The Role of Strong Authentication in the Identity Assurance Ecosystem

Strong Authentication Summit
BrightTALK.com

Brett McDowell, Executive Director, Kantara Initiative

kantara™ INITIATIVE

The case for Strong Authentication in Federated Identity

ATM Historic Analogy

Step 1 Step 2 Step 3

Separate Cards with Each Bank

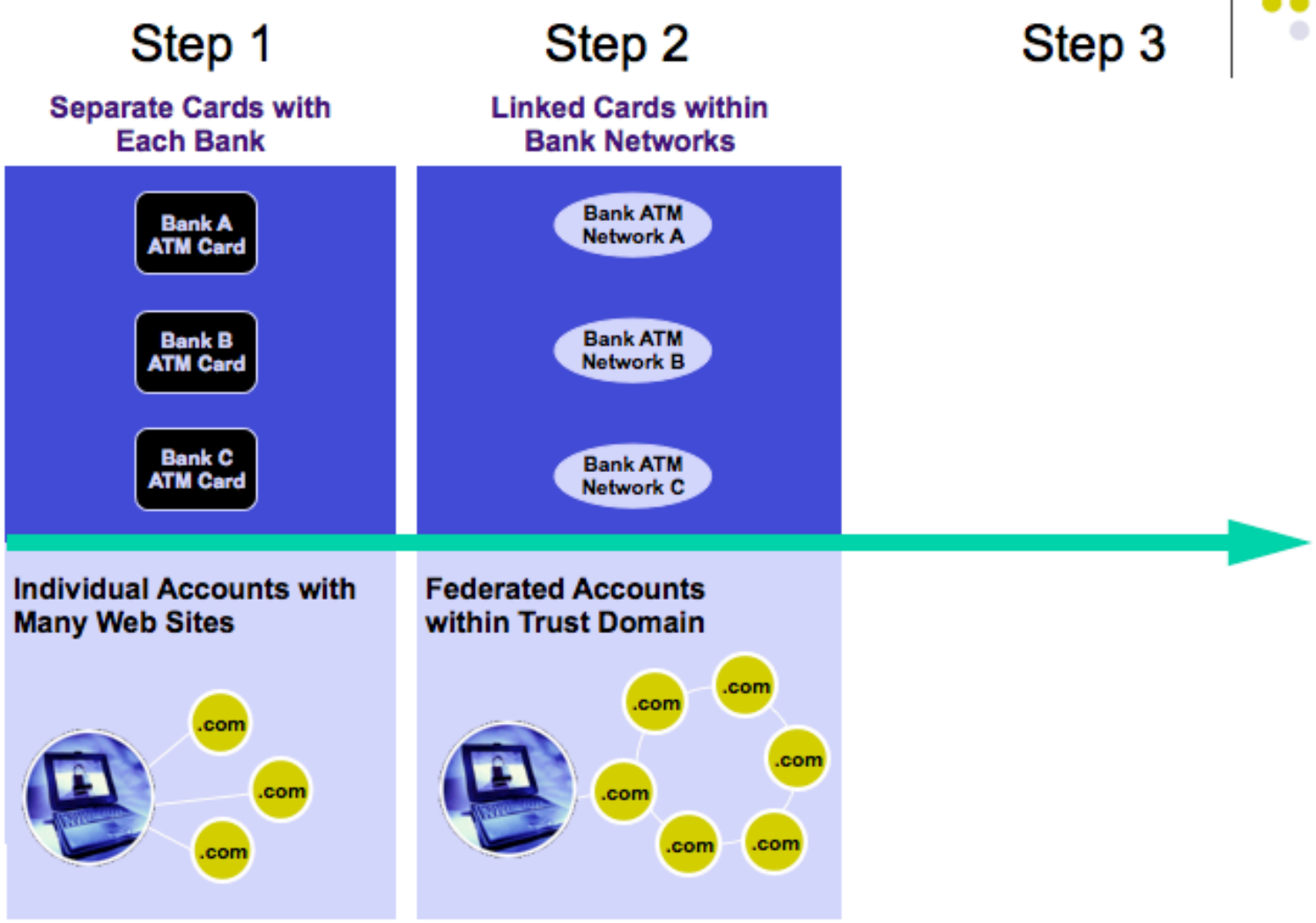
Bank A ATM Card

Bank B ATM Card

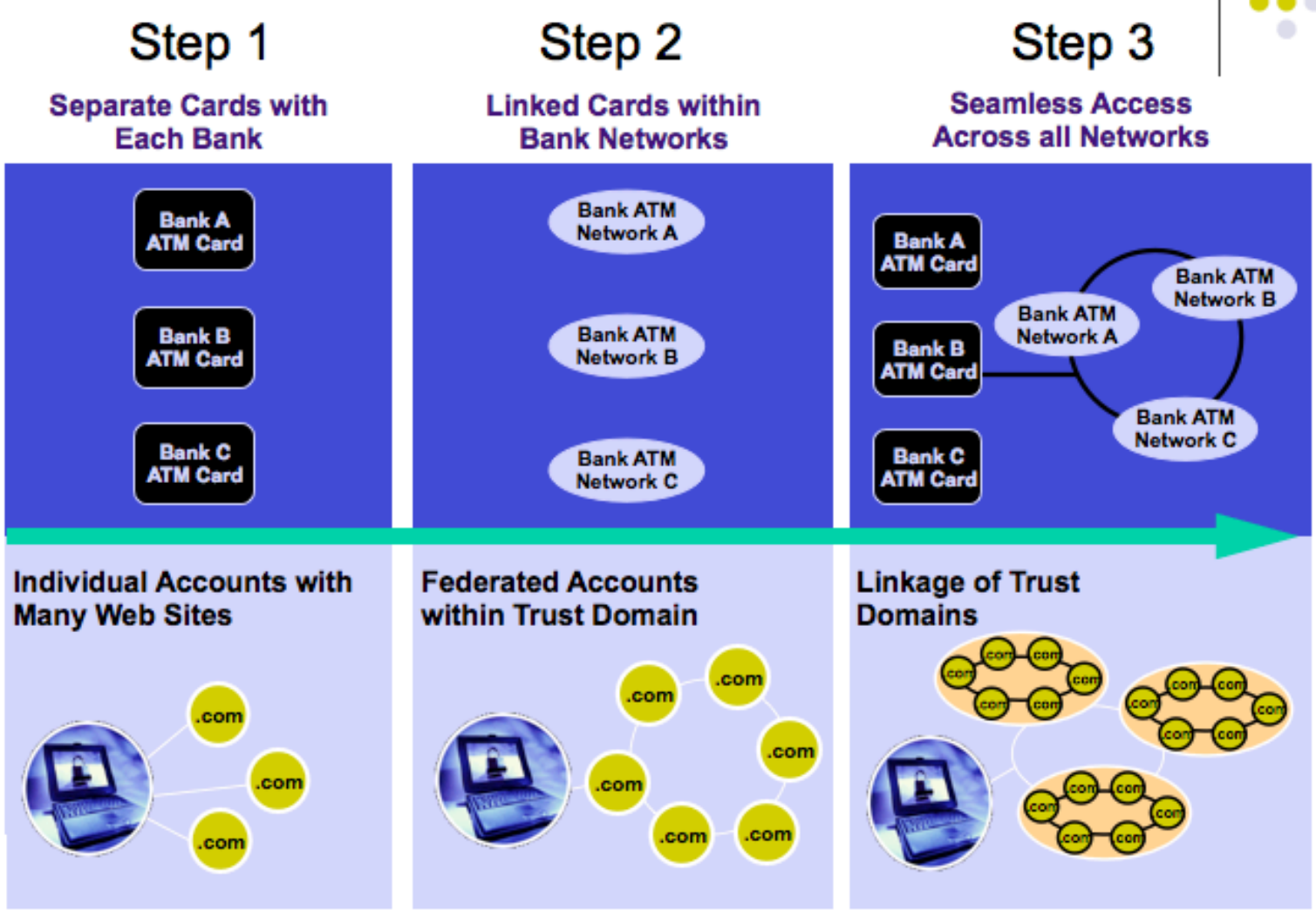
Bank C ATM Card

Individual Accounts with Many Web Sites

ATM Historic Analogy



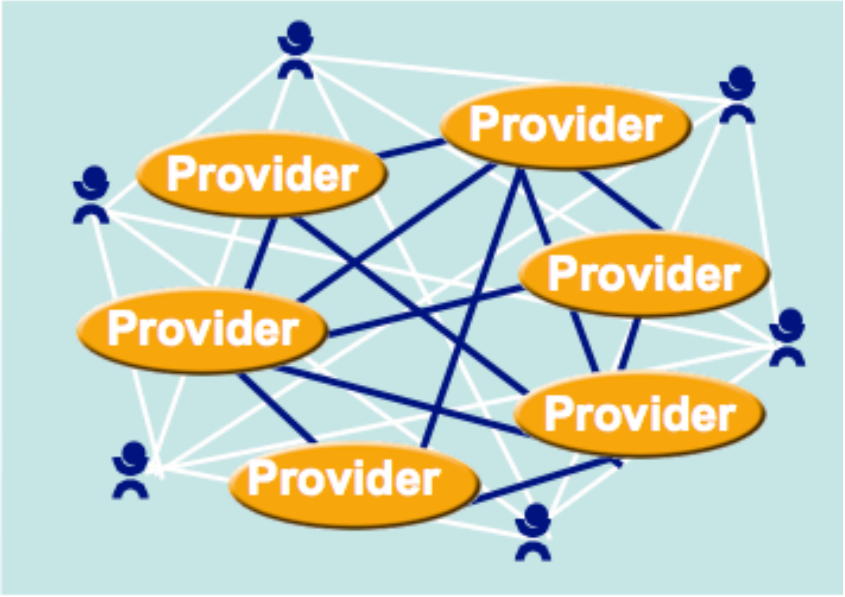
ATM Historic Analogy



Strong AuthN enables an Open Federated Model

Open Federated Model

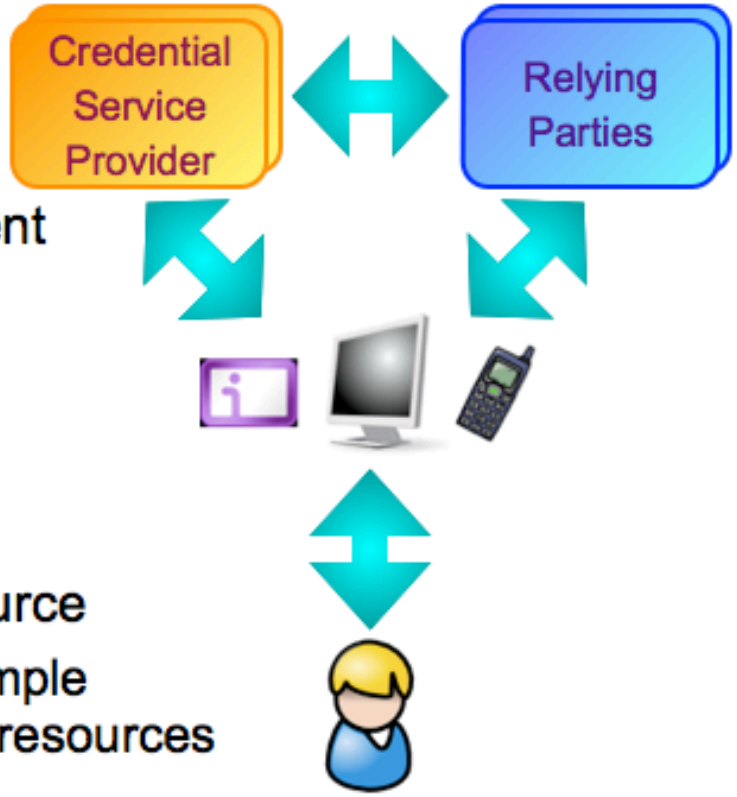
- User information is already in various locations
- No centralized control
- No single point of failure
- The user can use their credentials to receive services anywhere the credential is accepted



kantara INITIATIVE

Federated Identity requires Technical & Policy *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

Removing Barriers to Implementing Federated Identity

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.?

The Interoperability challenge: Identity Standards Landscape in 2008

- Several successful organizations addressing important aspects of the Federated Identity ecosystem
- Varying structures, participation rules, IPR licensing and specification & open source output
- "Best-of-the-best" in Federated Identity management was happening piecemeal, without systemic coordination

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

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

Industry Response: 80+ members in first 100 days

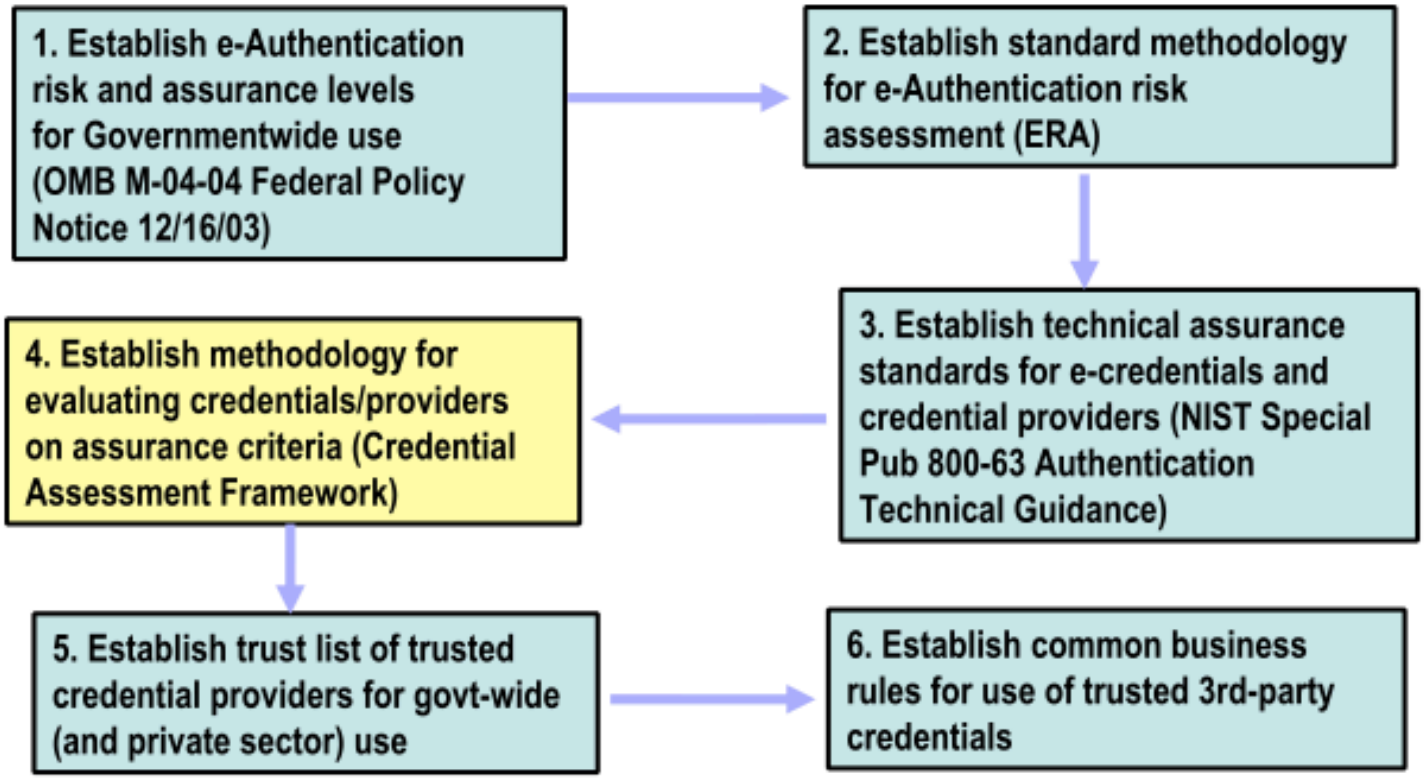
Kantara Initiative Groups

Group	Charter
Concordia DG	charter
Identity Community Update DG	charter
Japan DG	charter
Clients WG	charter
Consumer Identity WG	charter
eGovernment WG	charter
Health Identity Assurance WG	charter
Identity Assurance	charter
IdP Selection WG	charter
ID-WSF Evolution WG	charter
Japan WG	charter
Privacy and Public Policy WG	charter
Universal Login Experience WG	charter
User Driven Volunteered Personal Info WG	charter
User Managed Access WG	charter

http://kantarainitiative.org/wordpress/groups/

The US Government Approach to Federated Identity

United States history with Federated IdM (from GSA)



What's Next for US Government IdM (from GSA)

- Government-wide Identity has been Re-organized…
- CIO Council
  - Information Security & Identity Management (ISIMC)
    - Identity, Credential and Access Management Subcommittee (ICAMSC)
      - E-Authentication, FPKI, and HSPD-12 Consolidated under ICAM
      - OMB 04-04 and NIST 800-63 unchanged, still in effect
      - Chaired by Judy Spencer GSA/OGP and Paul Grant, DoD
- Moving toward Adoption of Industry Trust Frameworks
  - Industry alternatives to the CAF that are *comparable* can be adopted
    - Industry IDPs, Industry Trust Frameworks, Industry Auditors

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

US Trust Framework Program (www.idmanagement.gov)

Trust Framework Providers:

- Kantara Initiative - Application submission under review
- OpenID Foundation - Draft submission under review
- InfoCard Foundation - Draft submission under review
- InCommon Federation - Draft submission under review

The Scheme Adoption Process outlines the process that the ICAM community uses to develop and/or approve specification profiles for achieving portable identity over the Internet.

Adopted Schemes:

- ICAM OpenID 2.0 Profile - Fully adopted
- Kantara SAML 2.0 eGovernment Profile - Fully adopted
- ICAM IMI 1.0 Profile - Fully adopted
- ICAM WS-Federation - In development

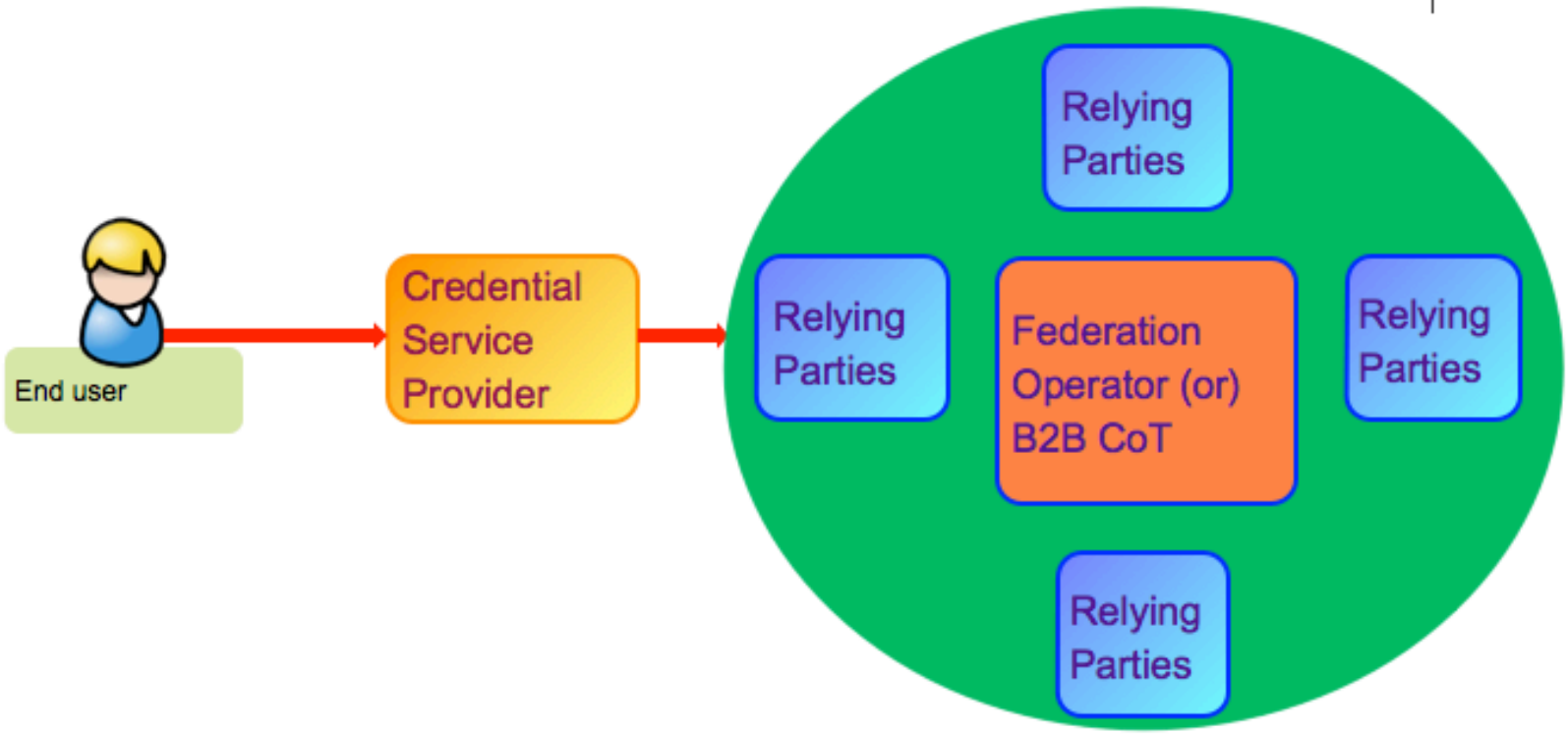
Identity Providers:

- Google - OpenID Foundation, Pilot assessment with NIH in progress
- Yahoo - OpenID Foundation, Pilot assessment in progress
- PayPal - InfoCard Foundation, Pilot assessment in progress
- Wave

kantara INITIATIVE

Kantara Initiative's Identity Assurance Certification Program

Identity Ecosystem: All About Trust



How to achieve operational interoperability at Internet scale

IdenTrust
IDENTITY ASSURED

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

Federal Bridge Certification Authority
Access with Trust

ACES
Access Certificates for Electronic Services

ECA
External Certificate Authority

Authentication
SECURE GOVERNMENT ACCESS | ONLINE

CertiPath

InCommon

ICP Brasil
O Brasil na era da certificação digital

iDA
SINGAPORE

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

IdenTrust
IDENTITY ASSURED

Federal Bridge Certification Authority

ACES
Access Certificates for Electronic Services

SAFE-BioPharma
SAFE-BioPharm
Signatures and Authen

kantara INITIATIVE

Identity Assurance Framework

thentication
GOVERNMENT ACCESS | ONLINE

CertiPath

InCommon

ICP Brasil
O Brasil na era da certificação digital

cofrac
MINISTÈRE DE LA JUSTICE
www.cofrac.fr
la preuve de la compétence

DIRECTIVE 1999/93/EU

iDA
SINGAPORE

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

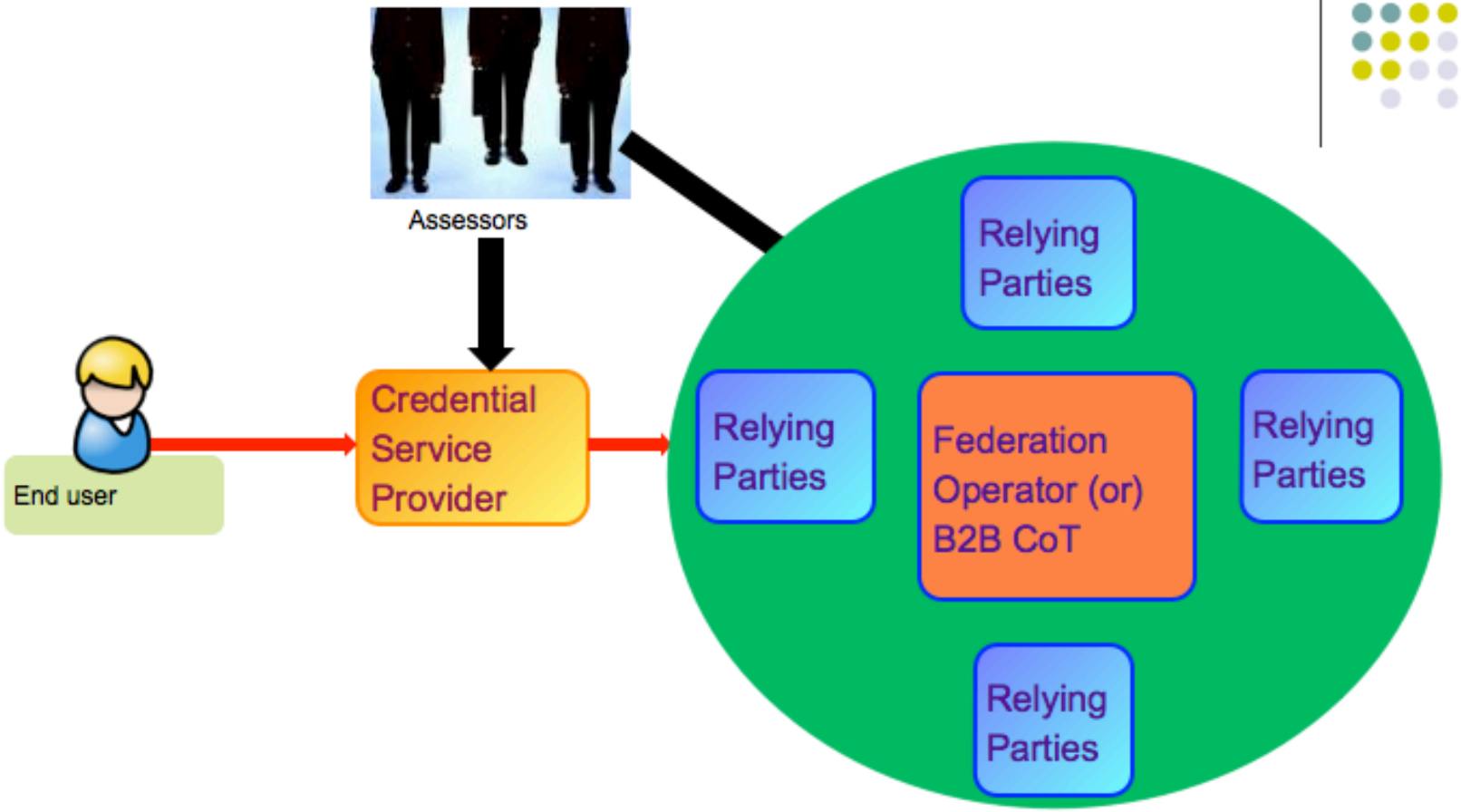
Bundesministerium
für Wirtschaft
und Technologie

IAF Assurance Levels Illustrated

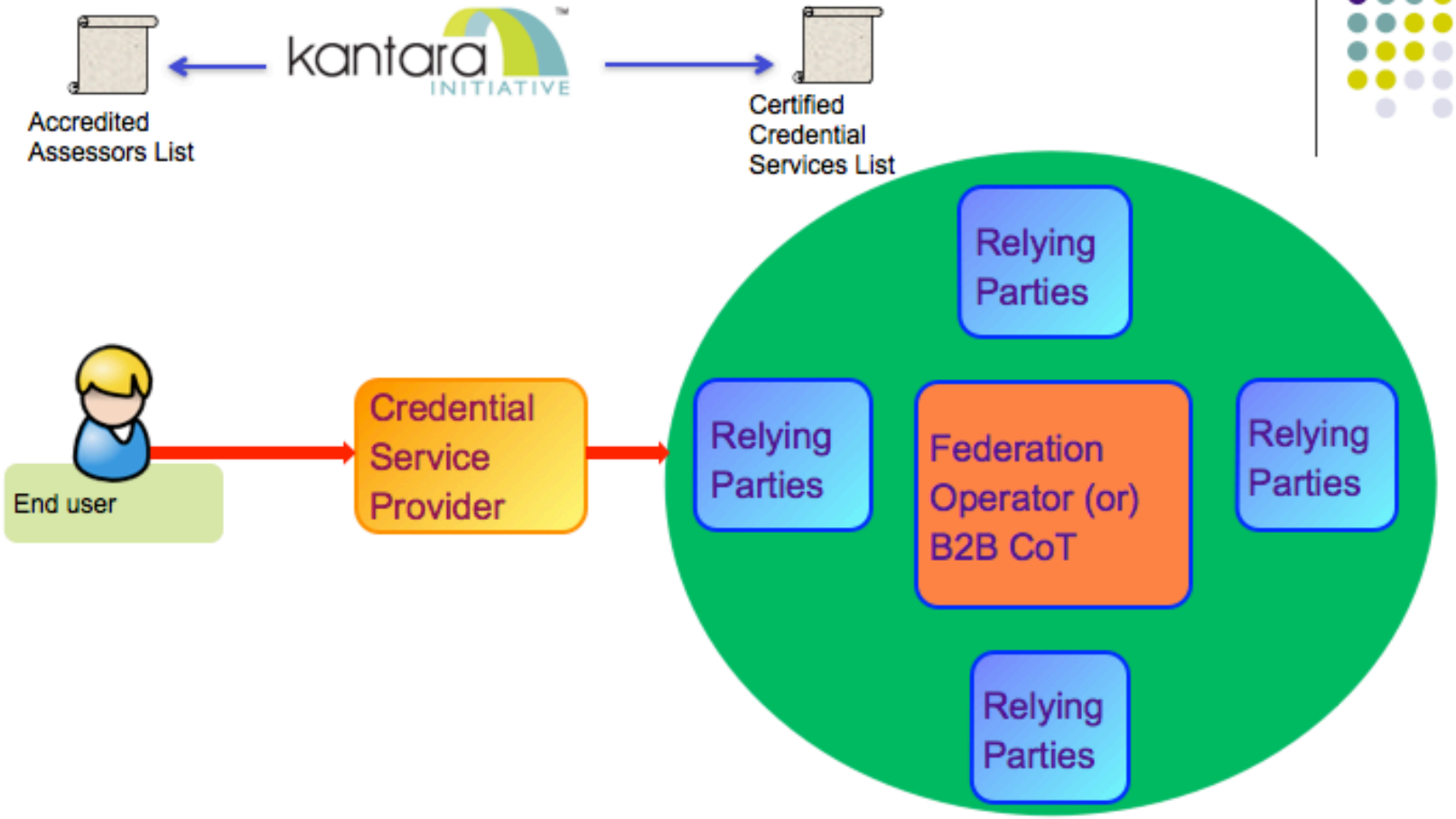
Assurance Level	Example	Assessment Criteria – Organization	Assessment Criteria – Identity Proofing	Assessment Criteria – Credential Mgmt
AL 1	Registration to a news website	Minimal Organizational criteria	Minimal criteria - Self assertion	PIN and Password
AL 2	Change of address of record by beneficiary	Moderate organizational criteria	Moderate criteria - Attestation of Govt. ID	Single factor; Prove control of token through authentication protocol
AL 3	Access to an online brokerage account	Stringent organizational criteria	Stringent criteria – stronger attestation and verification of records	Multi-factor auth; Cryptographic protocol; "soft", "hard", or "OTP" tokens
AL 4	Dispensation of a controlled drug or $1mm bank wire	Stringent organizational criteria	More stringent criteria – stronger attestation and verification	Multi-factor auth w/hard tokens only; crypto protocol w/keys bound to auth process

Note: Assurance level criteria as posited by the OMB M-04-04 & NIST SP 800-63

Identity Ecosystem: Assessing Trust



Identity Ecosystem: Certifying Trust



Getting Involved

Website

http://kantarainitiative.org/

Community mail list

http://kantarainitiative.org/mailman/listinfo/community_kantarainitiative.org

Identity Assurance Certification Program

http://kantarainitiative.org/confluence/display/certification/Identity+Assurance+Certification+Program

Membership documents

http://kantarainitiative.org/wordpress/?page_id=8

E-mail Brett McDowell

email@brettmcdowell.com

kantara™ INITIATIVE