OpenID Foundation Workshop

April 17, 2022

Welcome

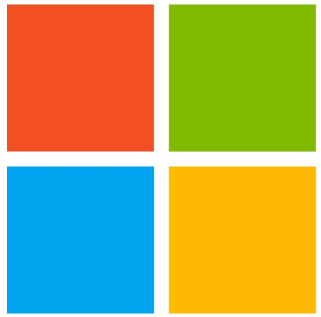
Nat Sakimura – Chairman
Gail Hodges –Executive Director

Note Well Statement

NOTICE: An OpenID IPR contribution agreement is not mandatory in order to participate in this workshop. If participants provide feedback, they (on behalf of themselves and any organization they represent) are deemed to agree that: Attendee gives the OIDF the right to use their feedback and comments. Attendee grants to the OpenID Foundation a perpetual, irrevocable, non-exclusive, royalty-free, worldwide license, with the right to directly and indirectly sublicense, to use, copy, license, publish, and distribute and exploit the Feedback in any way, and to prepare derivative works that are based on or incorporate all or part of the Feedback for the purpose of developing and promoting OpenID Foundation specifications and enabling the implementation of the same. Also, by giving Feedback, attendee warrants that they have rights to provide this feedback. Please note that feedback is not treated as confidential, and that OpenID Foundation is not required to incorporate feedback into any version of an OIDF specification.

***Please note that the workshop is being recorded and will be published to the OIDF website

Thank you!



Microsoft

OpenID®

Workshop Agenda

TIME	TOPIC	PRESENTER(S)
12:30-12:35	Welcome	Nat Sakimura & Gail Hodges
12:35-12:55	OpenWallet Foundation Update	Don Thibeau & Torsten Lodderstedt
12:55-1:20	GAIN Update	Elizabeth Garber & Dima Postnikov
1:20-1:40	OIDF Government Whitepaper Preview	Elizabeth Garber
1:40-2:00	OIDF Privacy Whitepaper Preview	Heather Flanagan
2:00-2:10	Break	
2:10-2:20	Connect WG Update	Michael Jones
2:20-2:30	OpenID for Verifiable Credentials Update	Torsten Lodderstedt & Kristina Yasuda
2:30-2:40	eKYC & IDA WG Update	Torsten Lodderstedt
2:40-2:50	FAPI WG Update	Nat Sakimura
2:50-3:00	iGov WG Update	John Bradley
3:00-3:10	MODRNA WG Update	Bjorn Hjelm
3:10-3:20	Shared Signals WG Update	Atul
3:20-3:30	Q&A & Member discussion topics	Gail Hodges & Nat Sakimura
3:30-3:45	Closing Remarks & Networking	

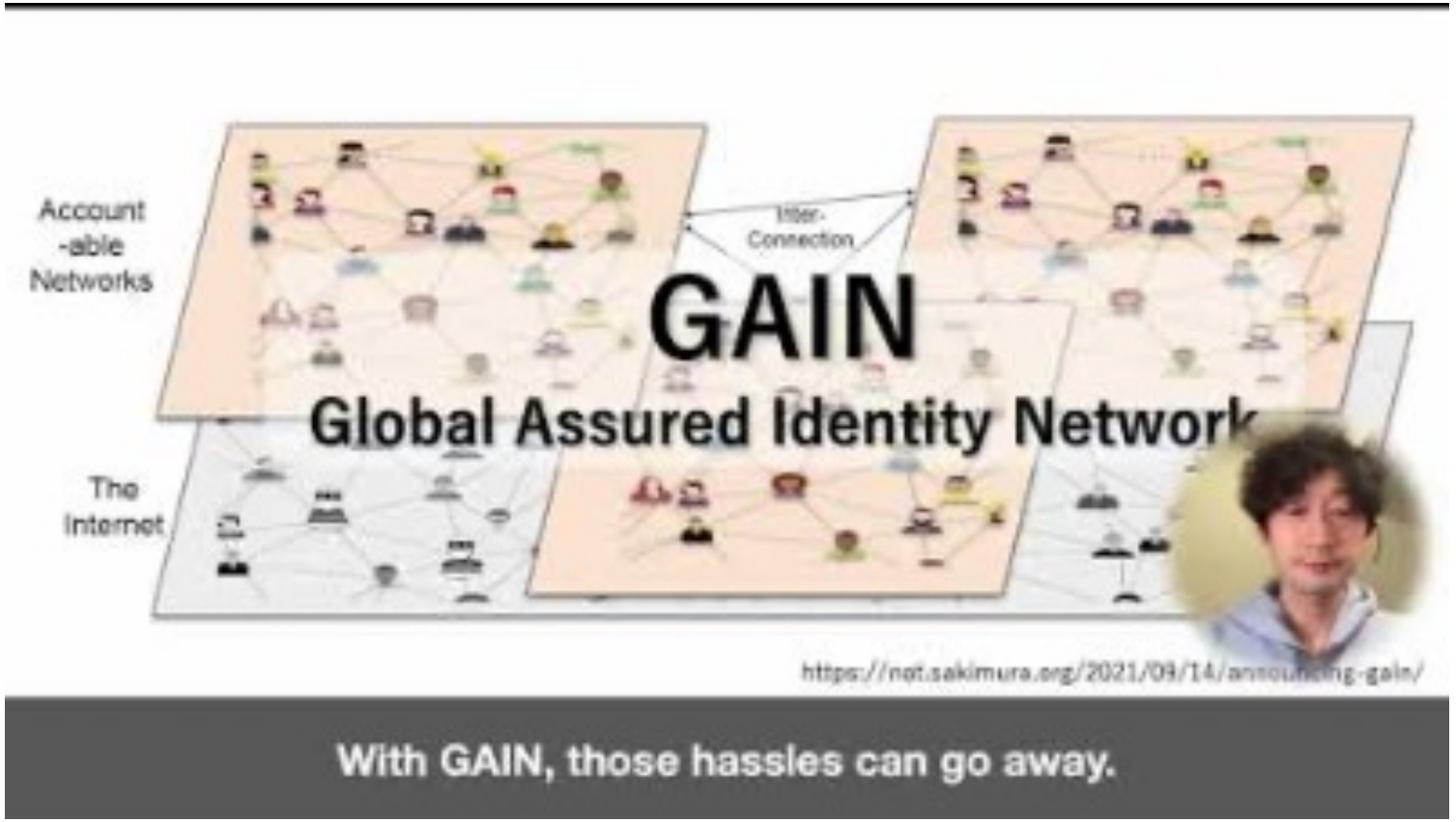
OpenWallet Foundation Update

Don Thibeau & Torsten Lodderstedt

GAIN POC Community Group Update

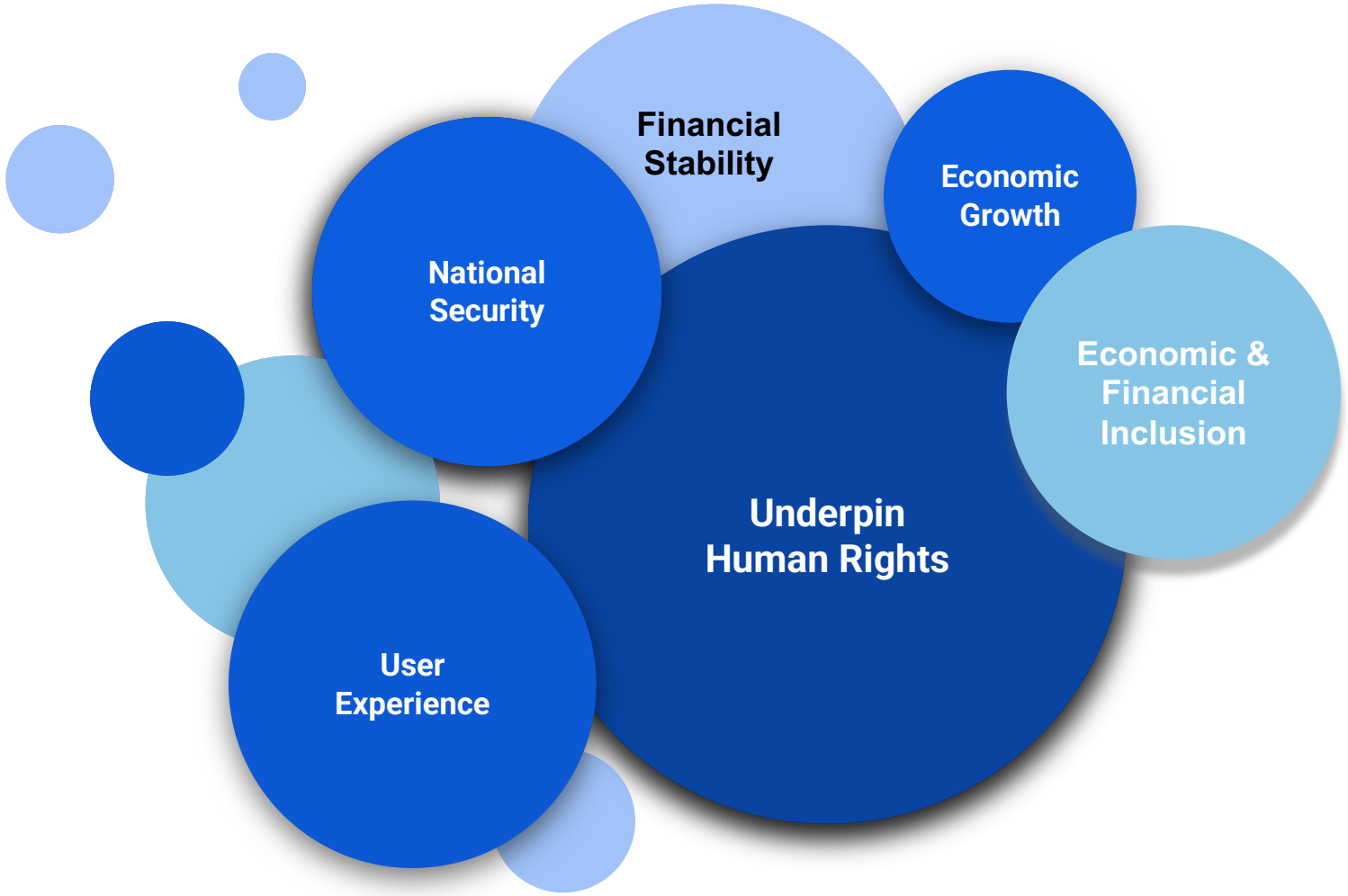
Elizabeth Garber & Dima Postnokov

GAIN Proof of Concept Demonstration

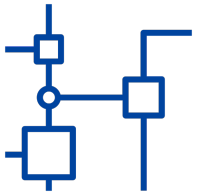


https://youtu.be/90JYrr_t8ao

Identity System Interoperability Benefits Society



GAIN is underpinned by 4 principles



Global Interoperability

Technology Agnostic

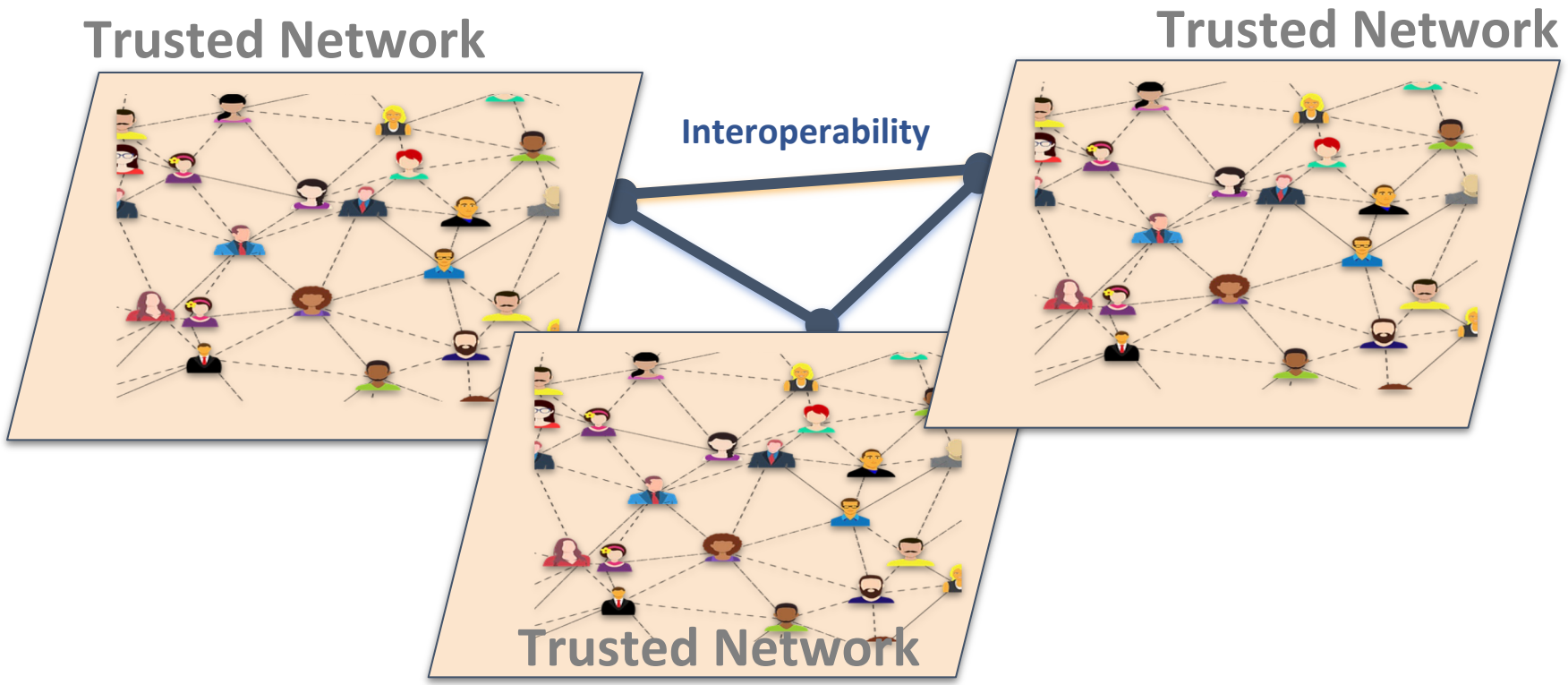
Open Standards

Internet Scale

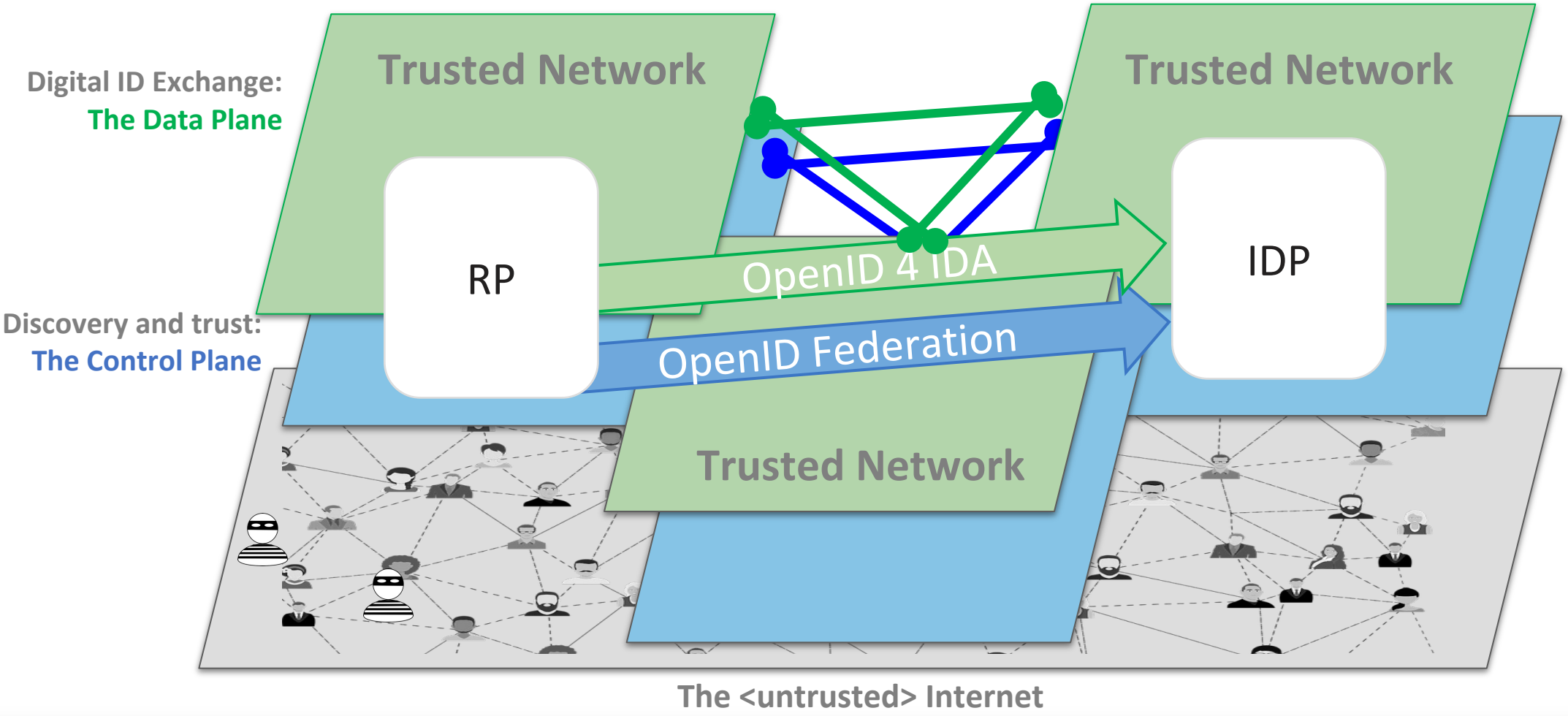
"Build on what's been built"***

***and adapt when exciting new things are built!

We’re looking to connect “islands of trust”

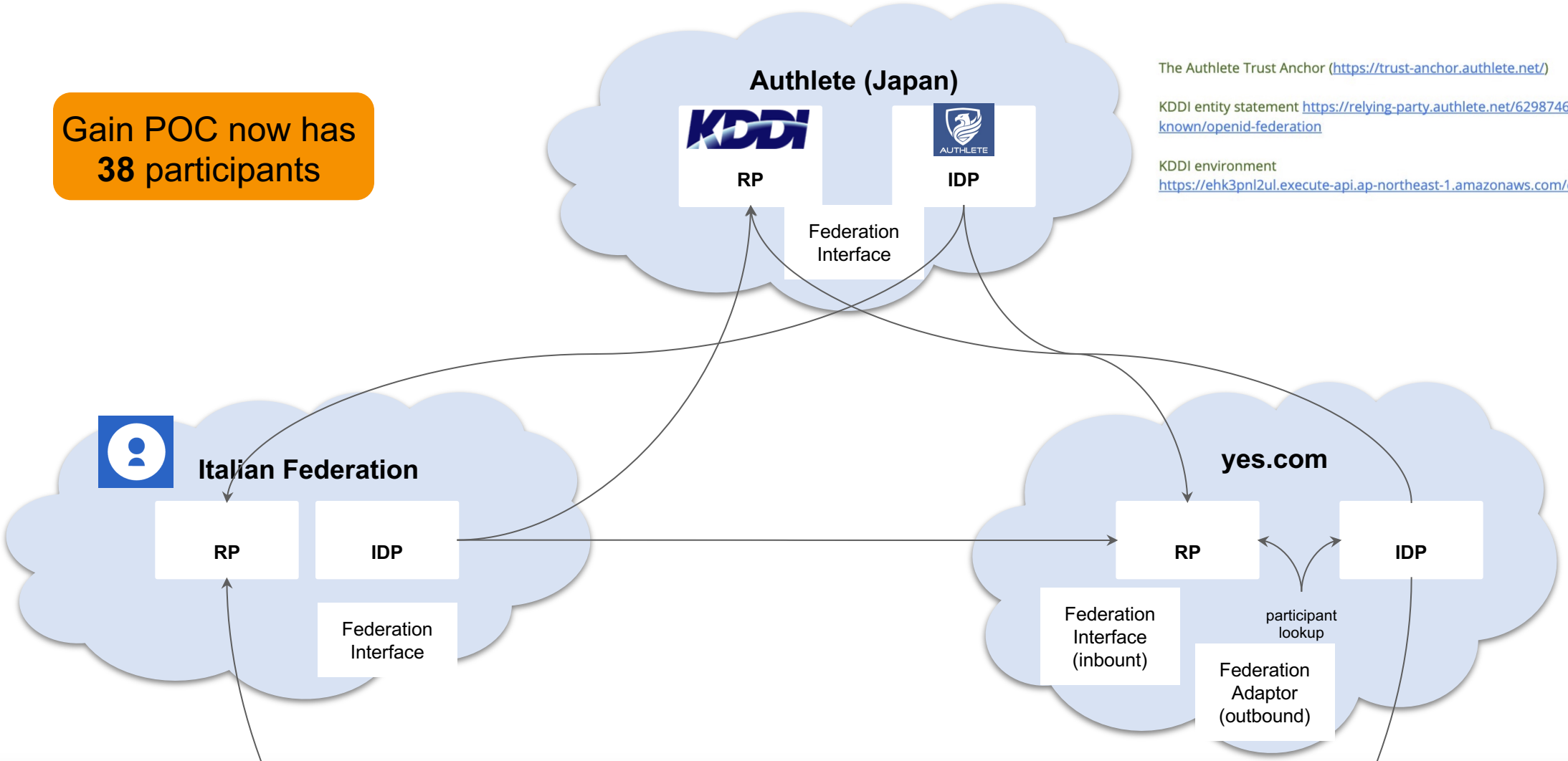


Implemented Baseline OIDC4IDA and Federation



We've connected 3 "islands"

Gain POC now has **38** participants



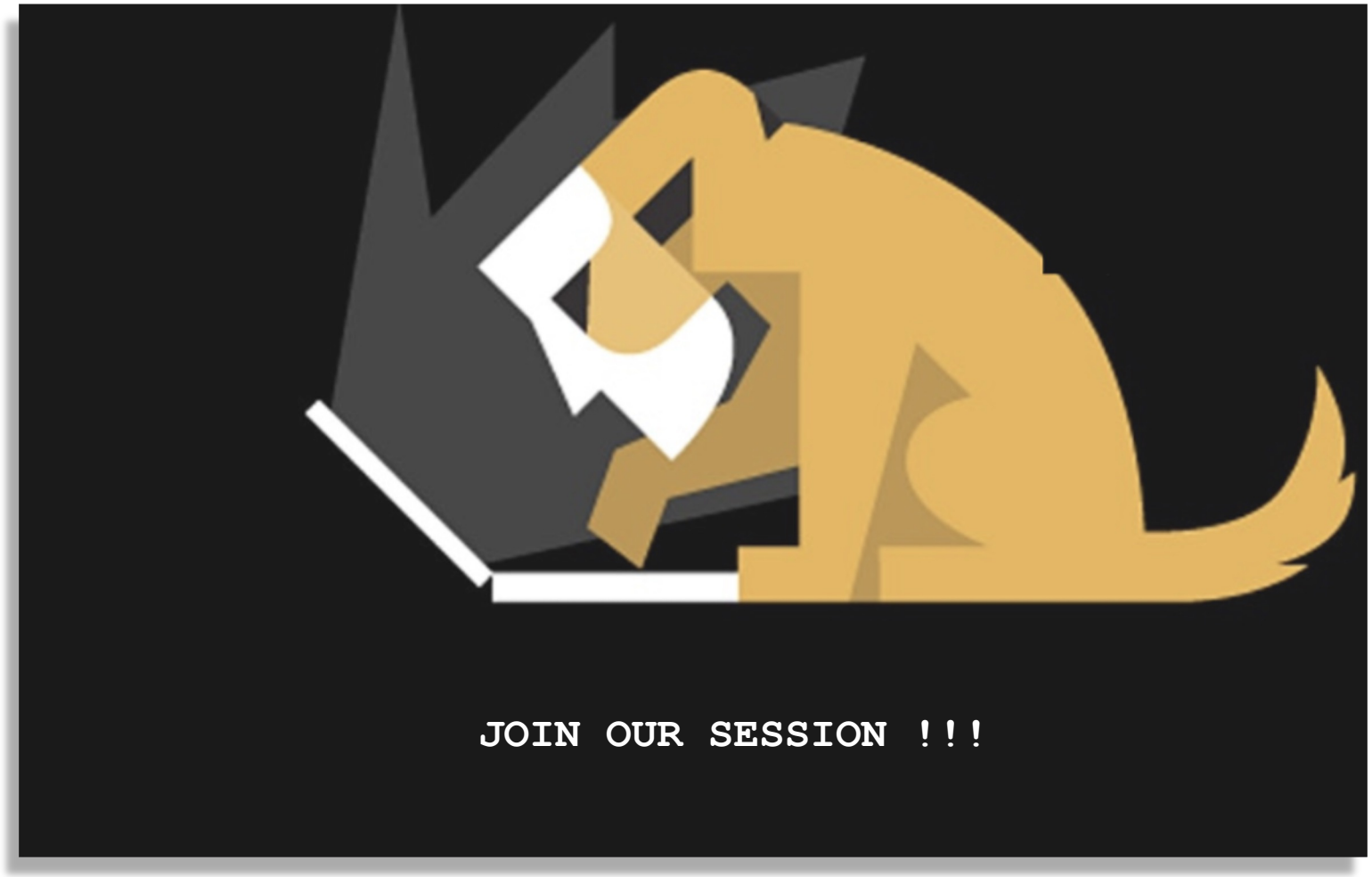
The Authlete Trust Anchor (https://trust-anchor.authlete.net/)

KDDI entity statement https://relying-party.authlete.net/6298746299842758/.well-known/openid-federation

KDDI environment
https://ehk3pnl2ul.execute-api.ap-northeast-1.amazonaws.com/dev

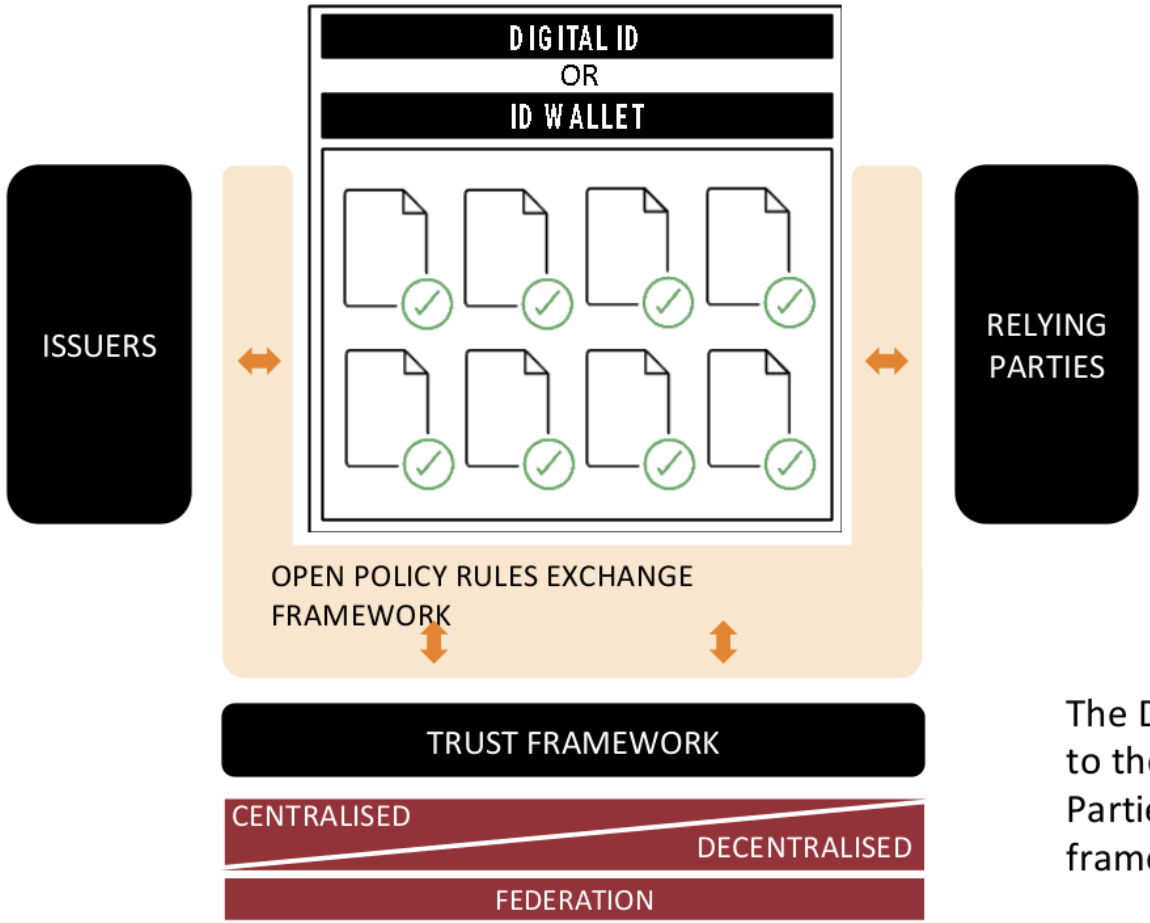
OpenID®

We’re looking to extend the POC to be multi-protocol



Meanwhile, at the OIX Global Interop Working Group…

….policy interoperability across all parties, regardless of ID “Style” and Technology agnostic



The Digital ID or Wallet is subject to the policies of Issuers, Relying Parties and prevailing tiust frameworks

OpenID®

GAIN Paper: One Year On

- **Learning has continued since Sept 2021 and the market continues to shift**
  - *Relevant regulatory movements, e.g. continued evolution of eIDAS 2.0*
  - *Developments in gov-issued ID, e.g. ISO 18013-5 (mobile drivers' licenses)*
  - *W3C recommendation on Decentralized Identifiers (DIDs)*
  - *Technical development & broader use of VCs - including GLEIF's vLEI pilots using KERI*
- **Two GAIN-specific working groups have refined the approach**
  - *OIDF's GAIN Community group (Technical POC) focused on Network-of-Network protocols*
  - *OIX GAIN Working group focused on framework-framework interop*
- **We are drafting a paper that includes the current thinking of those people and orgs now progressing the GAIN vision**
  - *Targeting a broader audience for interoperability (though still encouraging FI participation)*
  - *The current thinking & recommendations of the OIX and OIDF working groups*
  - *Defining GAIN as it relates to verifiable credentials and SSI*

OIDF Government Identity Whitepaper

Status Update

Elizabeth Garber

Role of Government

from the UN's illustrated Universal Declaration of Human Rights
https://www.un.org/en/udhrbook/index.shtml

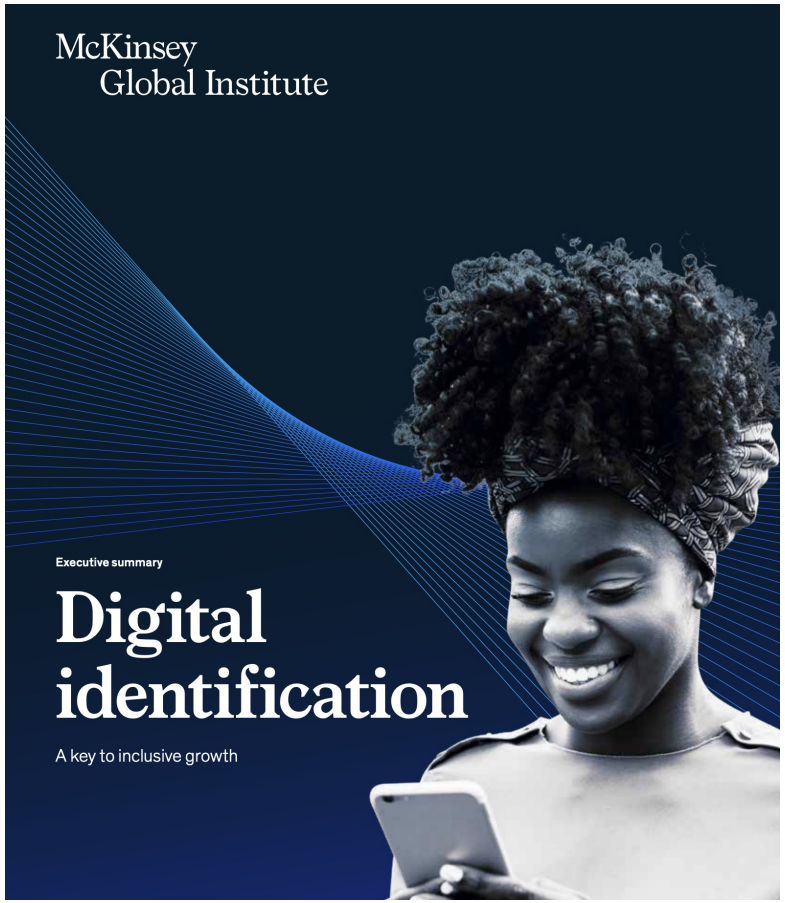
Grounded in the Universal Declaration of Human Rights & the International Bill of Rights.

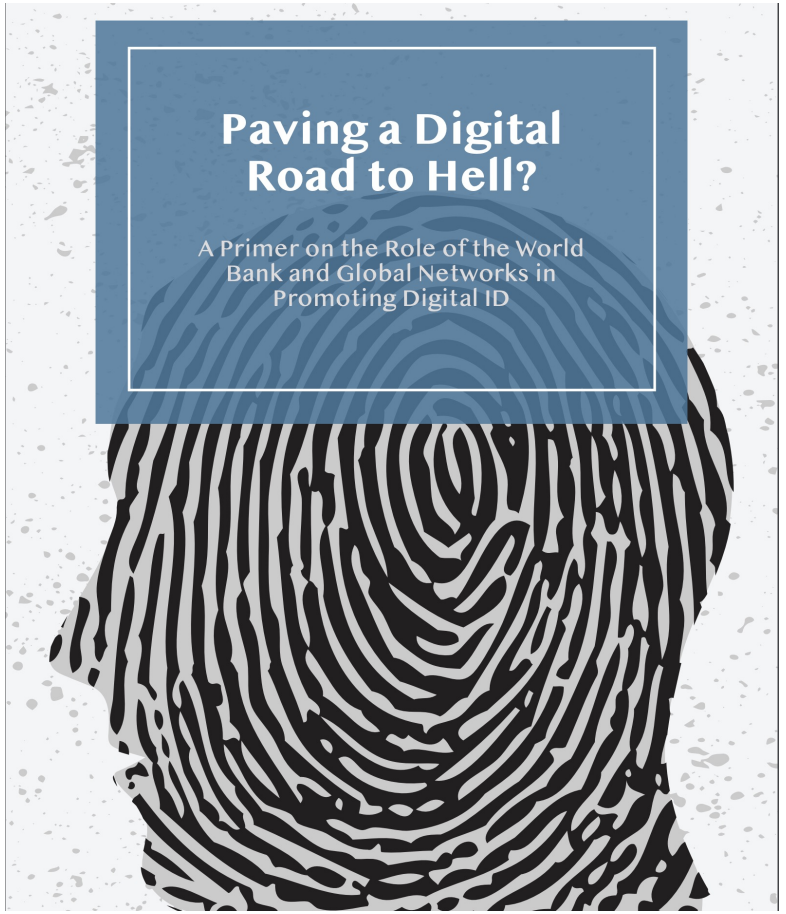
They include

- Civil Rights
- Privacy
- Physical Safety
- Political Rights
- Economic Opportunity

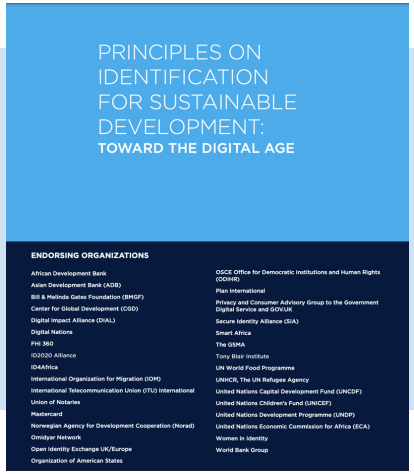
Written for government officials designing Digital Identity Systems that respect, protect, and fulfil these rights.

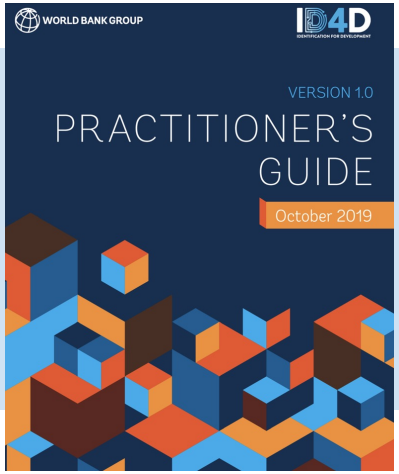
Tremendous Opportunity meets Tremendous Risk

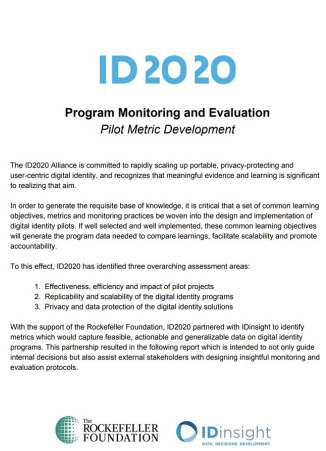


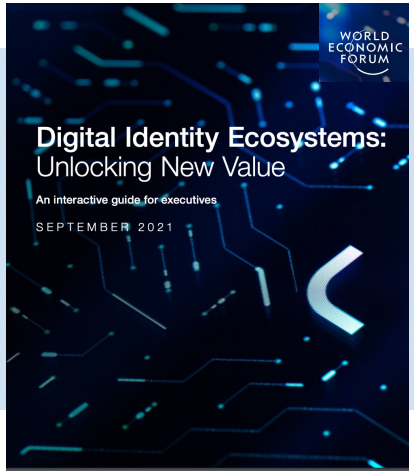


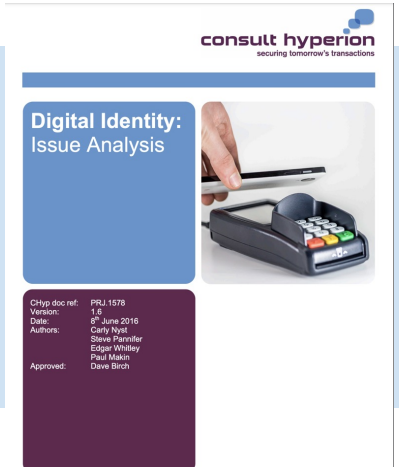
We Build Upon a Range of Literature







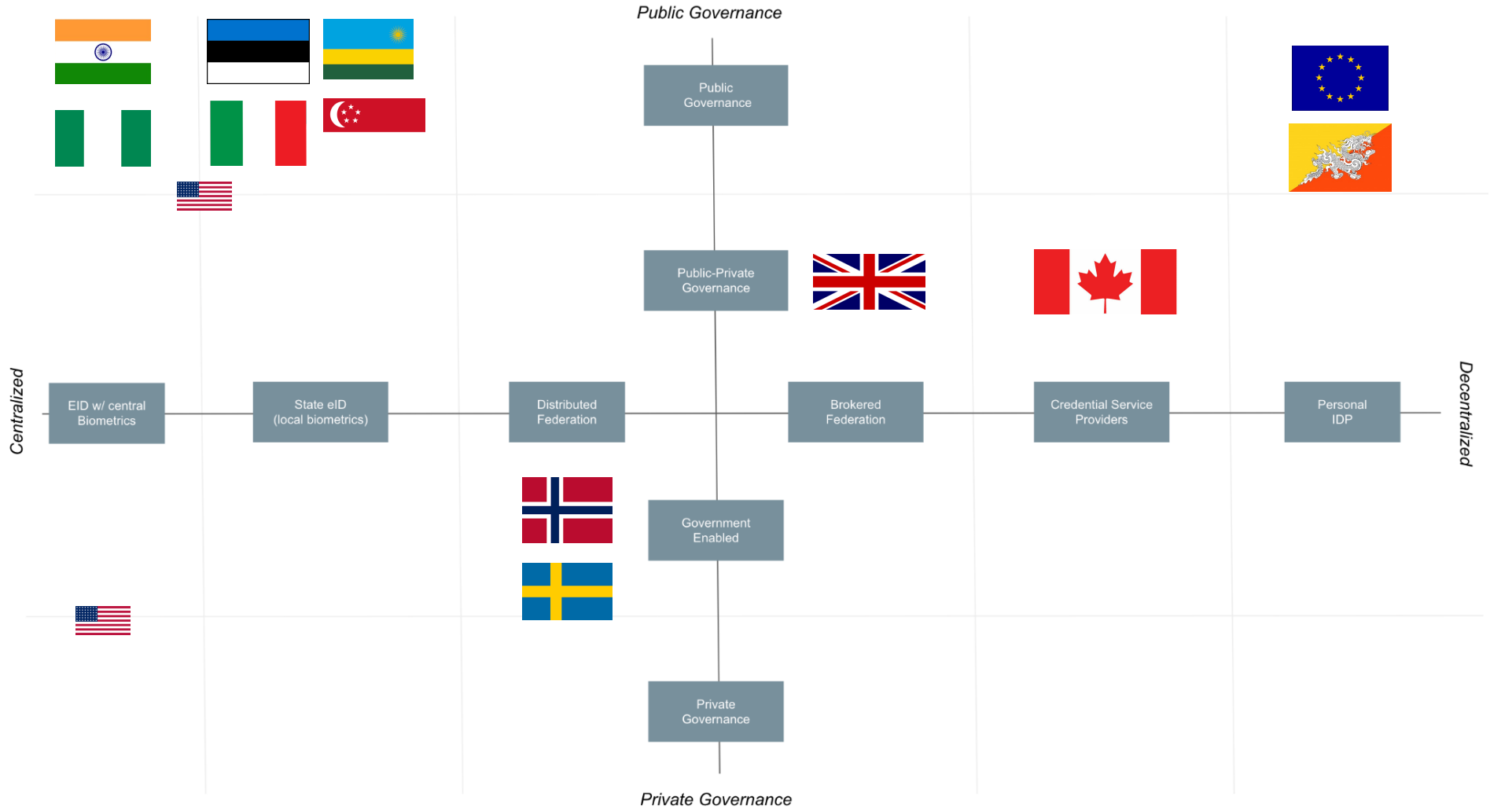




A lot of powerful work exists. In the paper, we aim to:

- Unify common themes
- Promote the most current, prescient ideas
- Identify & expand upon threads worthy of further thinking

We explore past, present, and future archetypes



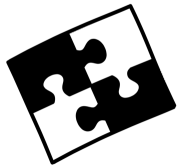
OpenID®

High-Level Insights

Holistic Strategy
Because Digital Identity ecosystems have complex stakeholders, use cases, and implications.

Human Centric Design
Organization-centered design has led to harms, unintended consequences, and lack of adoption.

Community Engagement
Essential in delivering human-centered design that meets the needs & earns the trust of stakeholders.



Interoperability
Identity ecosystems maximize benefits when they enable cross-sector, cross-border interoperability.

Mature Emerging Standards
Emerging technologies hold tremendous promise and governments should support their maturation.

Tools and Rules
Must evolve together to mitigate the risks of unintended consequences.

Institutional Protections
To underpin human rights in identity systems, data privacy and security laws refreshing & embedding.

Trust Establishment At Scale
Multi-party trust establishment remains a meaningful unsolved problem.

We endorse the OECD Draft Principles

Draft Recommendation on the Governance of Digital Identity

OECD
BETTER POLICIES FOR BETTER LIVES

Access to essential services across the public and private sectors and trust between individuals, businesses, and governments rely on being able to prove one's identity. Traditional identity verification involves physical proofs such as birth certificates, driver's licenses, ID cards, or passports. However, the digital transformation offers opportunities to consider technology for identity verification both online and offline. Digital channels now offer identity verification processes and access to authenticating verified identity claims through digital credentials and wallets, eID cards, and mobile ID applications.

Despite the benefits of digital identity, in many countries there often remains a lack of cross-sector collaboration, interoperability, and poor-quality user experience. Governments must take a holistic approach that addresses the needs of all stakeholders and focuses on user experience and effectiveness throughout the digital identity lifecycle. There is great variety in governance models for digital identity systems and solutions, which has created fragmented systems of multiple accounts and solutions for governments, businesses, and users to manage.

Establishing a successful digital identity system and widely adopted solutions can simplify interactions, enable personalisation, and reduce the risk of error and fraud. The success of digital identity systems relies on their usability and accessibility by the intended audience, including those who may not have access to technology or digital solutions, to ensure that essential services are available for all.

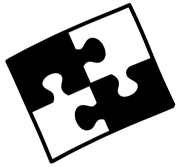
The security of digital identity systems is also a critical factor, requiring a user-centred understanding of risk, flexible regulation, and safe experimentation and innovation. Effective, usable, trusted, and secure digital identity systems must be developed and implemented through government policies, technical systems and processes, and involve governments at all levels.

As more essential services are accessed online and across borders, improving the governance and implementation of digital identity systems becomes increasingly important. Achieving this ambition is complex but international collaboration and the development of international instruments can help set expectations, create consensus, and build trust to increase the economic and social value that digital identity can provide to individual societies and the world.

The OECD's Public Governance Committee and its Working Party of Senior Digital Government Officials (E-Leaders) have developed a draft Recommendation on the Governance of Digital Identity that encourages Adherents to develop and govern digital identity systems as digital public infrastructure. This involves creating sound policies and regulatory frameworks for solution

Holistic Strategy
Because Digital Identity ecosystems have complex stakeholders, use cases, and implications.

Human Centric Design
Organization-centered design has led to harms, unintended consequences, and lack of adoption.



Interoperability
Identity ecosystems maximize benefits when they enable cross-sector, cross-border interoperability.

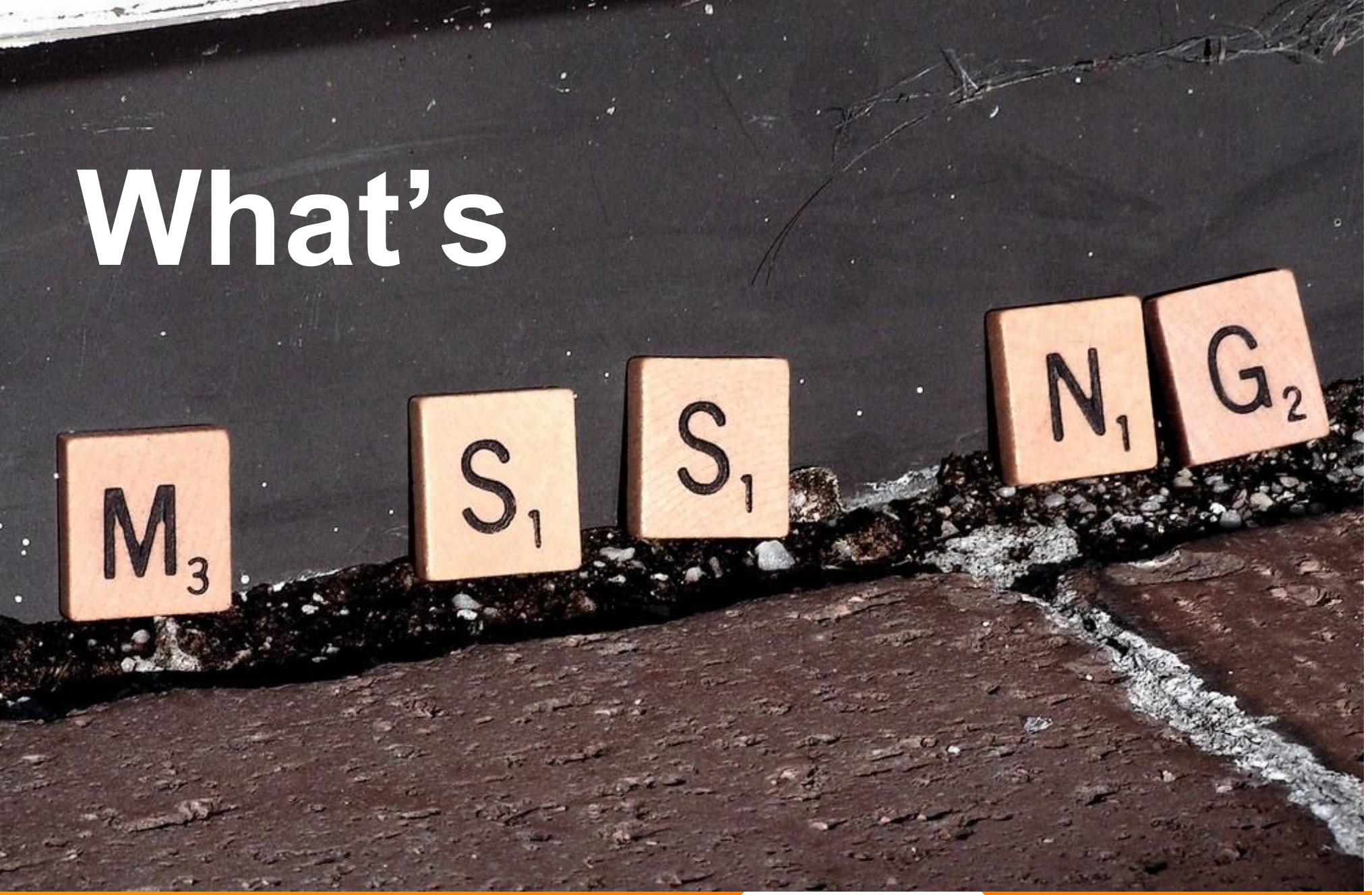
OpenID®

Topics where we are extending the conversation

- Thematic analysis of existing ID Principle frameworks
- Analysis of past, present, and future archetypes, including
  - Architectural models
  - Governance models
  - Highlights & Lowlights of existing and failed schemes
- Identification of trade-offs between goals (e.g. privacy vs. inclusion) or stakeholders (e.g. organizations vs. individuals) and general approaches to risk mitigation
- Discussion around gaps in institutional support - especially legal paradigms
- More granular feedback about:
  - Specific security & privacy tech (e.g. SSE)
  - Allowance for multiple personas
  - Delegation
  - Disputes

Theme	ID2020[85]	ID4D[86]	WEF [87]	DIACC & HTF	OECD
User Centric					
Designed for Human-Centric Outcomes	x	x		x	x
Designed for Users (incl children, vulnerable, & guardianship)	x	x	x	x	x
Designed for Service Providers	x			x	x
Caters for Pseudonymous Identity	x			x	x
User Choice & Control	x	x	x	x	x
Inclusion					
Universal Access / Remove Barriers	x	x		x	x
Voluntary / Not Mandatory	x	x		x	x
Unique to You / Persistent Identifiers	x	x			x
Portable / Resilient (Always Accessible)	x			x	x
Governance					
Critical / Strategic National Infrastructure					x
Independent Oversight		x			x
Transparent Policies	x			x	x
Clear Accountability	x	x	x	x	x
Public / Private Collaboration					x
Public Engagement / Dialogue				x	x
Accessible Onboarding & Regulatory Sandboxes					x
Long Term Sustainability		x	x	x	x
Environmental Impact					x
Privacy & Security					
Data Minimization / Selective Disclosure	x	x	x	x	x
Prevent Aggregation / Correlation	x				x
Privacy-by-Design	x	x	x	x	x
Security Minimum Standards	x	x	x	x	x
Enforce Privacy & Security Laws, Regulations, Guidelines					x
Interoperability					
Responsive	x	x			
Conform to Standards	x	x			x
Prevent Vendor Lock-In	x	x			x
Cross-Sector Interoperability	x			x	x
Technical Interoperability (cross border)	x	x	x	x	x
Legal Interoperability (cross border)	x				x

What's



?

OpenID®

“Government-issued Digital Credentials and the Privacy Landscape”

OIDF Privacy Whitepaper Listening Session

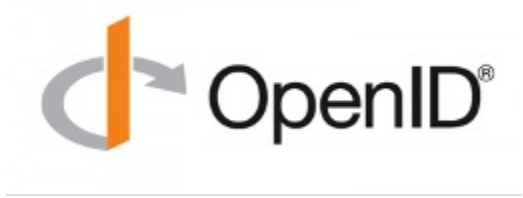
Heather Flanagan -- white paper lead editor

Where Did I Come From?

- Context for the paper: Global
- Target Audience: Government policymakers, civil society members, technologists
- Process: Interviews, listening sessions, research, more research, plus extra research

Contributors (so far)

Organizations:



Individual Contributors:

- Dr Joseph Atick, ID4Africa
- Vittorio Bertocci, Okta, Inc.
- Debora Comparin, Thales DIS
- Bill Nelson, Identity Fusion, Inc.
- Gail Hodges, Executive Director, OpenID Foundation
- Mike Kiser, SailPoint Technologies
- Stephanie de Labriolle, Executive Director, Secure Identity Alliance (SIA)
- Giuseppe De Marco, Dipartimento per la trasformazione digitale
- Rachelle Sellung, Fraunhofer Institute
- Kristel Teyras, Thales DIS
- John Wunderlich, Chair, Kantara Privacy Enhancing Mobile Credential Work Group

Recommendations

Back to Basics

- Individual Agency
- Systemic Transparency
- Data Minimization
- Advanced Cryptography

Addressing Ongoing Concerns

- Surveillance
- Diversity, Equity, Inclusion
- Single Points of Failure
- Inappropriate Use by Legitimate Actors
- Sustainable Protections

Emerging Concerns

- Digital Warfare
- Deepfakes

Civil Society

- Expertise in both directions

Read More!

https://openid.net/2023/04/05/open-for-comment-privacy-landscape-whitepaper/

📝 Open for Comment: “Government-issued Digital Credentials and the Privacy Landscape” Whitepaper

This entry was posted in Whitepaper *on April 5, 2023 by Mike Leszcz*

10 minute break

Visit: openid.net

OpenID Foundation
Working Group & Community Group Updates

OpenID Connect Working Group Update

Michael B. Jones

Working Group Overview

Objective of the Working Group

- The OpenID Connect working group created the OpenID Connect protocol enabling both login and logout, incubated OpenID Connect for Identity Assurance (now in the eKYC-IDA WG), is developing OpenID Connect Federation, and is the home of OpenID for Verifiable Credentials
- See the list of specs with descriptions at https://openid.net/wg/connect/status/

Published Specifications

- OpenID Connect Core, Discovery, Dynamic Client Registration, Multiple Response Types, Form Post Response Mode, RP-Initiated Logout, Session Management, Front-Channel Logout, Back-Channel Logout, Error Code unmet_authentication_requirements, Initiating User Registration

Specifications Under Development

- OpenID Connect Federation, OpenID for Verifiable Credentials (Self-Issued OpenID Provider V2, OpenID for Verifiable Presentations, OpenID for Verifiable Credential Issuance), UserInfo Verifiable Credentials, Claims Aggregation, Native SSO for Mobile Apps

Working Group Progress & Opportunities

Working group deliverables since last workshop in November

- Unmet Authentication Requirements is now Final (November 2022)
- Initiating User Registration via OpenID Connect is now Final (December 2022)
- Native SSO for Mobile Apps became Implementer's Draft (December 2022)
- Proposed Second Implementer's Draft of OpenID for Verifiable Presentations Specification (March 2023)
  - Vote now at https://openid.net/foundation/members/polls/311 !
- Multiple OpenID Connect Federation drafts published
- Multiple OpenID4VC drafts published (described in a different presentation)

Challenges and opportunities facing the working group

- OpenID Connect Federation in production use in Italy
- Discussions on expanding trust models usable by Federation deployments to include Web PKI
- Relationships with digital wallet initiatives and national identity systems worldwide
- Publicly Available Specification (PAS) submission of OpenID Connect specifications

Working Group Roadmap

DATE	DELIVERABLES	ASPIRATIONS	NOTES
Q2 2023	Next Federation Implementer's Draft	Broaden trust models usable by deployments to include Web PKI	We can discuss specifics this week
Q2 2023	Apply errata edits	Resolve the 26 errata issues	Then publish Second Errata Sets
Q3 2023	PAS submissions	Make OpenID Connect specs available to those with treaty-based procurement processes	Completed ISO/IEC JTC 1 PAS Submitter Application – ISO PAS status approved and template in development for submission with errata changes.
Q3/4 2023	Final Federation Spec	Trust establishment for broad set of use cases	Having Final spec will accelerate deployments

What the Working Group Hopes to Accomplish at IIW This Week

What sessions do those of you here plan to hold?

What hallway/table conversations do you want to have?

Today's OpenID Connect working group call cancelled in favor of this workshop

Do we want to hold Thursday's calls?

- 7am European-friendly OpenID Connect working group call
- 8am SIOP special topic call

OpenID for Verifiable Credentials Topic Update

Dr. Torsten Lodderstedt, yes
Kristina Yasuda, Microsoft

Overview

Objective

- Develop and publish credential exchange protocols for the Issuer-Holder-Verifier Model (aka Decentralized Identity)

Specifications Under Development

- OpenID for Verifiable Presentations (OID4VP)
  - ID 2 (open for voting from April 17th)
  - Development of Conformance tests has started
- OpenID for Verifiable Credential Issuance (OID4VCI) - aiming to start ID 1 in May
- Self-Issued OP v2 (SIOPv2) - aming to start ID 2 after OID4VCI
- Trust and Security for OID4VC, in review for WG adoption
- OpenID for Verifiable Presentations over BLE, 1st draft in WG review

Progress & Opportunities

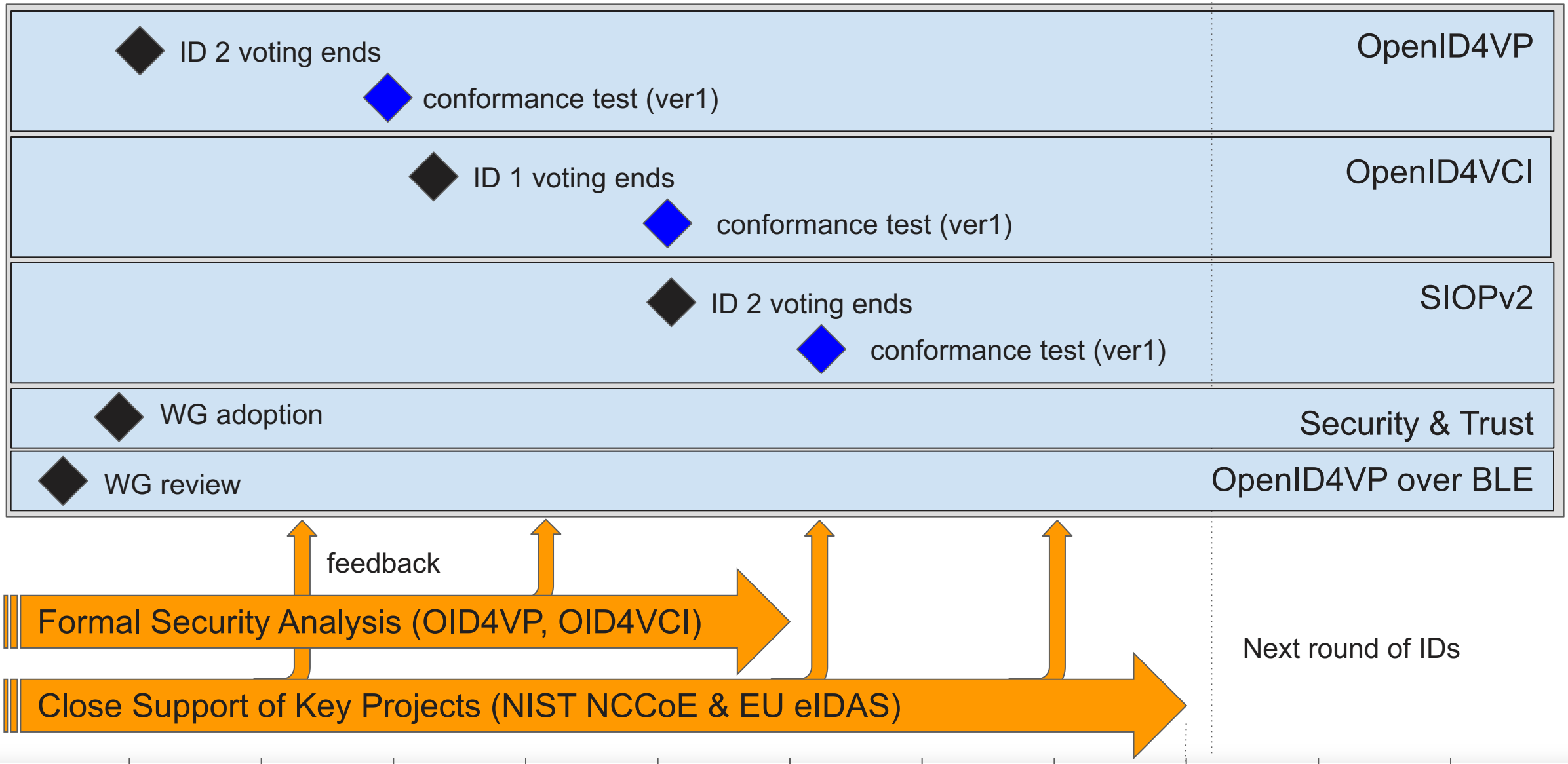
since last workshop in November…

- OID4VC was adopted by EU eIDAS Architecture and Reference Framework for credential exchange and authentication in online Use Cases
- Started work on overall Security Analysis
  - Started formal Security Analysis
- Started work on OID4VP over BLE (with MOSIP)
- Improved OID4VP specification
  - Added Signed and/or Encrypted Presentation Responses (JARM)
  - Combination of direct_post and redirect to cope with large payload in same device flow or to increase the security of the cross device flow
  - Added Client Identifier Schemes
  - Enhanced Security and Implementation Considerations

Opportunities & Challenges

- NIST NCCoE and EU eIDAS are huge opportunities for widespread adoption of OID4VC
- Liaison with European Commission under way
- OID4VP over BLE is opportunity to provide credential exchange protocols across online and offline space.
- Need more contributors with BLE expertise
- Proposal in Chromium to deprecate custom URL schemes as a way to invoke the wallets

Milestones


ID 2 voting ends
conformance test (ver1)
OpenID4VP
ID 1 voting ends
conformance test (ver1)
OpenID4VCI
ID 2 voting ends
conformance test (ver1)
SIOPv2
WG adoption
Security & Trust
WG review
OpenID4VP over BLE
feedback
Formal Security Analysis (OID4VP, OID4VCI)
Close Support of Key Projects (NIST NCCoE & EU eIDAS)
Next round of IDs
April
Oct
2024
March

What the Working Group Hopes to Accomplish at IIW This Week

Sessions

- OpenID4VC 101 (give update and increase awareness)

Side meetings

- OID4VC roadmap presentation and discussion based on the implementation experience
- Reviewing the query language in OID4VP
- Wallet attestation
- Discuss proposal in Chromium to deprecate custom URL schemes as a way to invoke the wallets
- Demos (at least 2 demo tables!)
- Survey: Open Source projects for OID4VC

Related sessions

- UserInfo profile of OID4VCI
- SD-JWT VC

Voting to approve OpenID 4 VP Implementers Draft 2 is open

- Please vote!
- https://openid.net/foundation/members/polls/311

eKYC & IDA Working Group Update

Mark Haine

eKYC & IDA WG Co-Chair

Working Group Overview

Objective of the Working Group

- Extend OIDC to included a standardized schema for expressing (and requesting) identity assurance metadata

Published Specifications

- OpenID Connect for Identity Assurance 1.0. (4th Implementer's Draft)
- JWT Claims registry request is submitted

Specifications Under Development

- OIDC4IDA - FINAL soon, very soon! - Current snapshot
- The Advanced Syntax for Claims – Current snapshot
- OpenID Connect for Authority – Current Snapshot
- OpenID Connect for IDA profiles?

Working Group Progress

Working group deliverables since last workshop in November

- We are in the final mile!
- JWT Claims registry request has been submitted
- Various editorial changes have been pushed through

External achievements

- W3C draft created to use IDA schema as an ‘evidence’ type under VC data model 1.1
- OIX using OIDC4IDA as a reference point for Global Interoperability Working Group
- Three significant projects are using the OIDC4IDA spec
  - TISA in UK
  - Connect ID in Australia
  - tbd/Block in the US (combining OIDC4IDA & VC data model)

Working Group Challenges and Opportunities

Challenges facing the working group

- Balancing the need to get the spec to final against the implementation lessons being learned
  - We could keep making “improvements” for quite a long time
- OIX keen to recommend that OIDC4IDA be “evolved to be a protocol independent data standard”
- Profiles for specific evidence artefacts and assurance process representation
  - Re-usable specs for things like specific pieces of evidence or specific assurance processes
- Extensions keep emerging particularly in the data schema area
  - E.g. creation of new claim that is an array of typed personal identifiers

and Opportunities

- for the IDA schema to be used in Verifiable Credentials - W3C draft exists for “evidence” property
- It is confirmed that implementations are awaiting “Final” at least:
  - 3 entities in Japan
  - 1 further entity in US

Working Group Roadmap

DATE	DELIVERABLES	ASPIRATIONS
Q2 2023	OIDC4IDA Final review	
Q3 2023	ASC Implementers draft OIDC for Authority Implementers draft	OIDC4IDA Final Profiles begin to emerge
Q4 2023		Projects start going live

What the Working Group Hopes to Accomplish at IIW This Week

Discuss IDA spec cross-over with VC

FAPI Working Group Update

Nat Sakimura, Co-chair, FAPI WG

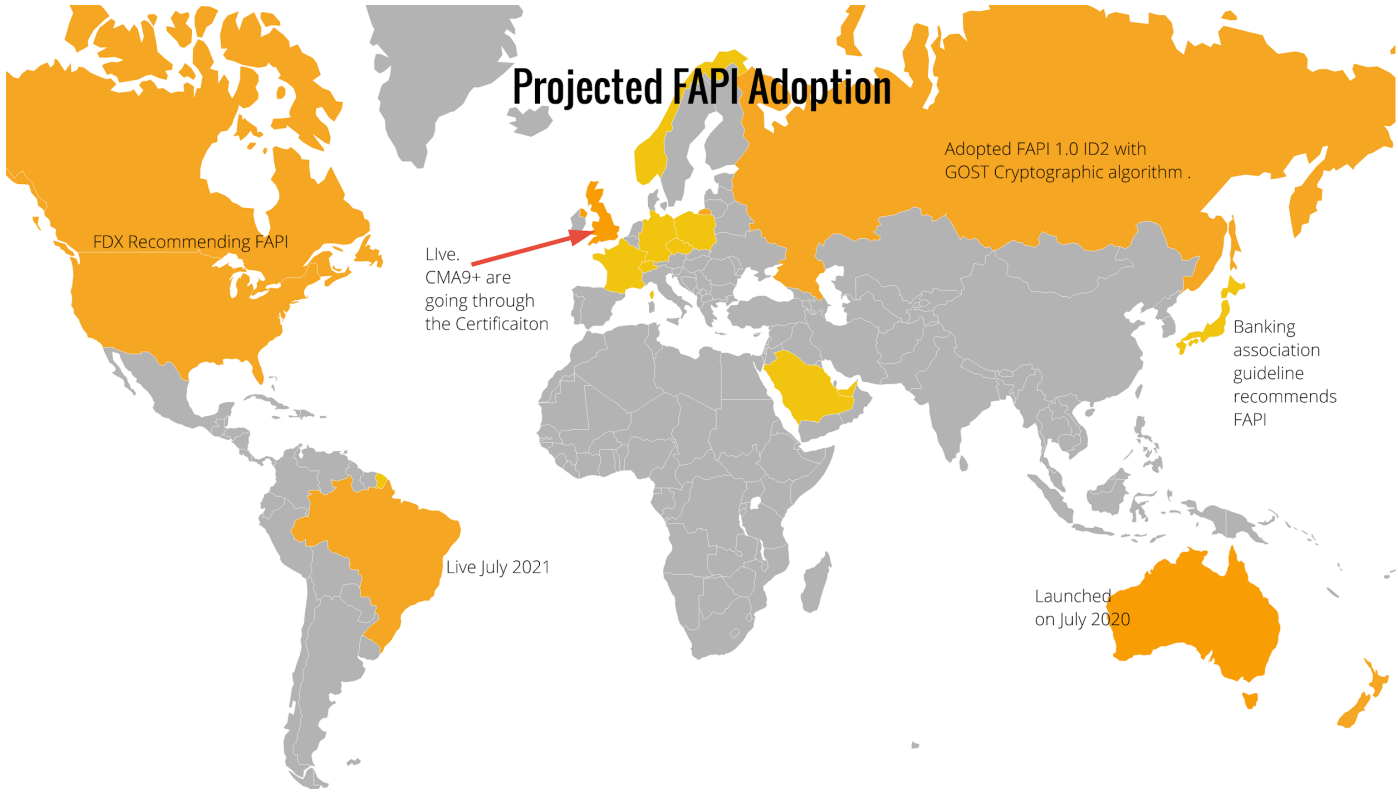
Working Group Overview

Objective of the Working Group

- Create general purpose high-security profiles for OpenID Connect and OAuth

Some notable aspects

- Extensive use of Formal Verification
- Close collaboration with national regulators and associations
  - e.g. Australia, Brazil, UK
  - Thanks for sponsoring the works!
- Trying to be ISO directive compliant so that translation/adaptation etc. would be easier.
- National level certifications



Working Group Progress & Opportunities

Published Specifications

- FAPI Security Profile (FAPI) 1.0 – Part 1: Baseline – A secured OAuth profile that aims to provide specific implementation guidelines for security and interoperability.
- FAPI Security Profile (FAPI) 1.0 – Part 2: Advanced – A highly secured OAuth profile that aims to provide specific implementation guidelines for security and interoperability.
- JWT Secured Authorization Response Mode for OAuth 2.0 (JARM) – This specification was created to bring some of the security features defined as part of OpenID Connect to OAuth 2.0

Working Group Progress & Opportunities

Implementer's Drafts

- FAPI: Client Initiated Backchannel Authentication (CIBA) Profile – FAPI CIBA is a profile of the OpenID Connect's CIBA specification that supports the decoupled flow
- FAPI 2.0 Security Profile and Attacker Model – FAPI 2.0 has a broader scope than FAPI 1.0 as it aims for complete interoperability at the interface between client and authorization server as well as interoperable security mechanisms at the interface between client and resource server
- Grant Management for OAuth 2.0 – This profile specifies a standards based approach to managing "grants" that represent the consent a data subject has given. It was born out of experience with the roll out of PSD2 and requirements in Australia

Active Drafts

- FAPI 2.0: Message Signing – an extension of the baseline profile that provides non-repudiation for all exchanges including responses from resource servers
- FAPI 1.0 — Lodging Intent ===> Now OAuth PAR + OAuth RAR

Adoption

FAPI 1:

- UK: Open Banking UK
- Brazil: OpenFinance, OpenInsurance
- USA: FDX (Financial Data Exchange)
- Saudi Arabia: Open Banking
- Japan: Minna No Ginko (moving towards FAPI 2.0)
- Australia: Consumer Data Right (moving towards FAPI 2.0)

FAPI 2:

- Norway: HelseID e-Health systems (integration ongoing)
- Australia: ConnectID (digital identity exchange)
- Germany: yes.com (private-sector open banking ecosystem)

Working Group Progress & Opportunities

White Paper

- “Open Banking and Open Data: Ready to Cross Borders?”

Formal Analysis

- Like it was done for FAPI 1.0, Formal security verification is being done for FAPI 2.0. Work Package 2 covers FAPI 2.0 Advanced and CIBA.

Certification

- Thriving for FAPI 1.0.
  - I stopped counting it. See https://openid.net/certification/#FAPI_OPs
- Starting for FAPI 2.0.

Working Group Roadmap

DATE	DELIVERABLES	ASPIRATIONS	NOTES
Q2 2023		FAPI 2.0 Message Signing -- 1st Implementer's draft	
Q3 2023	Formal Verification for FAPI 2.0 Message Signing and CIBA		
Q4 2023		FAPI 2.0 Message Signing -- 2nd Implementer's draft FAPI CIBA -- 2nd Implementer's draft Grant Management for OAuth 2.0 -- 2nd Implementer's draft	
Q1 2024		FINAL for FAPI 2.0 specs.	

iGov Working Group Update

John Bradley Chair

Working Group Overview

Objective of the Working Group

- The purpose of this working group is to develop a security and privacy profile of the OpenID Connect specifications that allow users to authenticate and share consented attribute information with public sector services across the globe. The resulting profile will enable standardized integration with public sector relying parties in multiple jurisdictions. The profile will be applicable to, but not exclusively targeted at, identity broker-based implementations.

Specifications Under Development

- International Government Assurance Profile (iGov) for OpenID Connect 1.0
- International Government Assurance Profile (iGov) for OAuth 2.0

Working Group Progress & Opportunities

The working group is reviewing input from MITRE on updating the Oauth profile to reflect upcoming changes in Oauth 2.1.

Input from Italy and other countries that have adopted the iGov profile and Connect Federation is being used to update the Connect profile.

A new implementer's draft is planed for Q2.

The goal is to have the profile final by the end of 2023 so that certification tests can be developed.

MODRNA Working Group

Bjorn Hjelm

Purpose

- **Support** GSMA technical development of Mobile Connect and similar industry and standards development.
- **Enable** Mobile Network Operators (MNOs) to become Identity Providers.
- **Developing** (1) a profile of and (2) an extension to OpenID Connect for use by MNOs providing identity services.

Participants and Contributors

Working Group Status

- Continuing to work on advancing working group drafts to Implementer's Draft status and support discussions across working groups.
- New documents include **CIBA Errata**, **CIBA Extension** and **IETF draft** to an IANA registry for CIBA endpoint parameters as well as discussions to create drafts for (3GPP) **MCX Profile** and profile for (GSMA) **RCS Verification Authority API**.
- Active engagement in **outreach** activities and serve as a **forum** for MNO engagement in the identity services ecosystem.

Specification Status

Final Publication status:

- CIBA Core

Implementer's Draft status.

- Authentication Profile
- Account Porting
- User Questioning API

Working Drafts status:

- MODRNA CIBA Profile
- Discovery Profile
- Registration Profile
- CIBA Core Errata
- CIBA Core Extension

MODRNA WG Collaborations and Outreach

1 *Evolution of **Mobile Connect** architecture, functionality and identity services to support new use cases.*

2 ***RCS** (Rich Communications Services) services and MaaP support for OpenID Connect.*

3 *Configuration of device-based services with embedded SIM (ODSA, C-V2X) leveraging OpenID Connect.*

3GPP Mission Critical Services

3GPP (Third Generation Partnership Project) Mission Critical (MC) services support PSA (Public Safety Agencies) and other critical communications.

Identity management is part of MC system security architecture and **OpenID Connect** MCX **Profile** defined for user authentication.

Development of **SEAL** (Service Enabler Architecture Layer) to support **vertical applications** (such as V2X) services is based on MC architecture.

Identity management is a common capability supporting **mission critical** and other **vertical applications**.

Liaison agreement with **ETSI** completed initial focus on **ETSI TC ESI** (Electronic Signatures and Infrastructure).

- European Telecommunications Standards Institute (ETSI)
  - ETSI supports the development and testing of global technical standards for ICT-enabled systems, applications and services.
    - Structure includes Technical Committees and industry specification groups.
    - Member of 3GPP and OneM2M partnerships.
  - Technical work covering multiple areas of digital communications and infrastructure.

Shared Signals

TIM CAPPALLI, CO-CHAIR

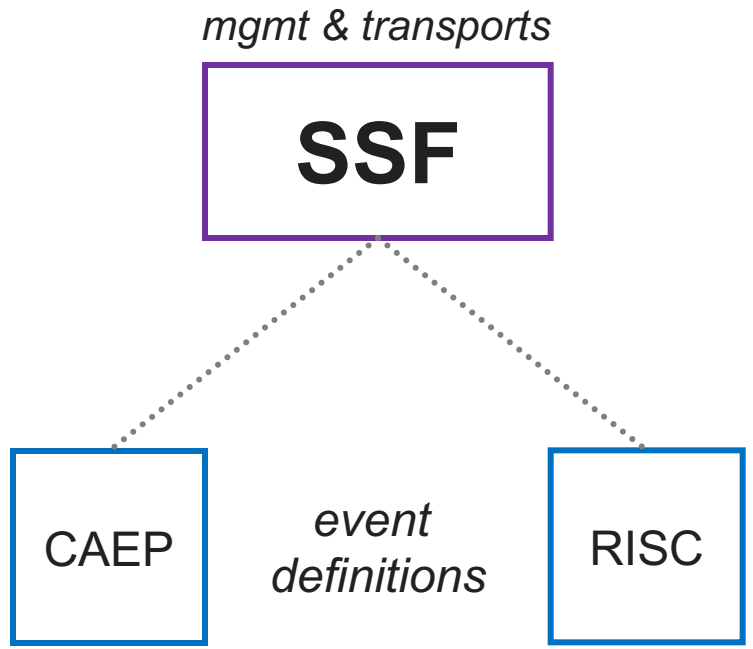
Working Group Overview

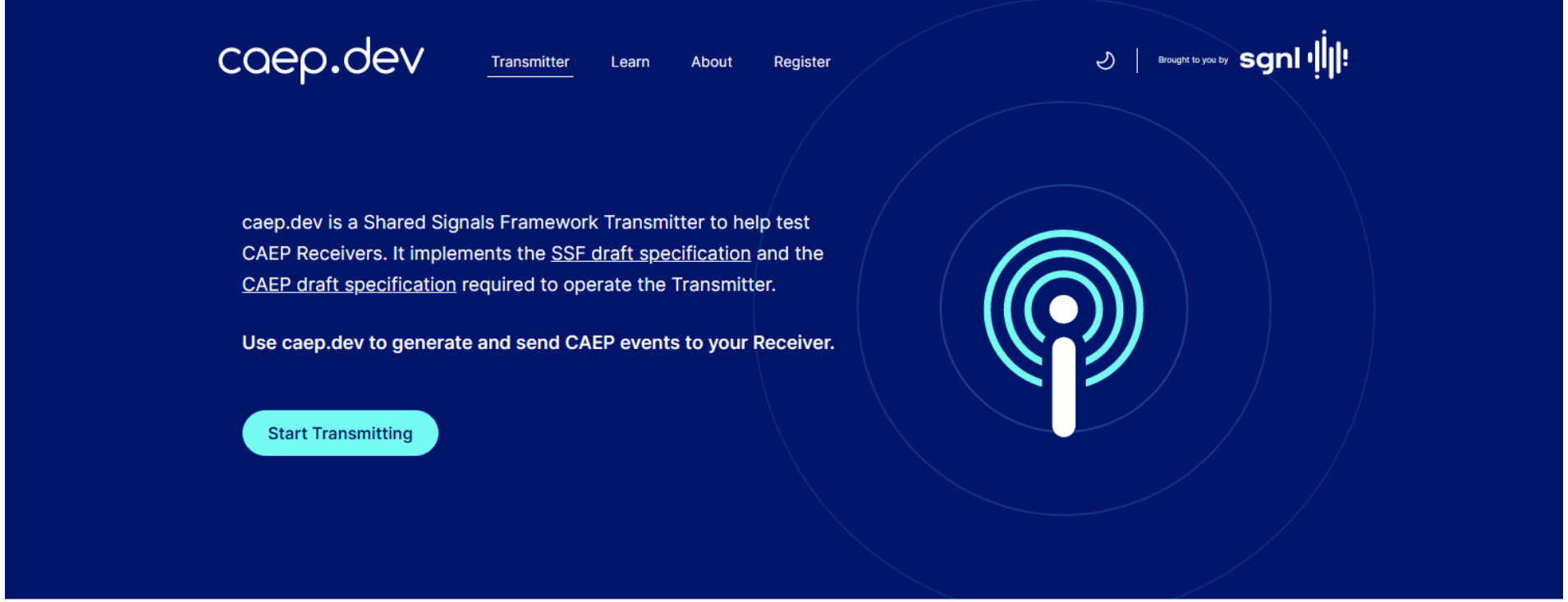
Objective of the Working Group

- Enable the sharing of security events, state changes, and other signals between related and/or dependent systems such as identity providers, risk engines, relying parties, device management platforms, network infrastructure, and policy engines

Specifications Under Development

- Shared Signals Framework (SSF)
- Continuous Access Evaluation Profile (CAEP)
- Risk Incident Sharing and Coordination (RISC)





CAEP Transmitter

Access Token

Don't have an access token? Register here

CAEP Event Type

Session Revoked

Getting Started

Register to get an access token and start sending CAEP events to your Receiver from this OpenID SSF Transmitter.

Check out our Instant Recipe to start transmitting in 4 simple steps.

OpenID

Working Group Progress & Opportunities

Focus Areas

- Implementer's draft feedback
- Issue backlog
  - Working through 30+ spec issues
- Overall spec cleanup
  - Fresh pass with new eyes
- Industry engagement
  - Evangelization at Gartner, EIC, and Identiverse

Lots of interest in the industry, but adoption remains a challenge

Working Group Roadmap

DATE	DELIVERABLES	ASPIRATIONS	NOTES
Q2 2023	< spec refinement >		
Q3 2023	- SSF implementer's draft #2 - CAEP implementer's draft #3		
Q4 2023		- Deployment guidance - SSF v1.0 - CAEP v1.0 - RISC v1.0	

Q&A &
Members Discussion

Gail Hodges & Nat Sakimura

Thank you.

Visit: www.OpenID.net