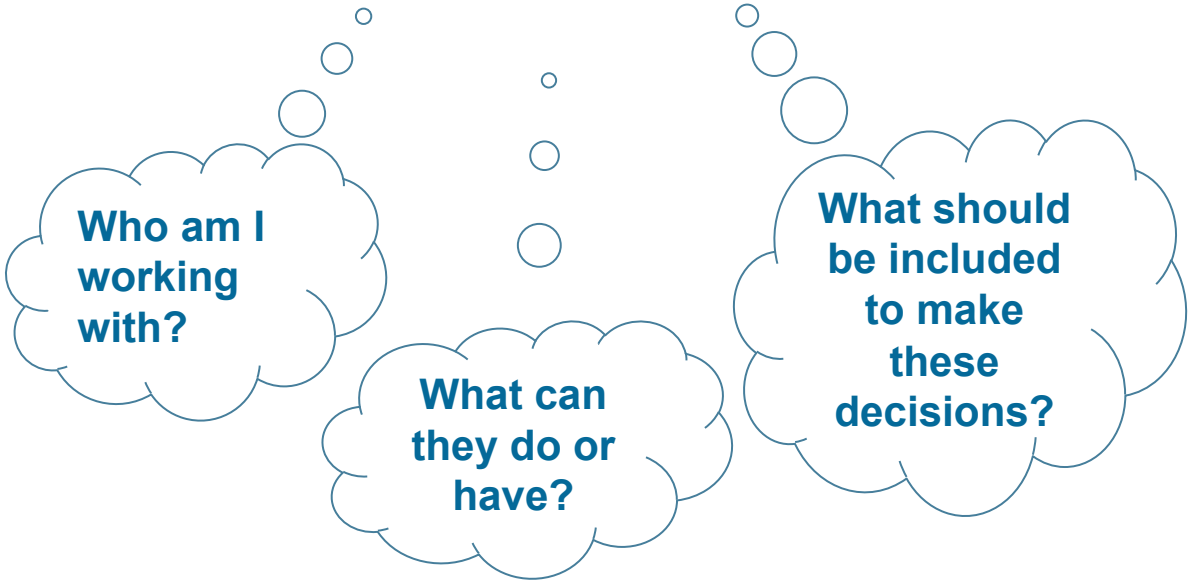
- **Centralized databases and services present both real and perceived security and privacy risks**
- **Regulations (e.g. FERPA and COPPA) require an established Trust Framework**
- **Centralized, disparate identity stores and applications hinder access to online media and learning**
- **Fragmentation among School Information Systems and Educational Support Systems, as well as low local IT budgets, inhibit ecosystems' scalability and national reach**

Roadblocks to HIE for Coordinated Care:

- **Reliance on current, identity-based solutions impose high costs, inhibit adoption and prevent scale**
- **Assurance exists only between integrated organizations, known users, and resources**
- **Systems have inconsistent roles, permission, identities, resources and administration**
- **Privacy challenges and regulatory compliance pose significant risk for Health IT adopters**

What is a Trust Network

A Trust Network is a neutral, peer-to-peer software platform for automating context-aware decisions.

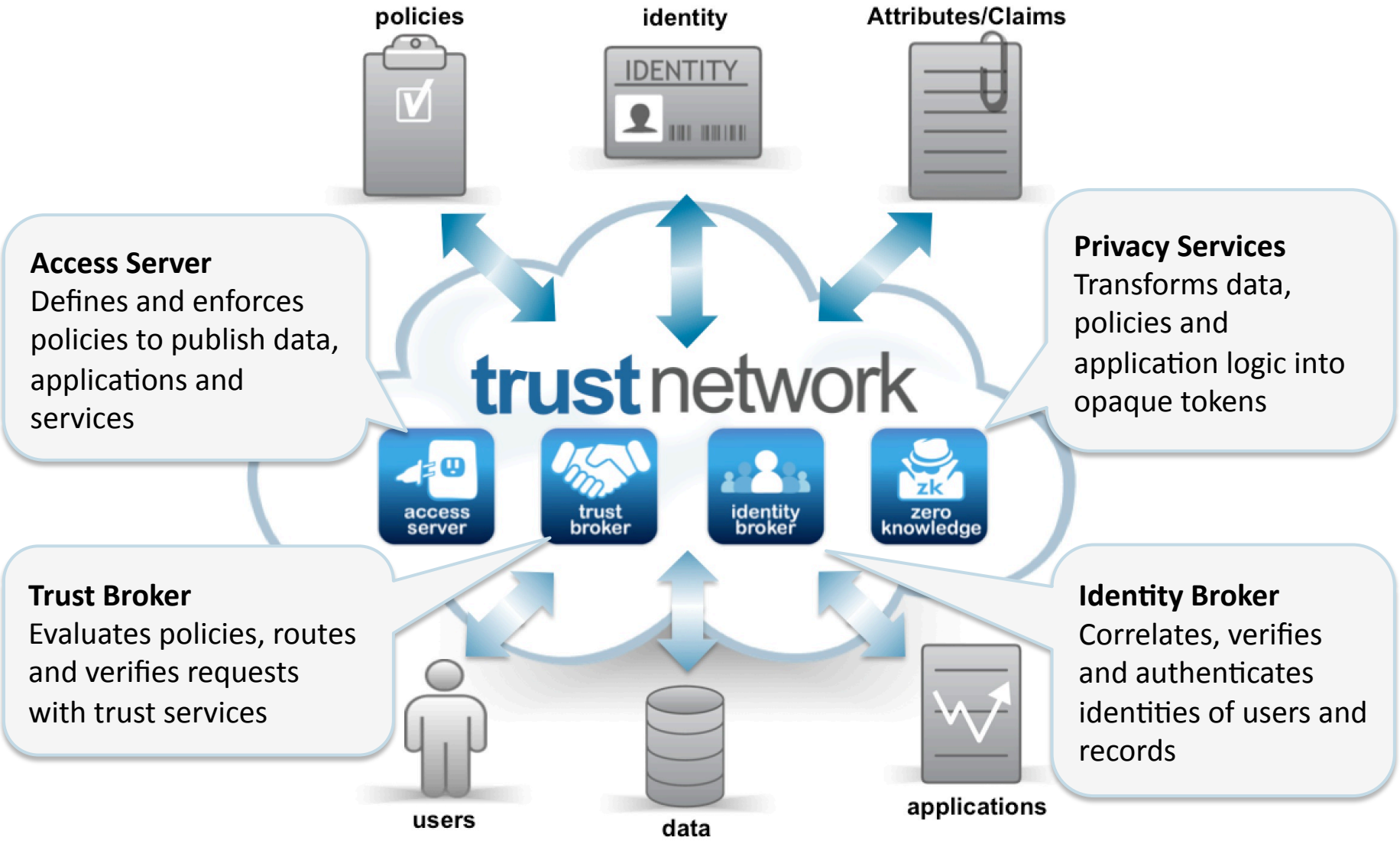


A Trust Network evaluates and enforces the criteria for **trusted interactions** between users, relying parties, attribute providers, and other online services.

Trust Network enables

- Syndicated Data, Services, Applications
- Secure and Resilient verification of facts
- Privacy-Enhanced Discovery and Access
- Automated Compliance and Accounting
- Administrative and End-User Convenience

How Does a Trust Network Work



Access Server
Defines and enforces policies to publish data, applications and services

Privacy Services
Transforms data, policies and application logic into opaque tokens

Trust Broker
Evaluates policies, routes and verifies requests with trust services

Identity Broker
Correlates, verifies and authenticates identities of users and records

Current Pilot Operations and Outcomes

Healthcare Pilot

- HIPAA-compliant eReferrals between Doctors and Staff, across HIE and State boundaries
  - Gorge Health Connect, OR
  - San Diego Health Connect, CA
- 4 Sources for Attribute Verification
  - AMA and LexisNexis - National
  - GHC and SD Health Connect
- Privacy-enhanced multi-factor authentication: Phone, KBA, Email
- Trust Framework developed with collaborative working group
  - National eHealth Collaborative leading 24 participants

Education Pilot

- K-12 education software and services providers utilizing Trust Network API's to provide enhanced student and parent access
  - 3 CA School Districts to pilot in Q1 2014 - Riverside, Pajaro Valley and King City School Districts
  - National Scale SIS and Attribute Verification Sources – SunGard and Clever
- Anywhere access to online training for authenticated / authorized employees (no VPN)
  - Demonstration testing by Accenture employees, accessing Knowledge Factor online learning programs

Healthcare : PCC Pilot eReferral Demonstration

HIPAA-compliant eReferrals between Physicians and Staff at disparate medical organizations, on different Health IT platforms, using a secure, Direct Messaging Gateway with Trust Network privacy protection.

Actors

State	HIE	Medical Org	Physicians	Role
Oregon	Gorge Health Connect	One Community Health Clinic	Dr. Art Ticknor and Staff	Primary Care Physician
California	San Diego Health Connect	UC San Diego Medical Center	Dr. James Killeen and Staff	Consulting Cardiologist

Services

	Purpose	Services
1	Sender access to Direct Message application	Medicity iNexx or MirthMail
2	Receiver access to standard email application	Gmail, MS Exchange, etc.
3	Verification of Physician status and Phone Authentication	AMA Physician Verification Srvc. + Authentify Phone Authentication Srvc.
4	Verification of Staff status and KBA Authentication	Local staff directory + LexisNexis Instant Authenticate

PCC Pilot eReferral Demo VIDEO

Special thanks to the Physicians, Staff and IT Professionals at all of the partner organizations participating in the NSTIC Pilot and Trust Network Ecosystem.

resilient network systems

Trust Framework Review

Pilot Ecosystem Trust Frameworks

- Trust Frameworks in development for Healthcare and Education ecosystems
- Leveraging working groups, as well as pilot experiences

Modular Assessment Criteria for Trust Network

- Kantara Initiaitive and partners are mapping current criteria to ecosystem model
- Level of Assurance equivalents to assessment, via dynamic implementation of policy enforcement at run-time

Trust Framework - Pilot Ecosystem Development

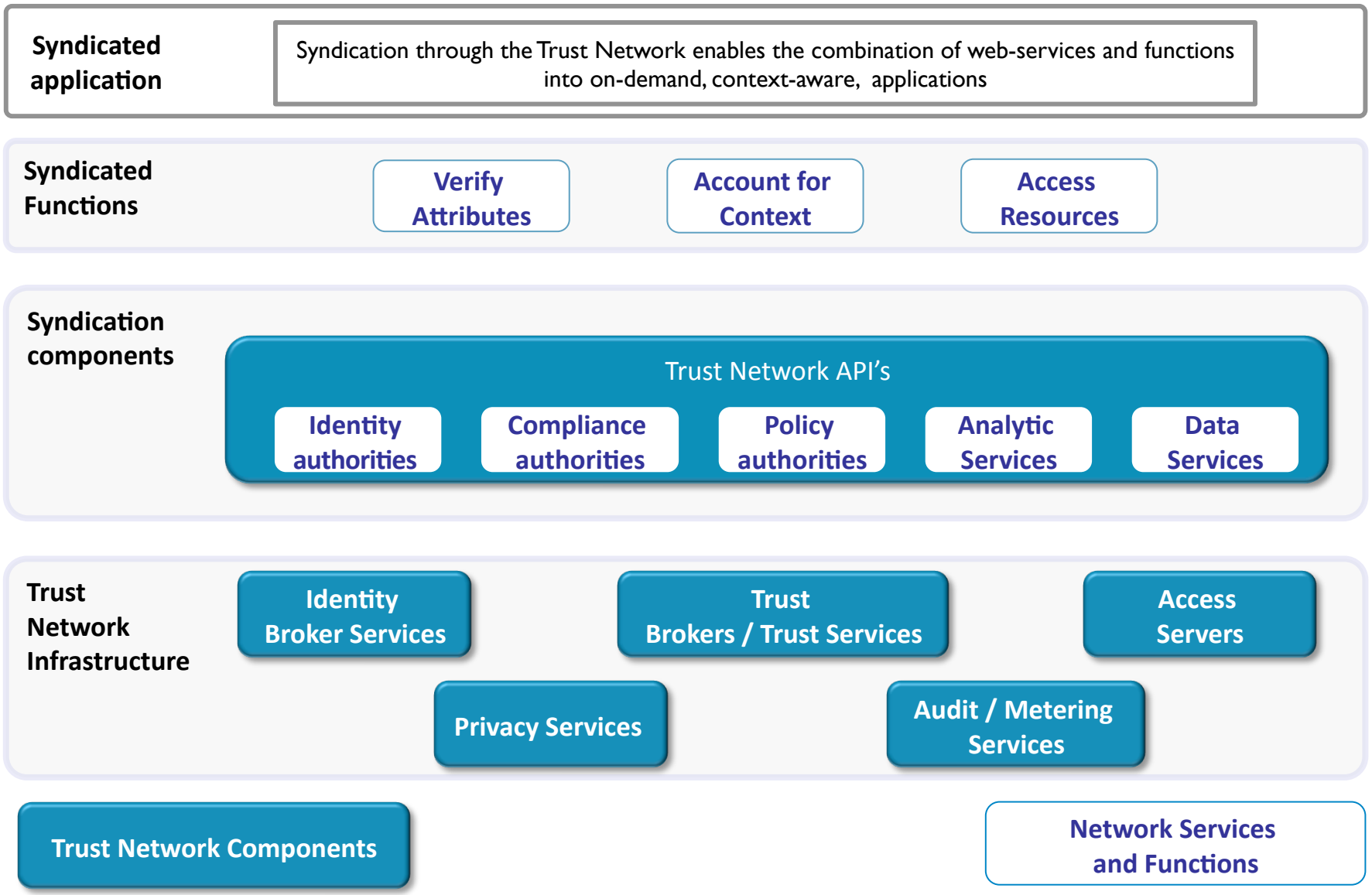
Healthcare Pilot

- **Trust Framework** developed with collaborative working group of 24 pilot participants and independent healthcare and privacy experts
- 11 working group sessions coordinated by the National eHealth Collaborative (NeHC)
  - Refined policy taxonomy and healthcare/privacy regulations
  - Drafted and reviewed Trust Framework document
- Trust Framework document for pilot is complete, and in operation by pilot participants
- Expansion planned for post-pilot commercialization of healthcare ecosystem

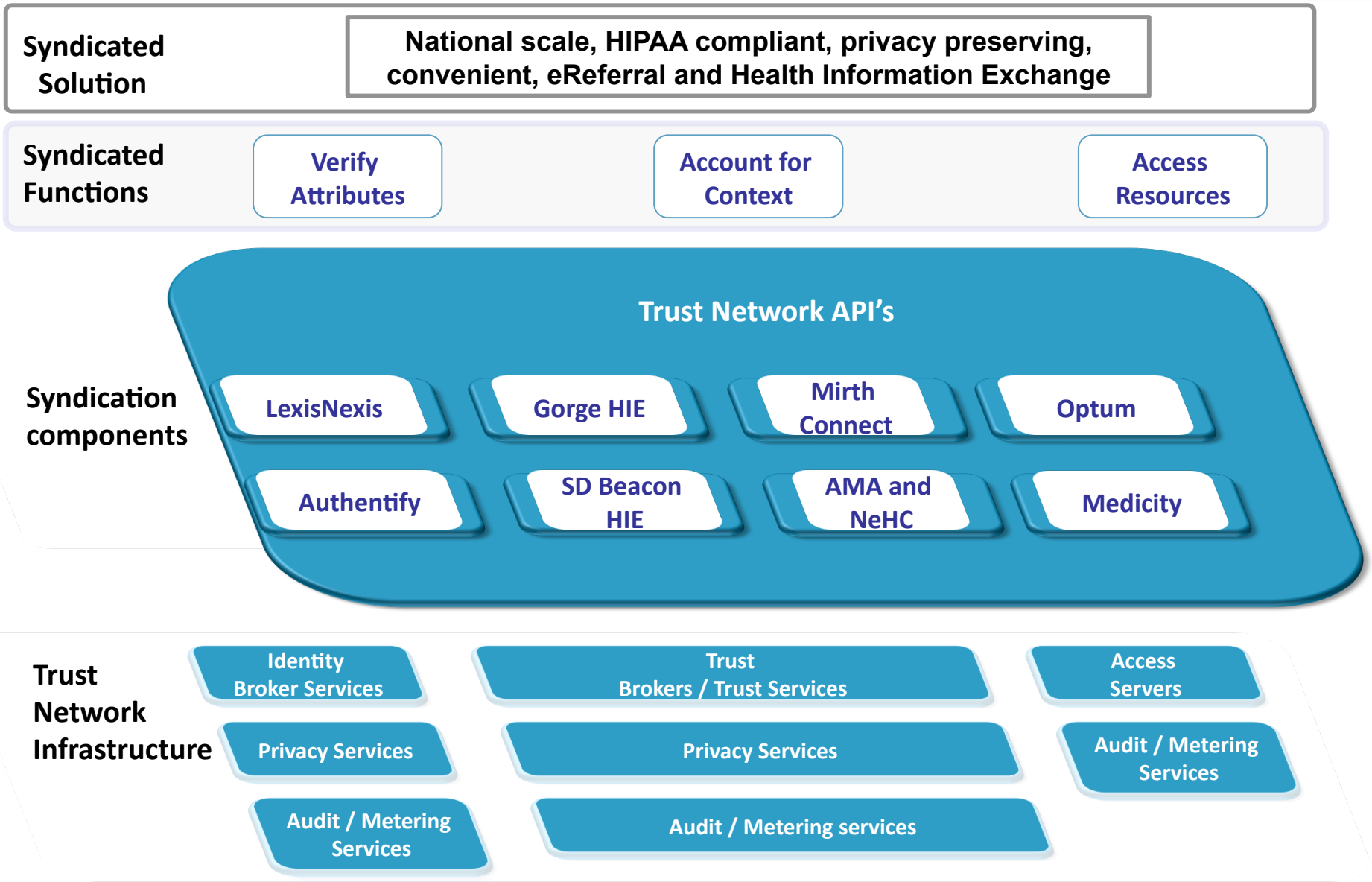
Education Pilot

- Trust Framework in development
- Leveraging experiences from Healthcare TF working group

Trust Network Syndication Architecture



Healthcare Pilot Overview



resilient network systems

Commercialization of the Pilot Ecosystems & Solutions

Syndicated Solution

National scale, HIPAA compliant, privacy preserving, convenient, eReferral and Health Information Exchange

Resilient Network Systems Challenge

How to bridge the gap between "Core Services" and developing Trust Ecosystems in various markets, and obtaining a viral network effect?

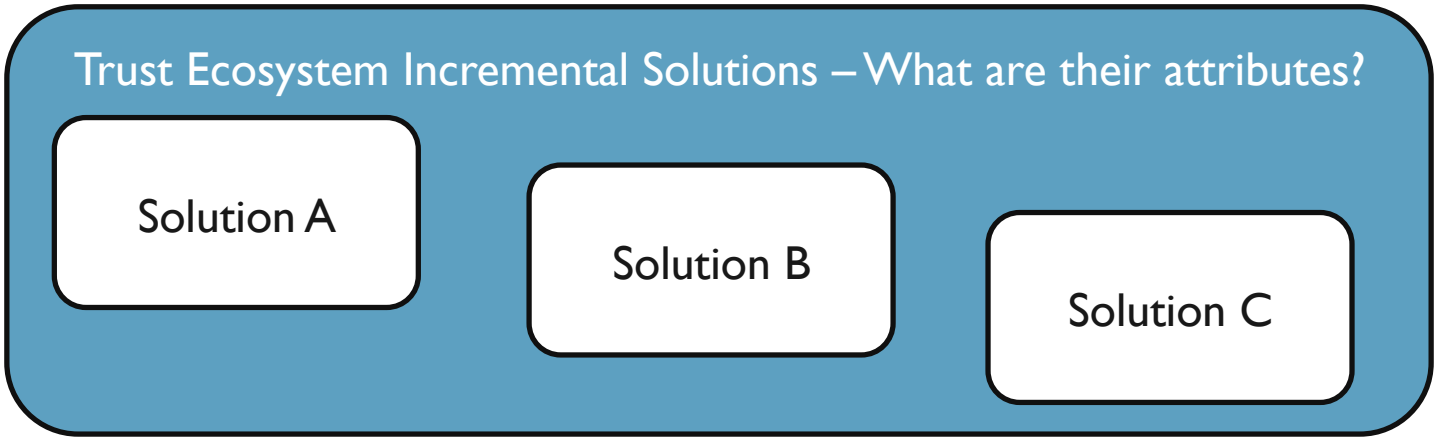
Core Services

- Access Server
- Trust Broker
- Identity Broker
- Zero-Knowledge Broker
- Logging & Metering
- Trust History
- Trust Vault
- Opaque Token Service

Commercialization of the Pilot Ecosystems & Solutions

Syndicated Solution

National scale, HIPAA compliant, privacy preserving, convenient, eReferral and Health Information Exchange



Core Services

- Access Server
- Trust Broker
- Identity Broker
- Zero-Knowledge Broker
- Logging & Metering
- Trust History
- Trust Vault
- Opaque Token Service

Commercialization of the Pilot Ecosystems & Solutions

General Attributes of Incremental Solutions

- Solutions build off of existing implementations for NSTIC Pilots
- Provide business value in and of themselves
  – solving a specific business problem
- Serve as on-ramps to broader Trust Ecosystem adoption
  – each developed with ability to integrate in larger Trust Ecosystem
- Meet requirements for Privacy, Security, and Context needed to solve business problems
- Scalable and sustainable with modest additional investment
- Offered via low-friction, convenient (e.g. Software-as-a-Service) models

Implementation Framework for Commercialization

1 Define the Users:

- What organizations are involved and interconnected
- Who are the users
- How are users identified
- What roles and relationships are used now and required

2 Define the Policy

- Describe security constraints
- Describe the context required for Trust
- Define privacy requirements and sensitive data
- Identify attributes and equivalents

3 Define the Resources:

- Identify the Resources (web applications, API, etc.) to be protected
- Identify and define Trust Authorities:
  - Identity Sources
  - Attribute Sources
  - Context Authorities

Learn More

Resilient Networks Systems NSTIC Pilots Website:
http://www.resilient-networks.com/nstic/

Points of Contact

- Joe Glynn – NSTIC Pilot Director for RNS
  - Joe.Glynn@resilient-networks.com
  - Phone: 415-291-9600 x116

- Brit Wanick – VP Services and Operations
  - Britton.Wanick@resilient-networks.com
  - Phone: 415-717-3899