Building Trusted Transactions

Identity Authentication & Attribute Exchange
In Public and Private Federations

Kantara Initiative
OrangeFT Paris 2010

Joni Brennan, Kantara Initiative

Kantara Initiative Overview

Open and Agile…

Kantara Initiative is Born (mid-2009)

kantara™
INITIATIVE

Kantara (kan-TAR-a): Swahili for "bridge"; Arabic roots in "harmony"

Internet Society

LIBERTY ALLIANCE PROJECT

DataPortability Project

XDI.org

OPENLIBERTY
SECURE IDENTITY WEB SERVICES

CONCORDIA IN IDENTITATE

kantara INITIATIVE

Primary focus to foster:

- industry coordination
- interoperability
- innovation
- broad adoption

...through the development of:

- technical specifications
- operational frameworks
- deployment best practices
- compliance programs

Trustees

AOL · BT · ca Transforming IT Management · Fidelity · Internet Society · LIBERTY ALLIANCE PROJECT

neustar · NRI · NTT · ORACLE

Members

AARP.org · BIPAC · .nyc · CSC · Danish Biometrics Research Project Consortium · IT- og Telestyrelsen Ministeriet for Videnskab Teknologi og Udvikling · DataPortability Project · DMA Direct Marketing Association

T · Drummond group · eHealthOhio · EIFEL Building a Learning Europe · ERICSSON · FISCHER INTERNATIONAL · ftgroup

Fraunhofer FOKUS · Fraunhofer SIT · FuGen Solutions · fun communications · FSTC · GPII GLOBAL PATIENT IDENTIFIERS INC. · gluu

GSA U.S. General Services Administration · HIMSS · idcentropy · INTERNET2 · kantega · MEDNET mednetworld.com Connecting Healthcare · mydex

National Notary Association · STATE SERVICES COMMISSION Te Komihana O Ngā Tari Kāwanatanga · NetStar 1 · NHK · PayPal · phase2 TECHNOLOGY · PingIdentity · Platinum SOLUTIONS

RedIRIS · SAFE-BioPharma · SIGNICAT · Smart Card Alliance · SPIKE networked enterprises · SUNET · swiss sign · TAS3

TERENA · i Scheme · UBISECURE · UNINETT · Vivat! impatient ideas · UNIVERSITY of WASHINGTON · POLITÉCNICA Ingeniamos el futuro · XDI.org

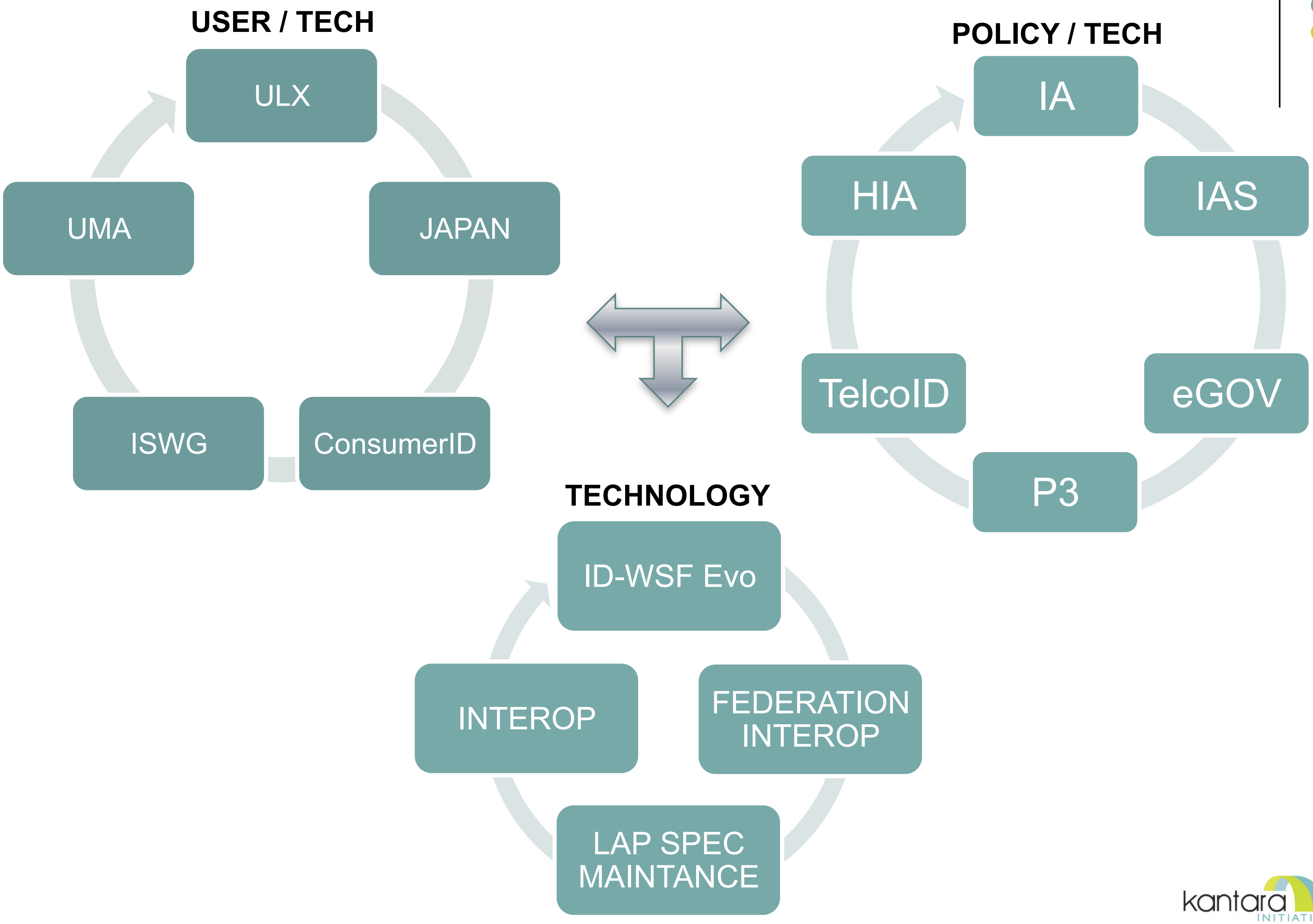
Kantara Initiative enables Harmonization

Bridging and harmonizing the identity community with actions that will help ensure secure, identity-based, online interactions while preventing misuse of personal information so that networks will become privacy protecting and more natively trustworthy environments.

It is our mission and goal to work openly with the Identity community to develop and harmonize real value solutions to solve issues facing Identity Access Management today…

http://kantarainitiative.org

KI Work Group Ecosystem



USER / TECH

ULX

JAPAN

ConsumerID

ISWG

UMA

POLICY / TECH

IA

IAS

eGOV

P3

TelcoID

HIA

TECHNOLOGY

ID-WSF Evo

FEDERATION INTEROP

LAP SPEC MAINTANCE

INTEROP

kantara INITIATIVE

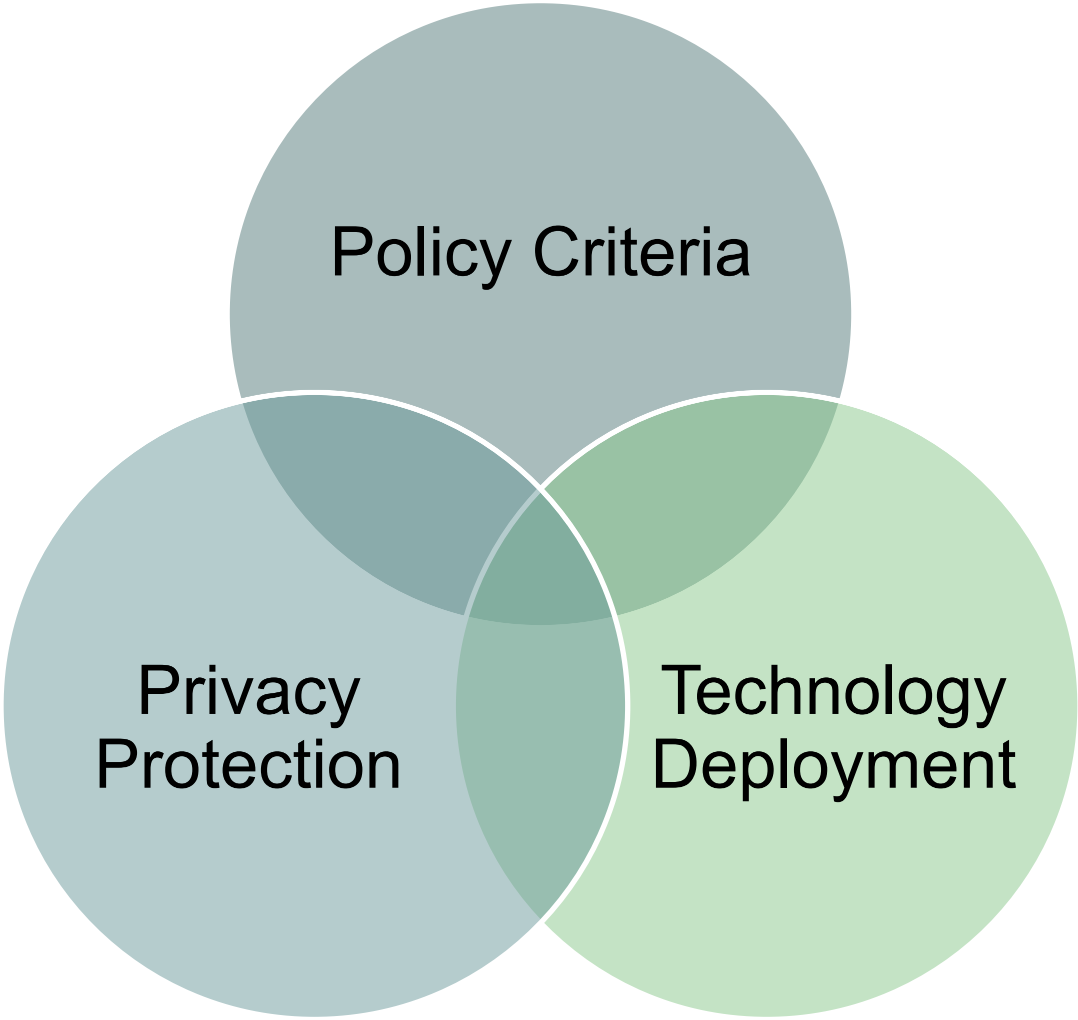
Trust Frameworks Overview

What are Trust Frameworks?

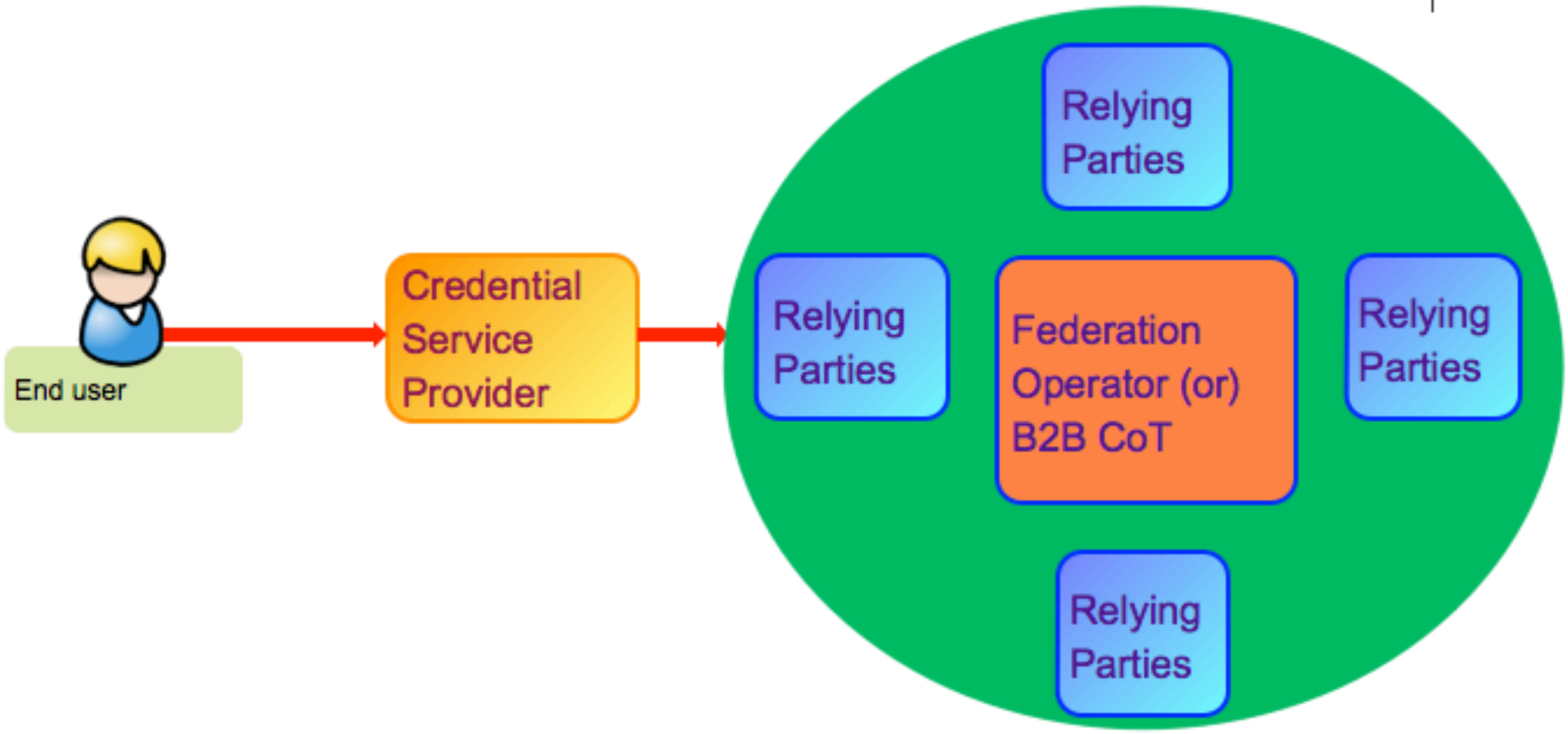
What do Trust Frameworks do?

The Trust Framework model enables internet scale interoperability and trust in entities and their authentication systems through trusted and certified credentials.

Three Main Components

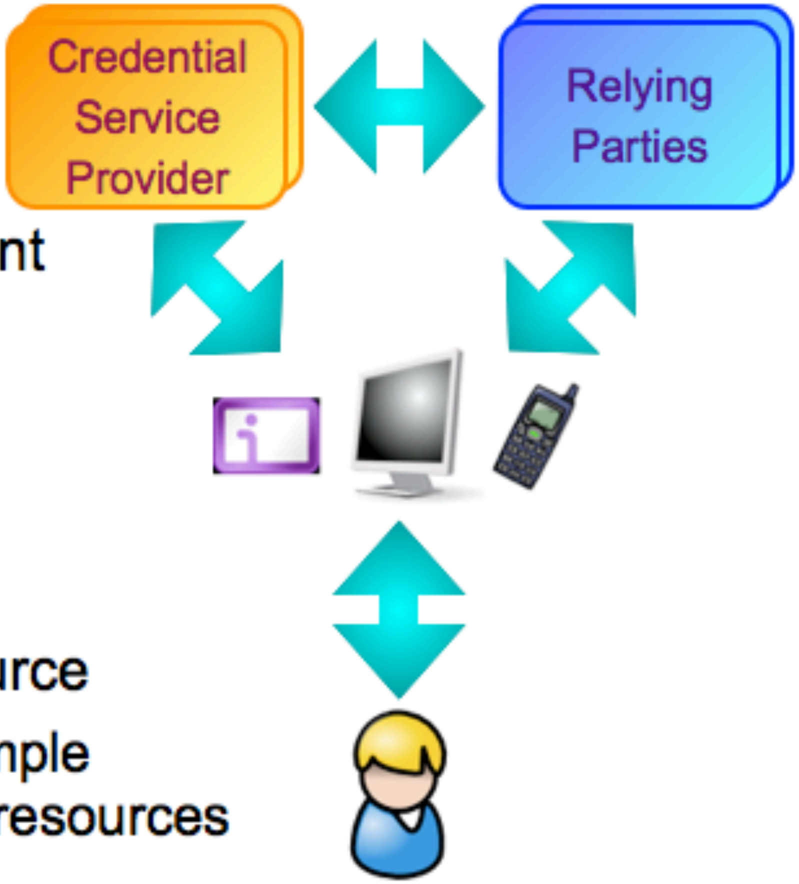


Identity Ecosystem: All About Trust



Federated Identity requires Technical <u>&</u> <u>Policy</u> *Interoperability*

- Credential Service Provider (CSP)
  - Identity Proofing
  - Credential Lifecycle Management
  - Operational Criteria for Trust
- Relying Party (RP)
  - Assesses Risk of Application
  - Complies with Best Practices
  - Provisions the Service or Resource
- User gets great experience: safe, simple access from any device to services/resources



kantara INITIATIVE

Interoperability & Assurance:

- **Technical Interoperability**
  - Does the system that authenticates me (vouches for me) “talk” to the systems that protect the resources I want to access?
- **Operational Interoperability via: Standard Assurance Levels**
  - Do the CSP and RP management entities “trust” each others' systems, operating procedures, vetting practices, audit reports, etc.?

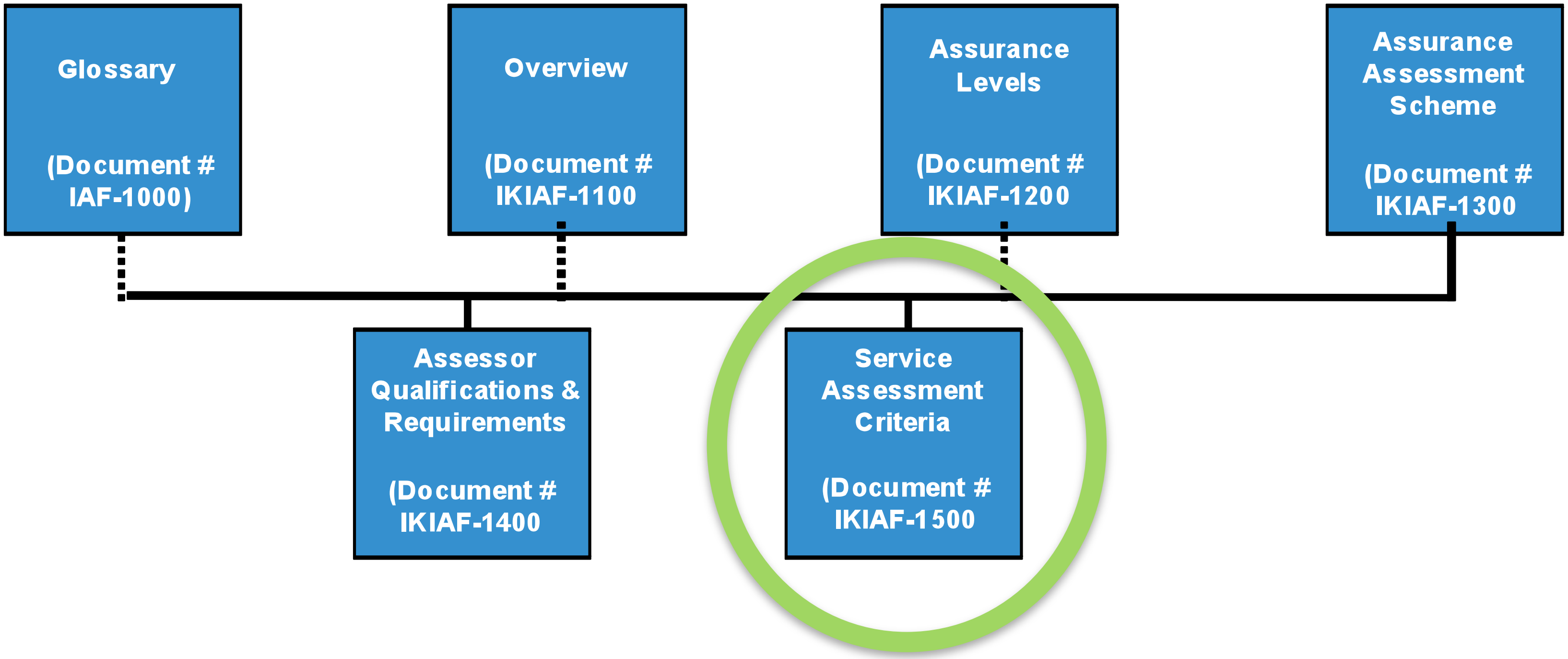
United States Government: Open Identity Solutions for Open Government (from GSA)

- The Open Identity Initiative seeks to leverage existing industry credentials for Federal use. The Initiative approves credentials for government use through our Trust Framework Providers who assess industry Identity Providers (IDPs).
- The Trust Framework Provider Adoption Process outlines the process that the ICAM community uses to sanctify organizations that assess commercial identity providers.

Kantara Initiative approach to Federated Identity

Identity Assurance Framework – one stop policy shop…

Identity Assurance Framework Components



Glossary

(Document # IAF-1000)

Overview

(Document # IKIAF-1100

Assurance Levels

(Document # IKIAF-1200

Assurance Assessment Scheme

(Document # IKIAF-1300

Assessor Qualifications & Requirements

(Document # IKIAF-1400

Service Assessment Criteria

(Document # IKIAF-1500

How to achieve operational interoperability at Internet scale

IdenTrust™
IDENTITY ASSURED

Federal Bridge Certification Authority
Access with Trust

ACES
Access Certificates for Electronic Services

ECA
External Certificate Authority

SAFE-BioPharma™
SAFE-BioPharma Association
Signatures and Authentication for Everyone

e-Authentication
SECURE GOVERNMENT ACCESS ONLINE

CertiPath

InCommon®

ICP Brasil
O Brasil na era da certificação digital

iDA
SINGAPORE

cofrac
Ministère de la Justice
www.cofrac.fr
la preuve de la compétence

DIRECTIVE 1999/93/EU

Real Casa de la Moneda
Fábrica Nacional de Moneda y Timbre
CERES

Bundesministerium für Wirtschaft und Technologie

How to achieve operational interoperability at Internet scale

Identity Assurance Framework

Kantara Initiative Accreditation and Certification

- Who should apply and how?
  - Assessors / Auditors
  - Credential Service Providers, Identity Providers

- For More Information
  - Visit our Assurance Certification Center: http://bit.ly/assurance_certification
  - Connect with me: joni@ieee-isto.org

What’s Next?

- Profiles, profiles and more profiles
  - Jurisdictional (governments), HealthCare, Financial, Telecommunications, etc
- Federation Interoperability Work Group (FIWG)
  - With input from international stakeholders FIWG developing tools for Federations to use for Interoperation.
  - Enabling communication of Meta-Data between Federations
  - Open for adoption by communities world-wide via Creative Commons IPR

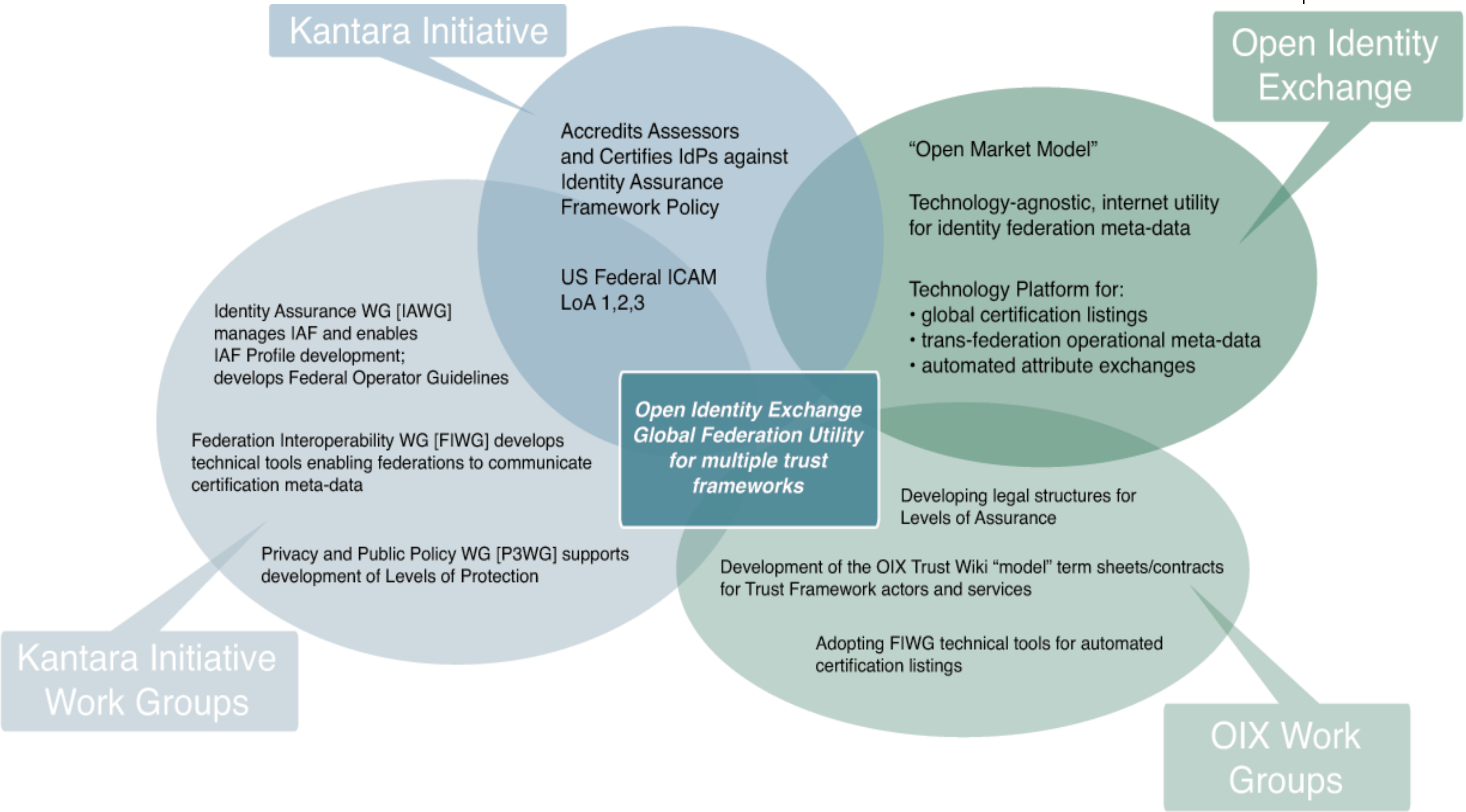
Benefits of Adoption

- US Government ICAM Adopted Level 1, 2, 3 non-crypto
- Identity Assurance Framework (IAF) is technology Agnostic
  - Can be adopted as organizational policy framework regardless of the technology protocol in place.
  - Lowers cost to jurisdictions and entities enabling eased transition in to Trust Framework Model
- Has Kantara Initiative international community input
  - Austria, Canada, Denmark, France, Japan, New Zealand, Sweden, United Kingdom, United States – the list keeps growing
- Enables Inter-federation through trusted and certified credentials
  - Could be applied across jurisdictional federations like the European Union.
- Enables Government entities to leverage private-sector activities

Working Together

Building Trust…

Collaboration



Kantara Initiative

Accredits Assessors and Certifies IdPs against Identity Assurance Framework Policy

US Federal ICAM LoA 1,2,3

Open Identity Exchange

"Open Market Model"

Technology-agnostic, internet utility for identity federation meta-data

Technology Platform for:

- global certification listings
- trans-federation operational meta-data
- automated attribute exchanges

Identity Assurance WG [IAWG] manages IAF and enables IAF Profile development; develops Federal Operator Guidelines

Federation Interoperability WG [FIWG] develops technical tools enabling federations to communicate certification meta-data

Privacy and Public Policy WG [P3WG] supports development of Levels of Protection

Kantara Initiative Work Groups

Open Identity Exchange Global Federation Utility for multiple trust frameworks

Developing legal structures for Levels of Assurance

Development of the OIX Trust Wiki "model" term sheets/contracts for Trust Framework actors and services

Adopting FIWG technical tools for automated certification listings

OIX Work Groups

Kantara Initiative Work Groups

Kantara Initiative –

Identity Assurance (IAWG)

http://kantarainitiative.org/confluence/display/idassurance/

eGovernment (eGovWG)

http://kantarainitiative.org/confluence/display/eGov/

Federation Interoperability

http://kantarainitiative.org/confluence/display/fiwg/

Privacy and Public Policy (P3WG)

http://kantarainitiative.org/confluence/display/p3wg/

Open Identity Exchange (OIX) Work Groups

Telco Data Work Group

Verizon, AT&T, TNS, Pacific East, etc.

Public Media

National Public Radio, Public Broadcasting Service, etc.

Librarians, Authors, Publishers

National Institute of Health, National Library of Medicine, ORCID, APA, etc

Identity Attributes Trust Framework

Google, Yahoo!, AOL, Hot Mail, etc.

OIX/Kantara Collaborative Work Groups

US ICAM Higher Levels of Assurance

OIX, KI, US GSA, US NIH, etc.

- *A public private partnership to define new technical /policy profiles for higher levels of assurance (NIST LoA 2 and 3)*
- *A forum and forcing function to map policy and legal issues to government and citizen interaction over the web*
- *A collaboration among leading industry organizations to break new ground in trust framework development*

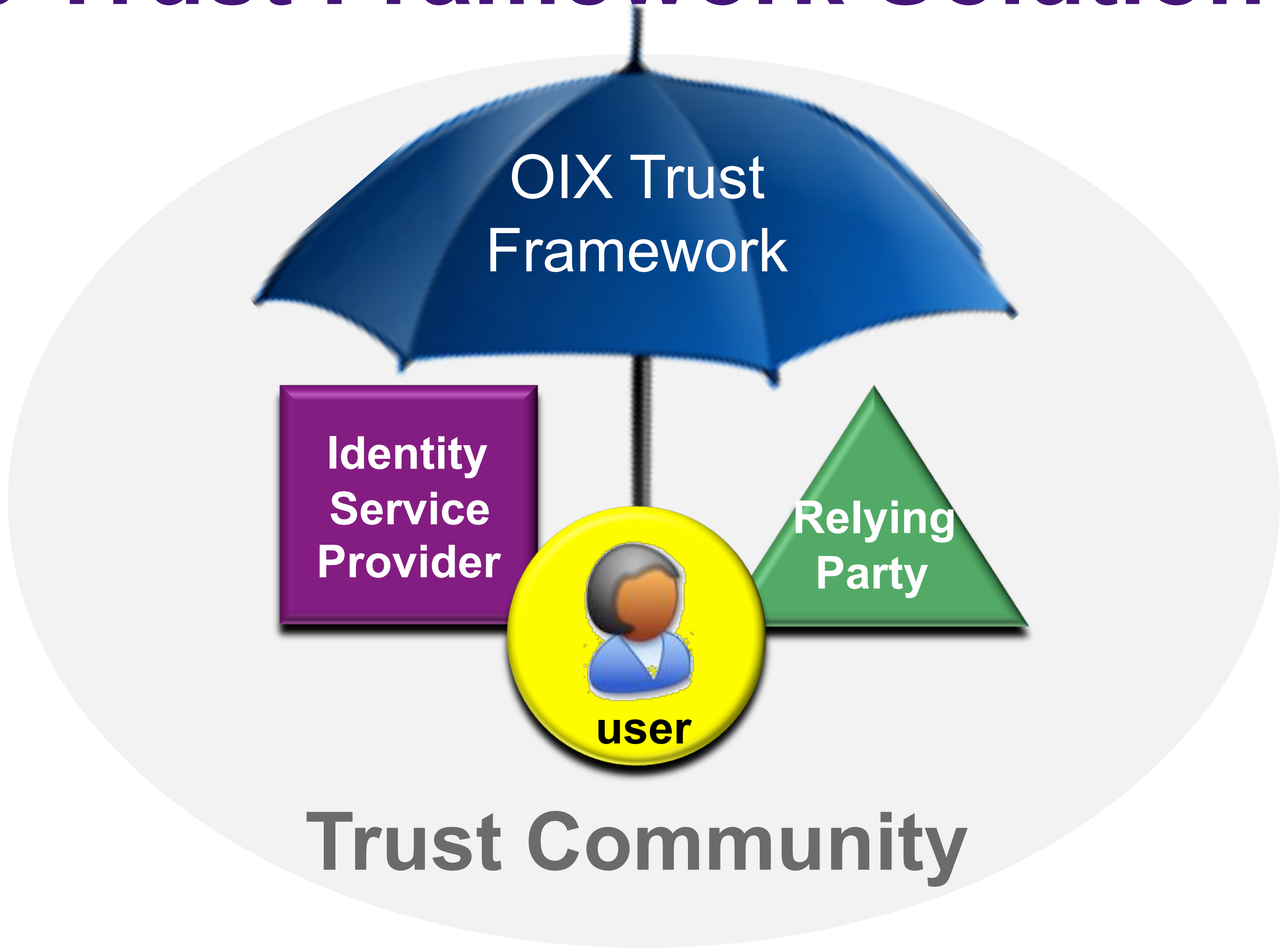
Introduction to OIX

A Market Solution to Online Identity Trust…

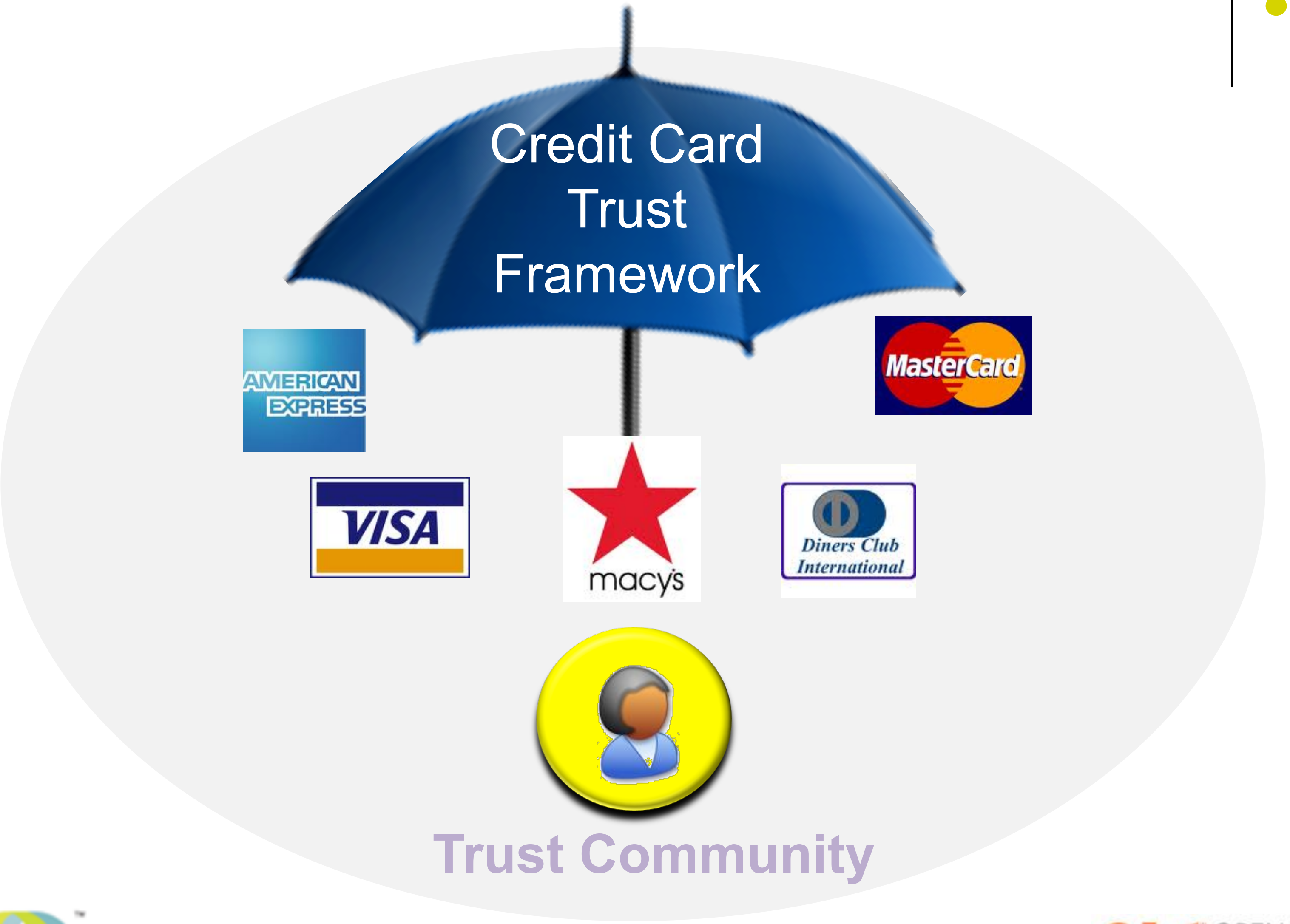
A Matter of Trust

- Relying Parties must be able to trust that the Identity Provider is providing accurate customer data
- Identity Providers must be able to trust that the Relying Party is legitimate (i.e., not a hacker, phisher, etc)
- Direct RP-to-IDP trust agreements are a common solution, but are impossible to manage at Internet scale

The Trust Framework Solution



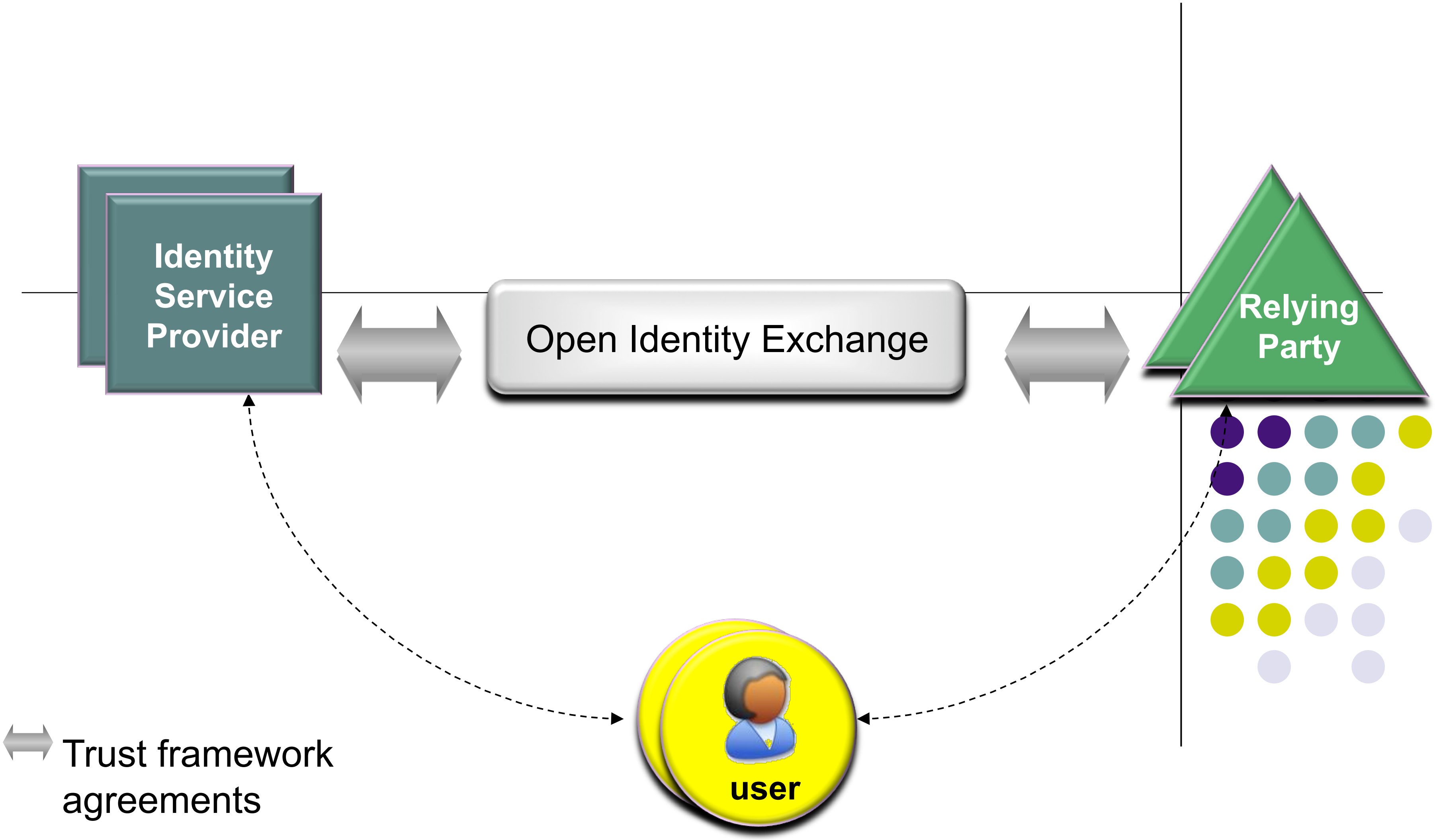
Proven Trust Frameworks Exist!



Credit Card Trust Framework

Trust Community

The OIX Identity Trust Framework Model



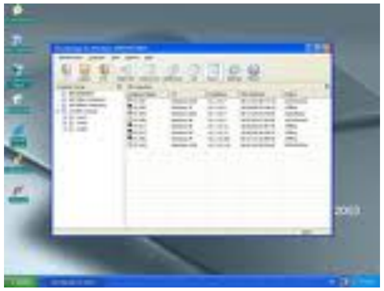
⟺ Trust framework agreements

kantara INITIATIVE

OIX OPEN IDENTITY EXCHANGE

What OIX Provides

- Referee
  - Neutral, technology agnostic provider of trust frameworks



- Certification Listing Service
  - Machine-readable information about trust framework participants and certifications

kantara INITIATIVE

OIX OPEN IDENTITY EXCHANGE

OIX Drives Adoption

- By improving market efficiency
- By providing openness and transparency
- By ensuring credibility and accountability in the system
- By enabling improved user experience

Real World Examples

- OIX U.S. ICAM (Identity, Credential, and Access Management) Trust framework
  - For U.S. federal government agencies
- OIX Telecom Data Trust Framework
  - For Telco Data Services providers
  - For Data Aggregators

Summary

OIX and KI work together to provide an Internet-scale solution to enable trusted online digital identities

Thank You!

Get in touch…

Joni@kantarainitiative.org