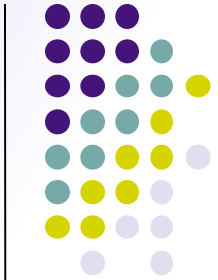


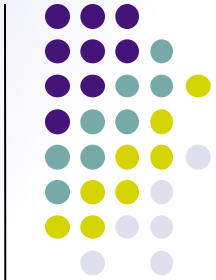
kantara INITIATIVE

Trust Frameworks: Tools to build Identity Ecosystems

It takes a village!

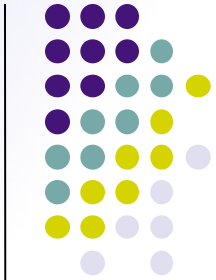
support@kantarainitiative.org)

Agenda:



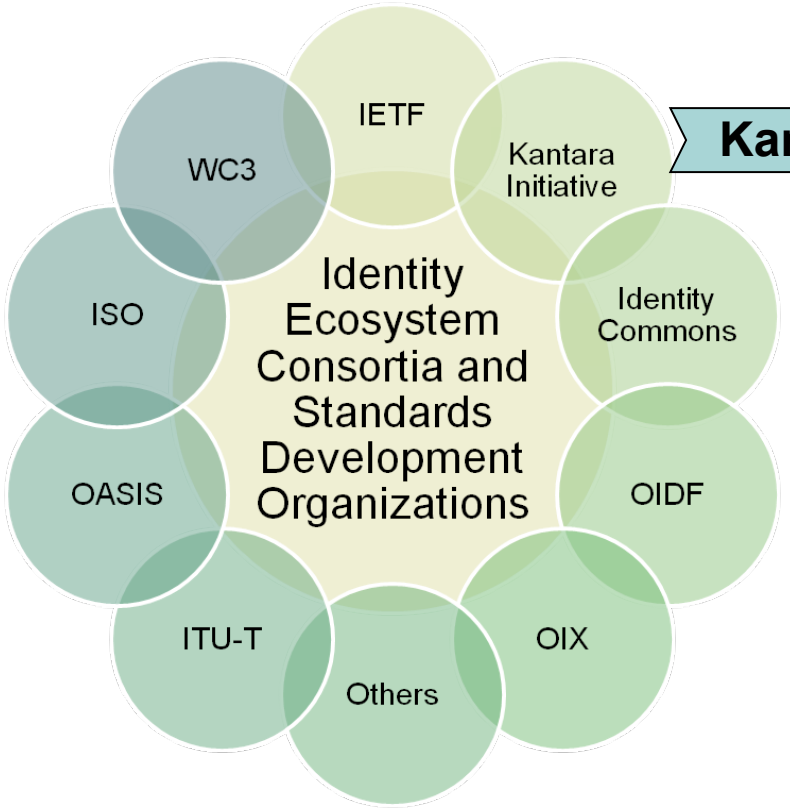
- Overview of Kantara Initiative
- Federation and Trust Frameworks
- Identity Assurance Framework
- Accreditation / Certification
- Next Steps

Kantara Initiative: Overview
Values



- **Trust:**
  Operating Accreditation, Approval and Certification programs to ensure trusted network environments are available to support generative growth within the Internet.
- **Privacy:**
  Developing solutions for secure, identity-based, privacy-respecting online interactions.
- **Community:**
  Bridging technologies and policies to harmonize effective solutions related to online identity.

Kantara Initiative: Overview
Federation, Compliance, and Interoperability

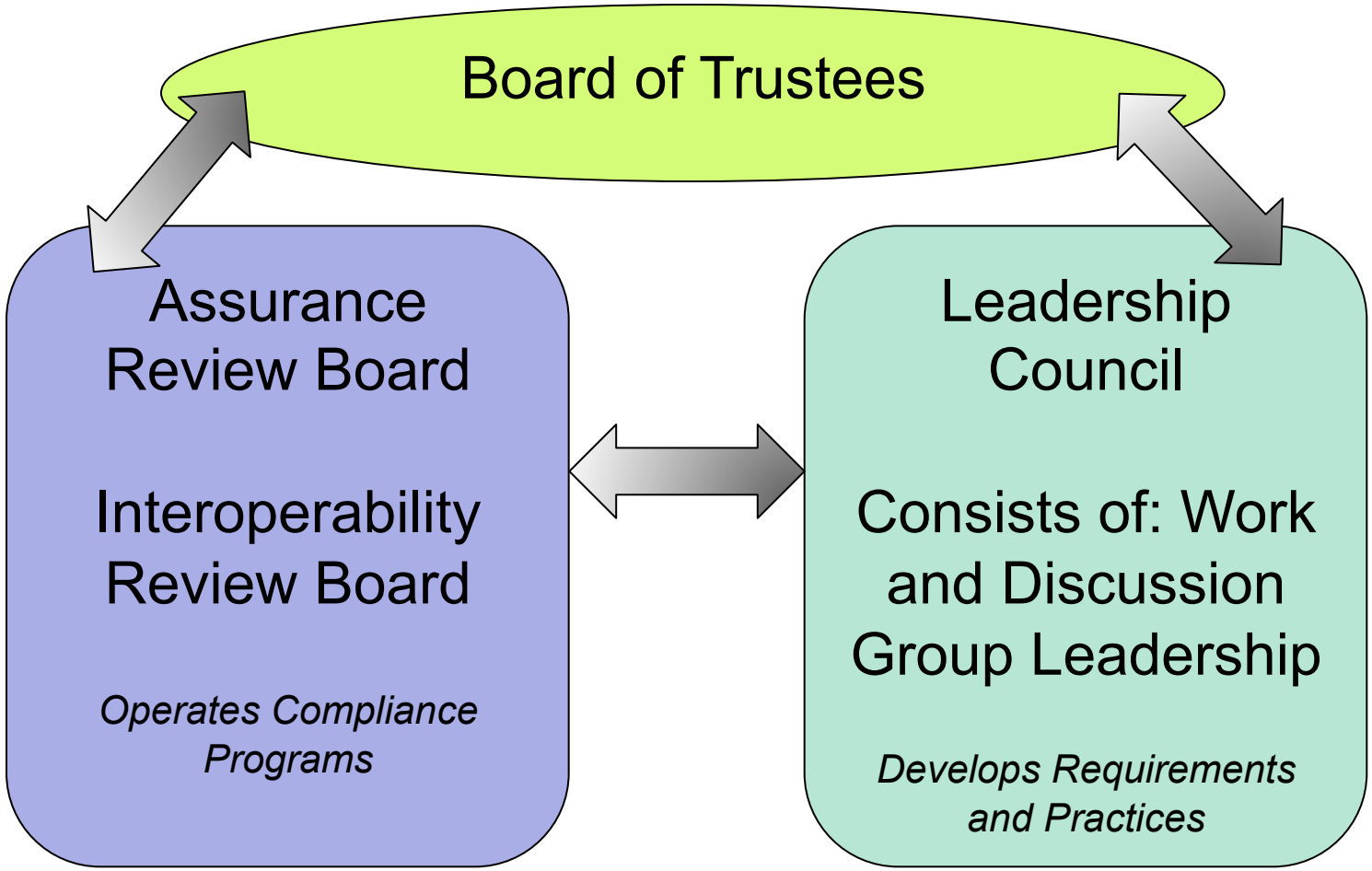


Kantara Builds Bridges

Focus on the **harmonization** of existing and evolving solutions.

Operating compliance programs for **multiple solutions** that fit a variety of requirements and jurisdictions.

Kantara Initiative: Overview
Governance Model



Trustees

Government Facing

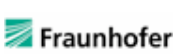
Government of Canada

Credential Services

Verticals - Health, Telco, Entertainment, Finance

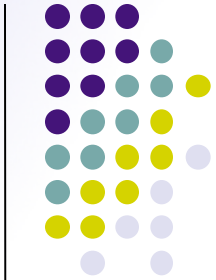
Audit and Testing

Research and Education



Technical and User Community Organizations

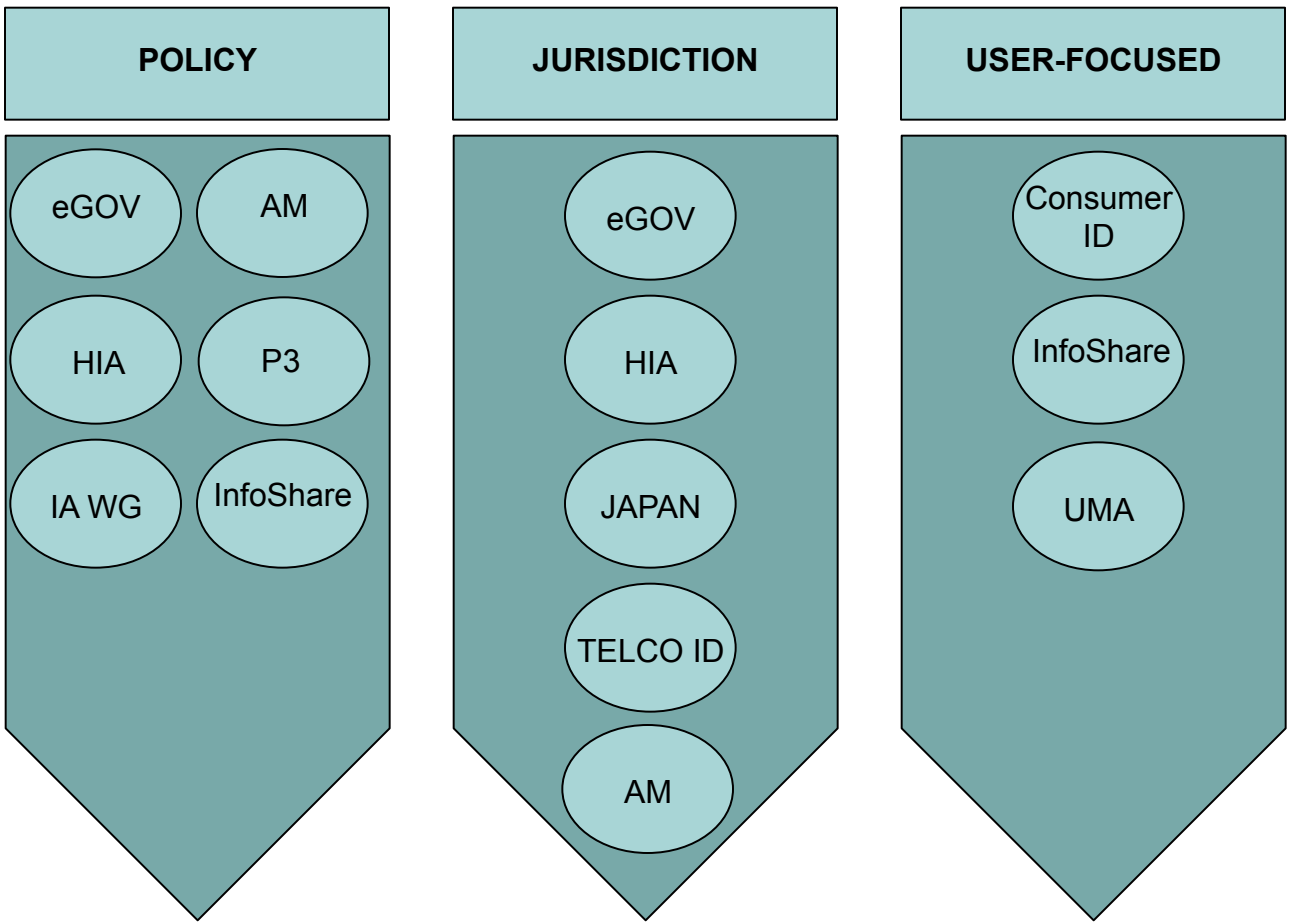
Kantara Initiative: Overview
Liaisons and Governments



- ISO: 29115, 29100, 29191, 27001, 27002, etc
- ITU-T: X.1254 (was X.EAA), OITF
- OASIS: eGovernment, SAML SSTC, etc
- OECD Internet Technical Advisory Committee (ITAC)
- Governments:
  - Providing neutral forum for Government Programs and Agencies to share information and identify common goals
  - Performing confidential and non-confidential program reviews upon request for specific international governments and government agencies

Kantara Initiative: Overview
Work and Discussion Groups

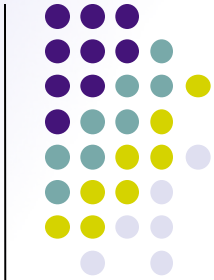
KANTARA INITIATIVE WORK AND DISCUSSION GROUPS



WORK & DISCUSSION GROUP ACRONYMS:

- (AM) Attribute Management
- (BCTF) Business Cases for Trusted Federations
- (Consumer ID) Consumer Identity
- (eGOV) eGovernment
- (FI) Federation Interoperability
- (HIA) Heath Identity Assurance
- (IA) Identity Assurance
- (Info Sharing WG) Information Sharing
- (Japan) Japan
- (P3) Privacy and Public Policy
- (Telco ID) Telecommunication Identification
- (UMA) User Managed Access

Kantara Initiative: Overview
Groups and Programs



KANTARA INITIATIVE PROGRAMS

COMPLIANCE and CERTIFICATION

INTEROPERABILITY

Interop Review Board (IRB)

- Certification, Verification
- Tools, Demos

- eGOV
- FI
- OSSI

ASSURANCE

Assurance Review Board (ARB)

- Certification
- Accreditation

- HIA
- IA
- InfoShare
- P3

NON-CERTIFICATION

HARMONIZATION

User-Centric, Jurisdiction and Vertical Based

- Consumer ID
- Japan
- Telco ID
- UMA

WORK & DISCUSSION GROUP ACRONYMS:

- (BCTF) Business Cases for Trusted Federation
- (eGOV) eGovernment
- (FI) Federation Interoperability
- (IOP) Interoperability
- (HIA) Heath Identity Assurance
- (IA) Identity Assurance
- (Info Sharing) Information Sharing
- (OSSI) Open Source Strategic Initiative
- (P3) Privacy and Public Policy
- (Consumer ID) Consumer Identity
- (Japan) Japan
- (Telco ID) Telecommunication Identification
- (UMA) User Managed Access

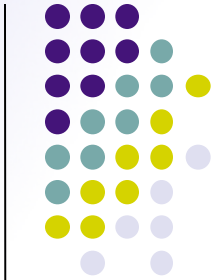
Federation and Trust Frameworks
Federation Good

What is good?

- Strengthening communities
- Opening of new markets
- Enhanced privacy for end users
- More and better services to the users
- Re-use of user names and passwords

Source: http://www.apan.net/meetings/Sydney2010/Session/Slides/Middleware/APAN29_interfederation-Simeonsen.pdf

Federation and Trust Frameworks
Federation Bad



What is bad?

- Lingua franca for inter-federation? SAML2?
- How to announce new services?
- Legal stuff...

Source: http://www.apan.net/meetings/Sydney2010/Session/Slides/Middleware/APAN29_interfederation-Simeonsen.pdf

Federation and Trust Frameworks
Federation Ugly

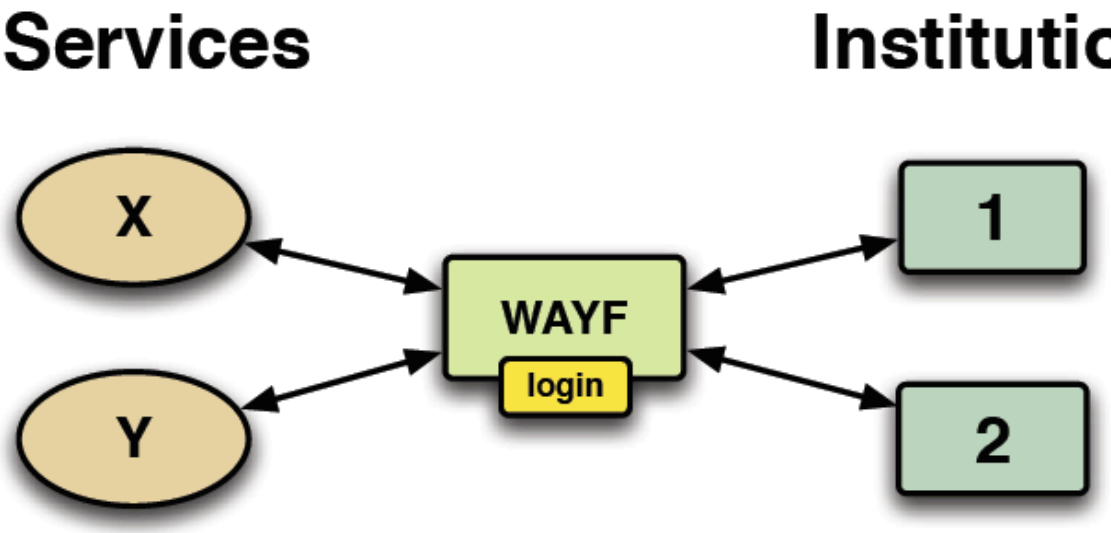
What is ugly?

- Identity-management requirements
- Semantics
- SAML2 interoperation profiles (saml2int.org) no longer 'just' Shibboleth

Source: http://www.apan.net/meetings/Sydney2010/Session/Slides/Middleware/APAN29_interfederation-Simeonsen.pdf

Federation and Trust Frameworks
What does Federation look like?

Hub-and-spoke, central login



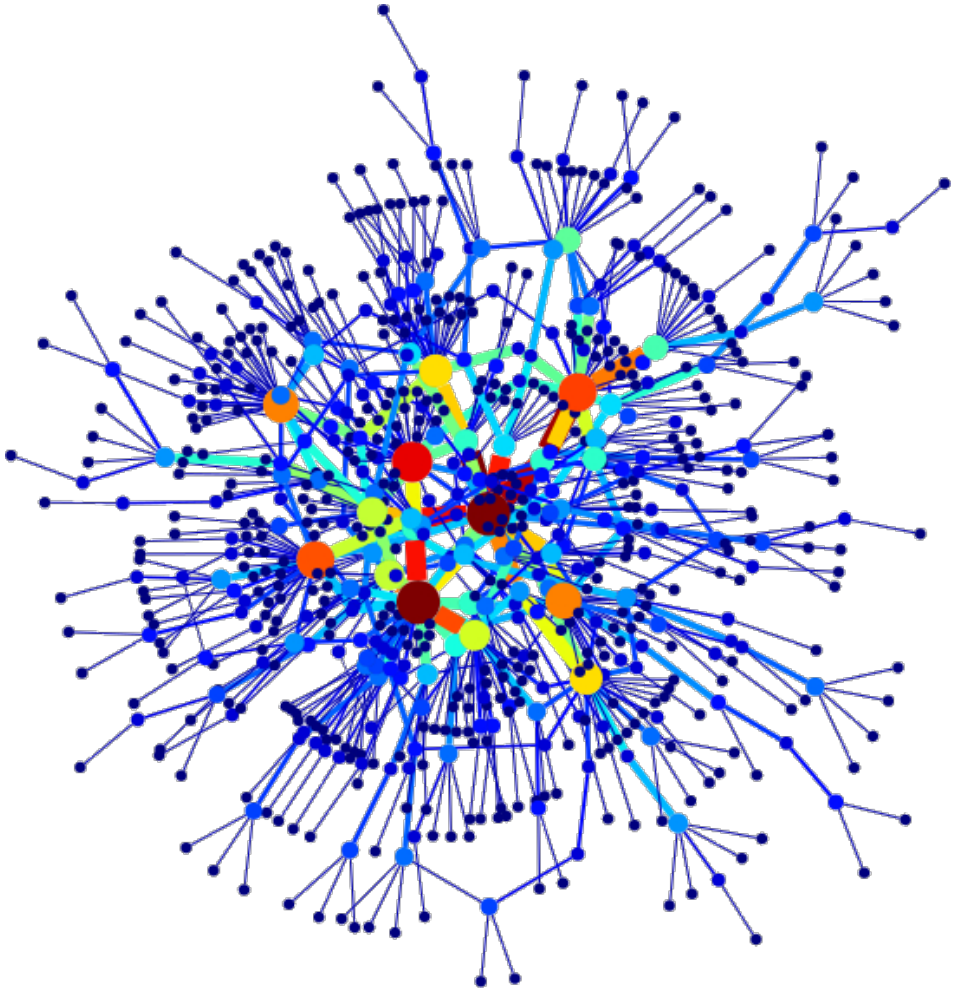
Source: http://www.apan.net/meetings/Sydney2010/Session/Slides/Middleware/APAN29_interfederation-Simeonsen.pdf

Federation and Trust Frameworks
What does Federation look like?

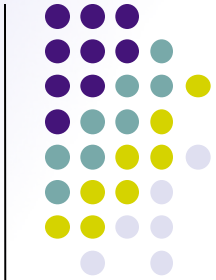
Source: http://www.apan.net/meetings/Sydney2010/Session/Slides/Middleware/APAN29_interfederation-Simeonsen.pdf

Federation and Trust Frameworks
Leveraging Scale-Free Networks

"Inter-Federation"



Federation and Trust Frameworks
Target Audience & Value Proposition



Target Audience

- Enable **End-users (Enterprise, Governments, Communities)** to **trust** credentials issued by **Identity Providers / Credential Service Providers**

Value Proposition

- Increased security
- Compliance with laws, regulations, and standards
- Improved interoperability
- Enhanced customer service
- Elimination of redundancy
- Increase in protection of Personally Identifiable Information (PII)

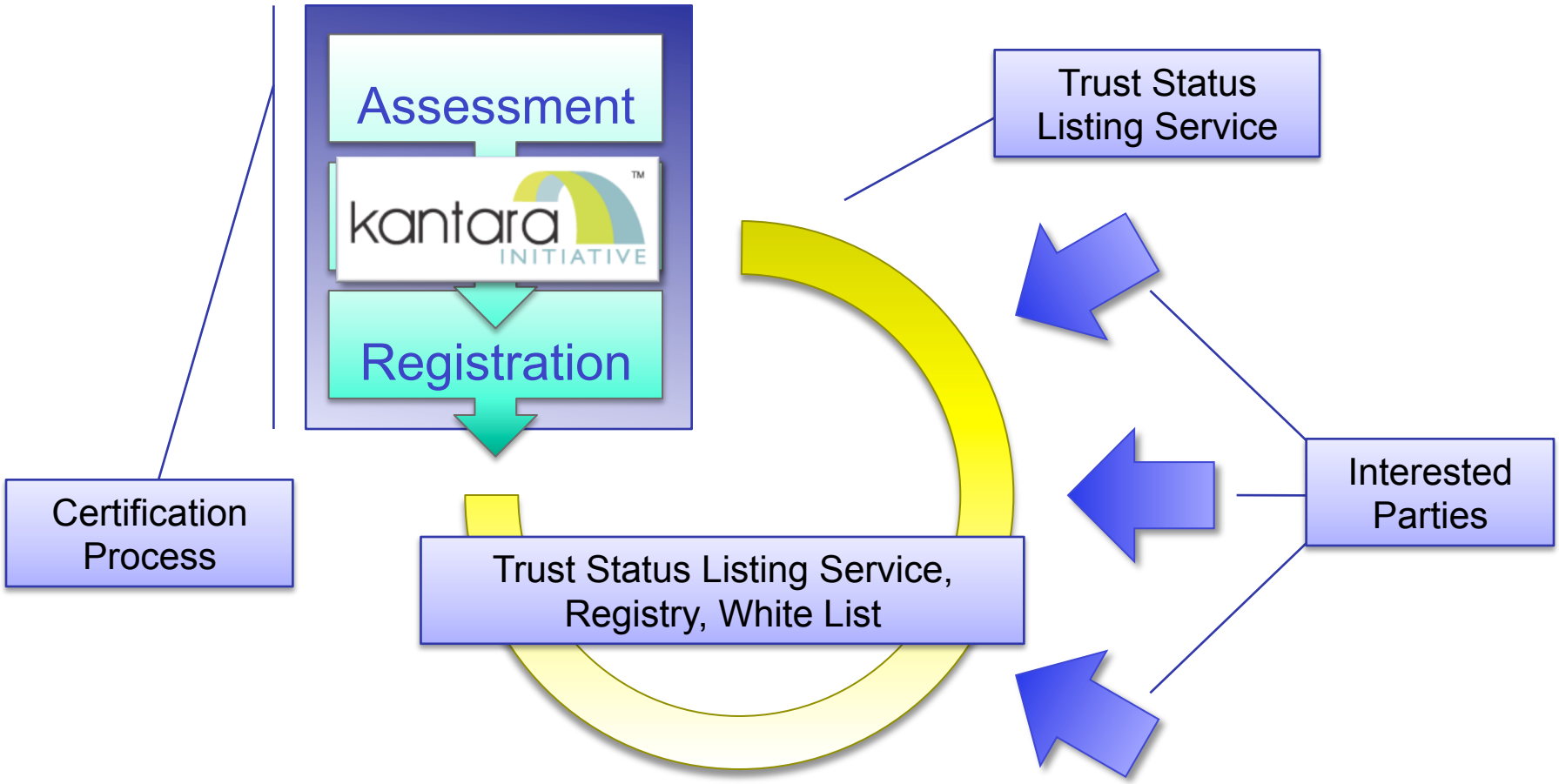
Federation and Trust Frameworks

Levels of Assurance : 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

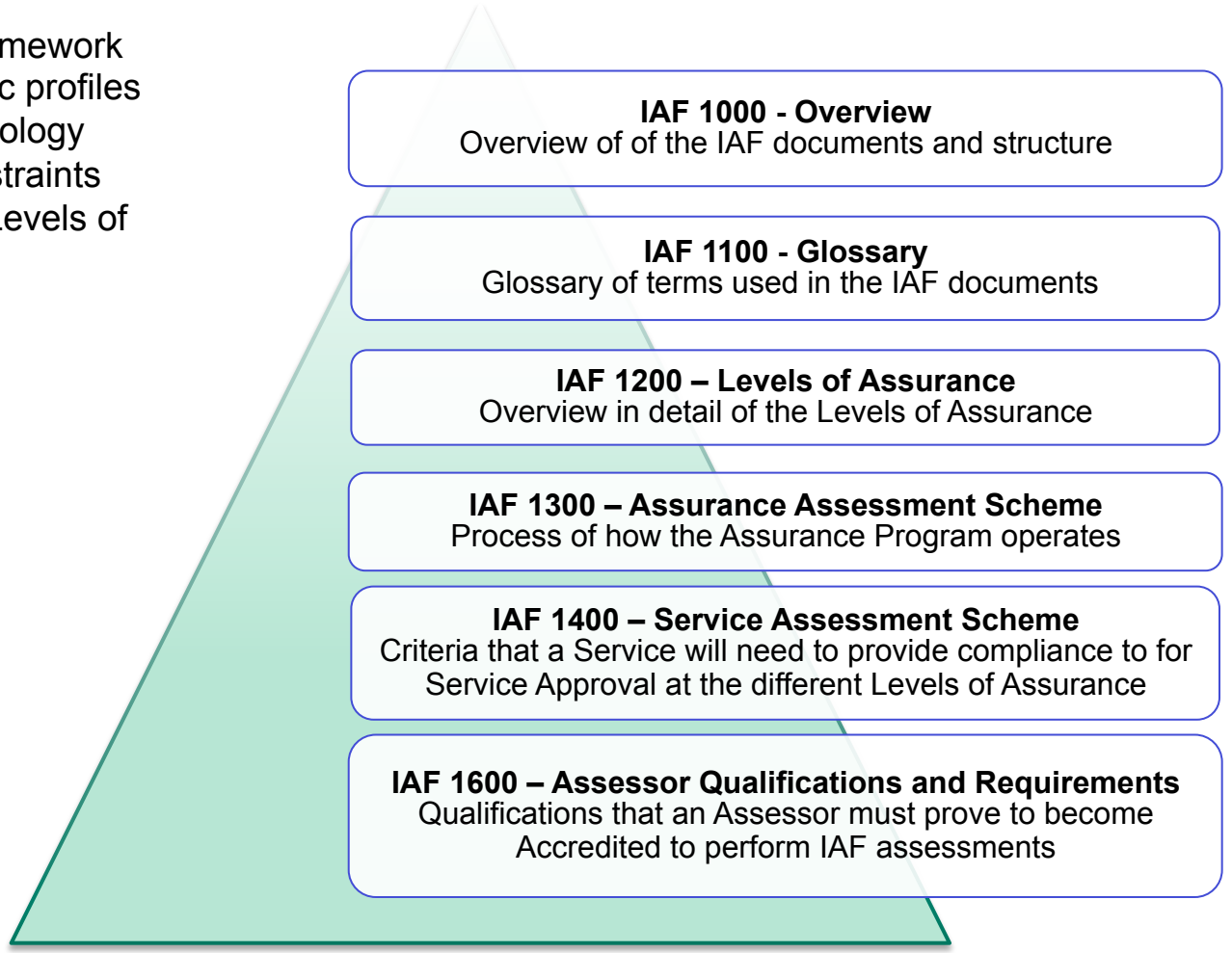
Note: Assurance level criteria as posited by the OMB M-04-04 & NIST SP 800-63

Trust Framework Model

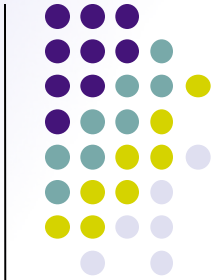


Identity Assurance Framework:
Documents

Note: a Trust Framework may apply specific profiles for specific Technology and Privacy Constraints used to achieve Levels of Assurance



Identity Assurance Framework: Actors

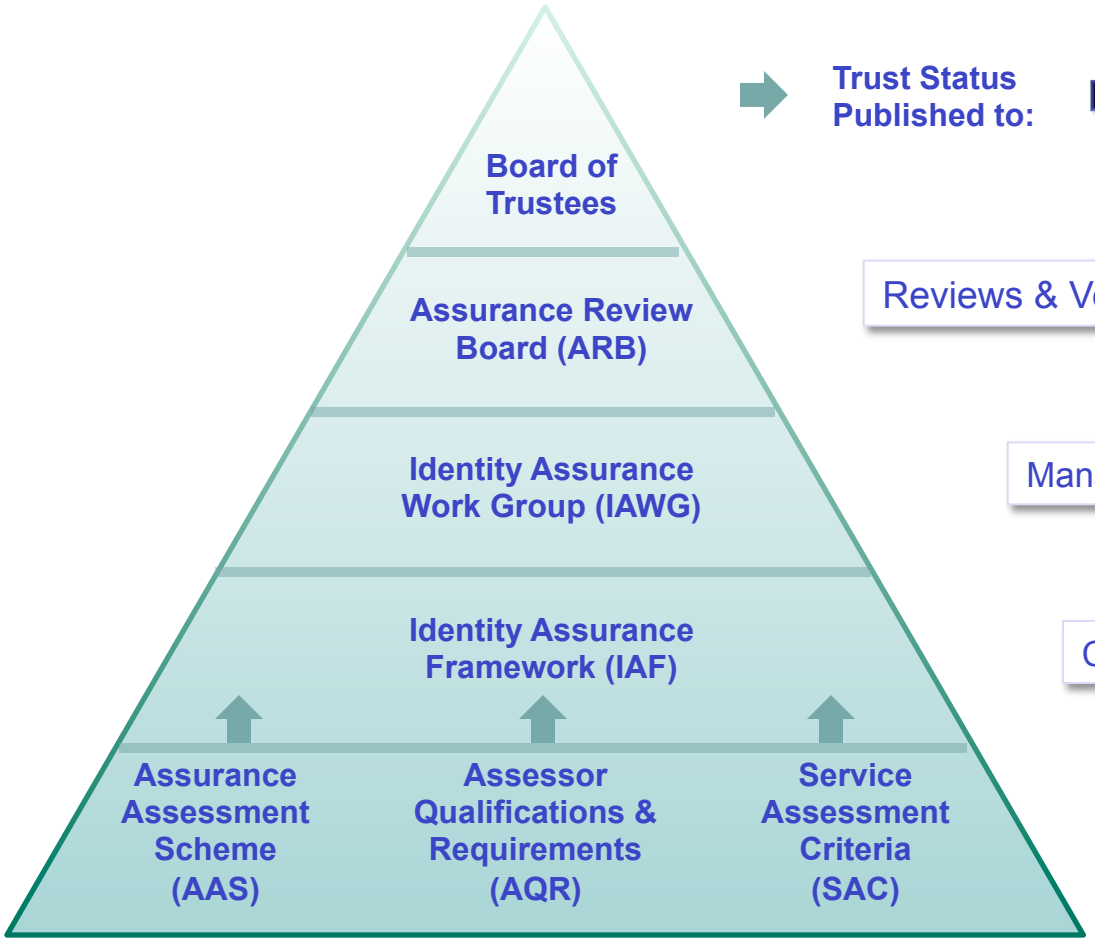


KANTARA INITIATIVE IAF

APPROVED APRIL 2010
http://kantarainitiative.org/confluence/x/e4R7Ag

ASSESSORS	CREDENTIAL SERVICE PROVIDERS	FEDERATION OPERATORS	IDENTITY ASSURANCE FRAMEWORK 2.0 MAP
Get accredited by Kantara as an assessor against the IAF 1600 AQR Leverage demonstrable competencies to expedite certification	Get assessed by a Kantara Accredited Assessor for IAF certification against the IAF 1400 SACs Submit certification application to Kantara's Assurance Review Board (ARB) Obtain and maintain compliance and certification	Define criteria for identity assurance for their federation Map policy against IAF SAC and IAF profiles Accept or recommend IAF certification to its constituents	**NON-NORMATIVE**: • **(IAF 1000)** Overview • **(IAF 1100)** Glossary • **(IAF 1200)** Assurance Levels **NORMATIVE**: • **(IAF 1300)** Assurance Assessment Scheme • **(IAF 1400)** Service Assessment Criteria • **(IAF 1600)** Assessor Qualifications & Requirements

Kantara Trust Framework



Trust Status Published to: **List Services, Registries, Whitelists**

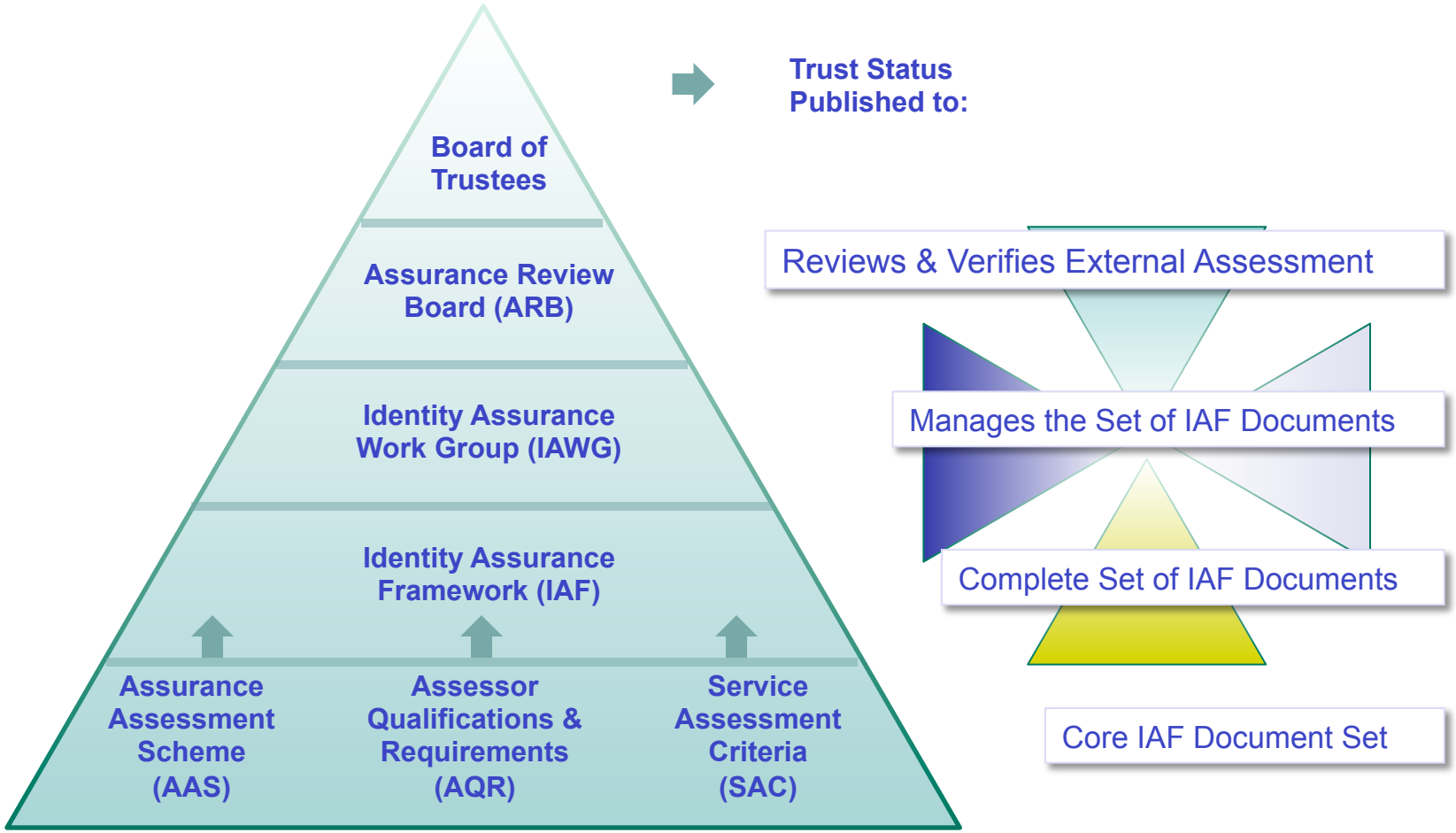
Reviews & Verifies External Assessment

Manages the Set of IAF Documents

Complete Set of IAF Documents

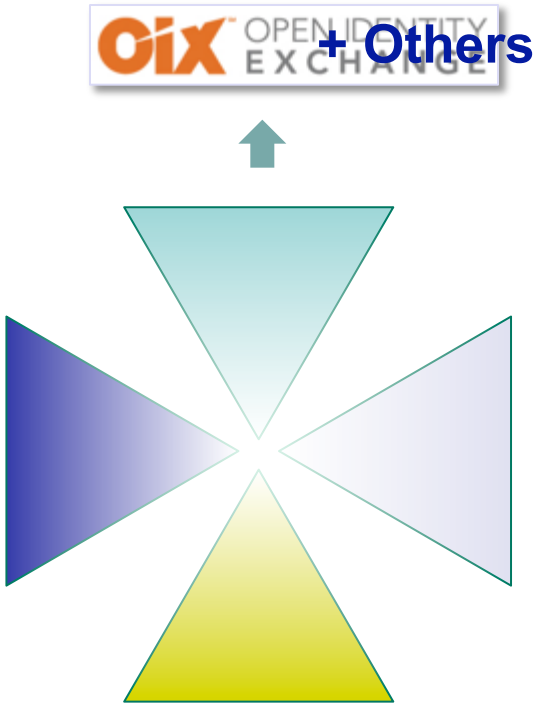
Core IAF Document Set

Kantara Trust Framework



Multiple Trust Frameworks

- Technical
  - SAML
  - OpenID
  - OAuth
- Verticals
  - Social Networks
  - Healthcare
  - Banking
- Jurisdictions
  - National Governments
  - Local Governments



Kantara Trust Framework:
Progress

Kantara Accredited to LoA 1-4

Deloitte.

Electrosoft
IT Security Solutions and Compliance

eValid8 CORPORATION

Kantara Approved to LoA 3 non-crpyto

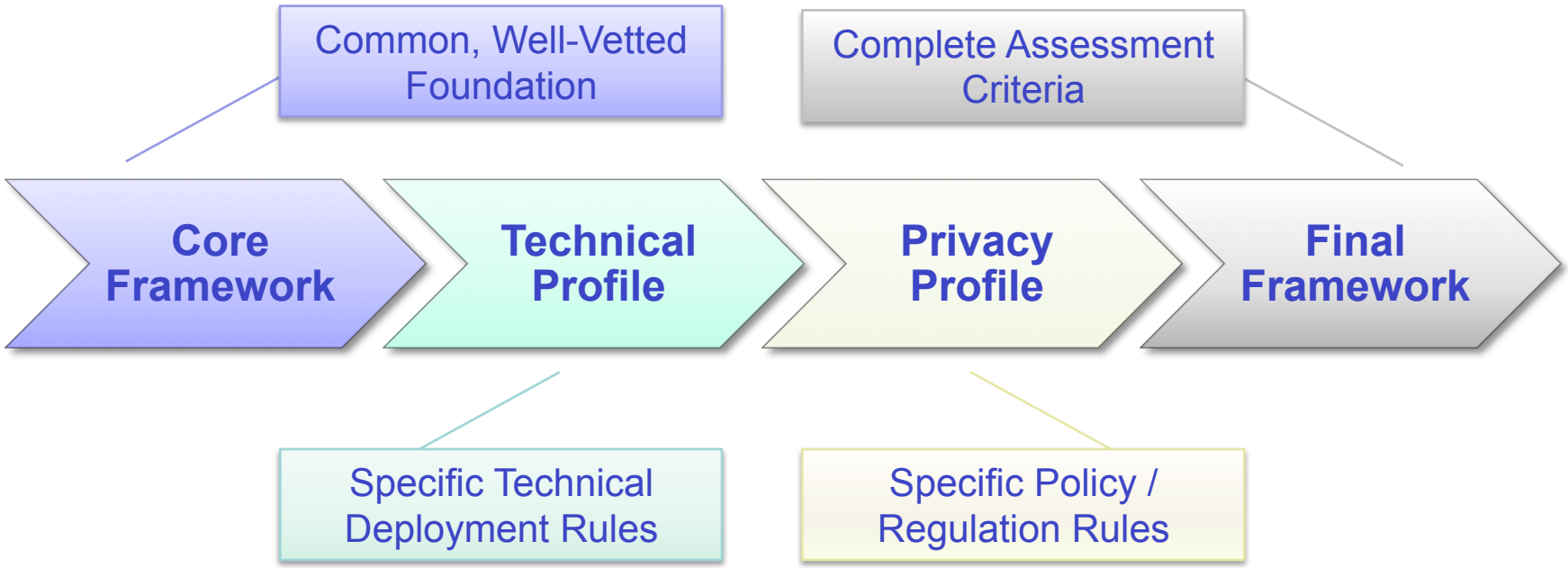
verizon

Verizon Universal Identity Service (VUIS)*
* ICAM Trust Framework Approval

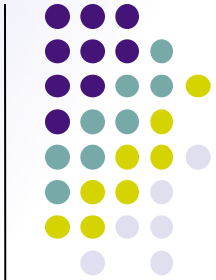
Registered Applicants

- **Accreditation:** europoint, Zygma
- **Service Approval:** Experian℠

Trust Framework Profiles



Building on the Core

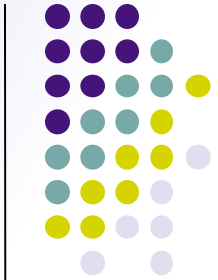


- **Identity Assurance:**
  Building in service module approach enabling Identity Proofing, Credential Management and Organizational component assessments

- **Privacy Assurance:**
  Building upon the Kantara US Federal Privacy Profile the Privacy and Public Policy (P3) WG is building Privacy Assessment Criteria (PAC) for audit controls applied in a Privacy Assessment.

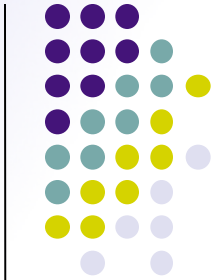
- **Attribute Management (AM) Assurance:**
  Performed landscape review of varying AM standards and development activities in Identity focused communities

Status and Lessons Learned



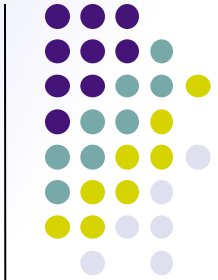
- Status:
  - Operational SAML Framework
  - Operational Organization
  - Approved for US Government Use through LOA 3
  - Referenced by eGov communities including Canada, New Zealand, Sweden
  - Assessments in progress
  - International Partners
- Lessons Learned So Far:
  - Need Additional Members, Participants, and Customers
  - Need Additional Technical Frameworks
  - Need Additional Levels of Assurance
  - Need Additional Privacy Profiles

Shaping the Future of Digital Identity



- **Kantara Initiative Website:**
  - http://kantarainitiative.org
- **Community Mail List:**
  - http://kantarainitiative.org/listinfo/community
- **Assurance Certification Center:**
  - http://kantarainitiative.org/confluence/x/EYCYAQ
- **Membership Documents:**
  - http://kantarainitiative.org/wordpress/membership/

Thanks!



kantara INITIATIVE

Questions?

- **Kantara Executive Director:** Joni Brennan joni @ kantarainitiative.org
- **General Inquiries:** support @ kantarainitiative.org