

OpenID Foundation Workshop

Tokyo

January 18, 2024





Welcome

Nat Sakimura – OpenID Foundation Chairman

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.

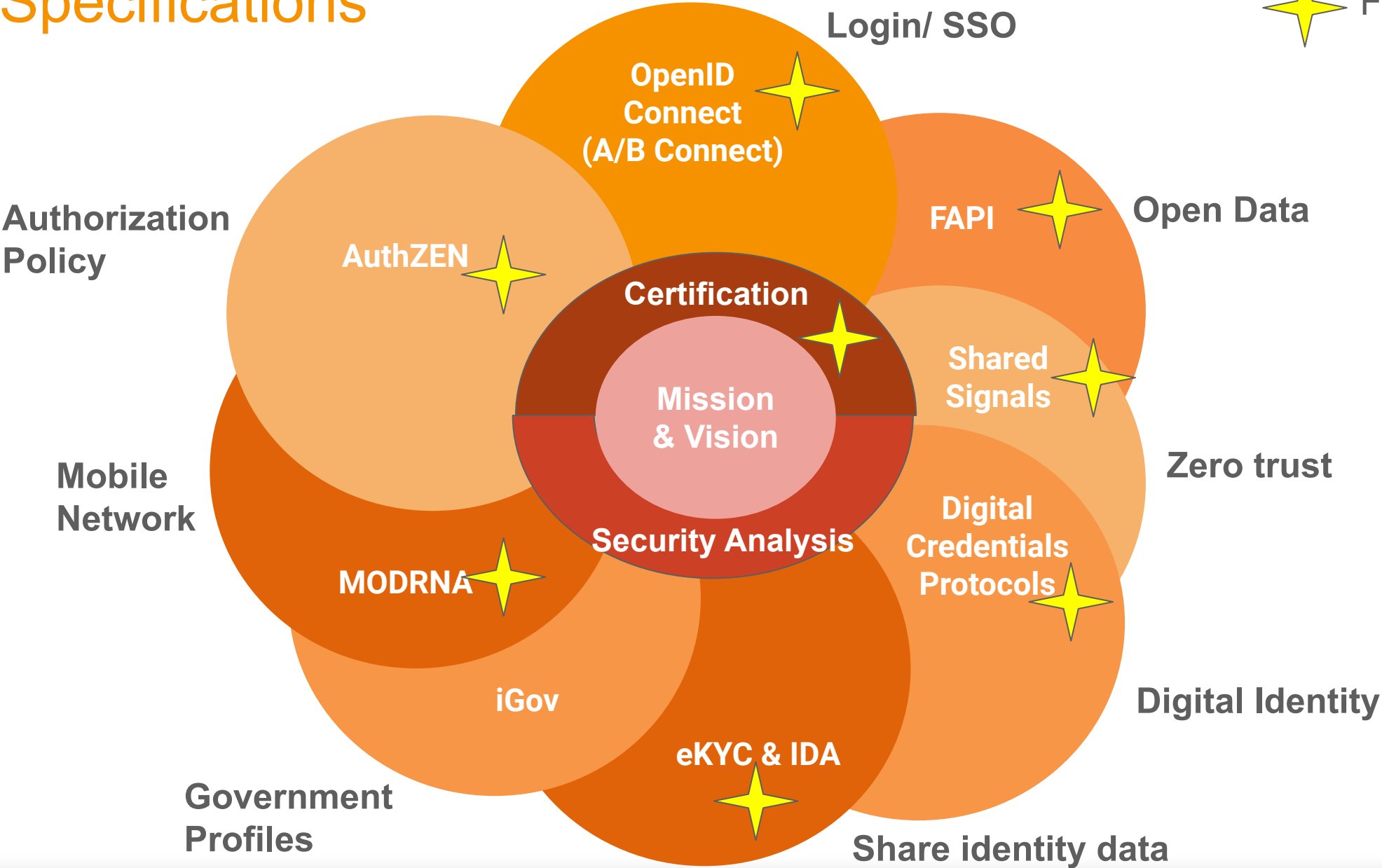
*****Please note that the workshop is being recorded and will be published to the OIDF website**

Thank you!



OIDF Specifications

★ Focus today



Workshop Agenda

TIME	TOPIC	PRESENTER
1:00-1:05	Welcome & Note Well Statement	Nat Sakimura
1:05-1:20	AuthZen WG Update	David Brossard
1:20-1:35	Shared Signals WG Update	Tom Sato
1:35-1:45	2024 OIDF Strategic Initiatives	Gail Hodges & Dima Postnikov
1:45-2:00	2024 OIDF-J Activity Plan	Naohiro Fujie
2:00-2:15	Connect WG Update	Michael Jones
2:15-2:30	eKYC & IDA WG Update	Mark Haine
2:30-2:45	MODRNA WG Update	Bjorn Hjelm
2:45-3:00	Digital Credentials Protocols (DCP) WG Update	Dr. Torsten Lodderstedt
3:00-3:15	FAPI WG Update & Ecosystem Engagement	Nat Sakimura, Elcio Calefi and Mike Leszcz
3:15-3:35	OIDF Certification Program Update Including Upcoming Conformance Tests	Joseph Heenan
3:35-3:55	SIDI Hub Brief	Gail Hodges, Mark Haine
3:55-4:00	Closing Remarks + Open Q&A	Nat Sakimura



OpenID Foundation Working Group Updates



AuthZEN Working Group Update

David Brossard

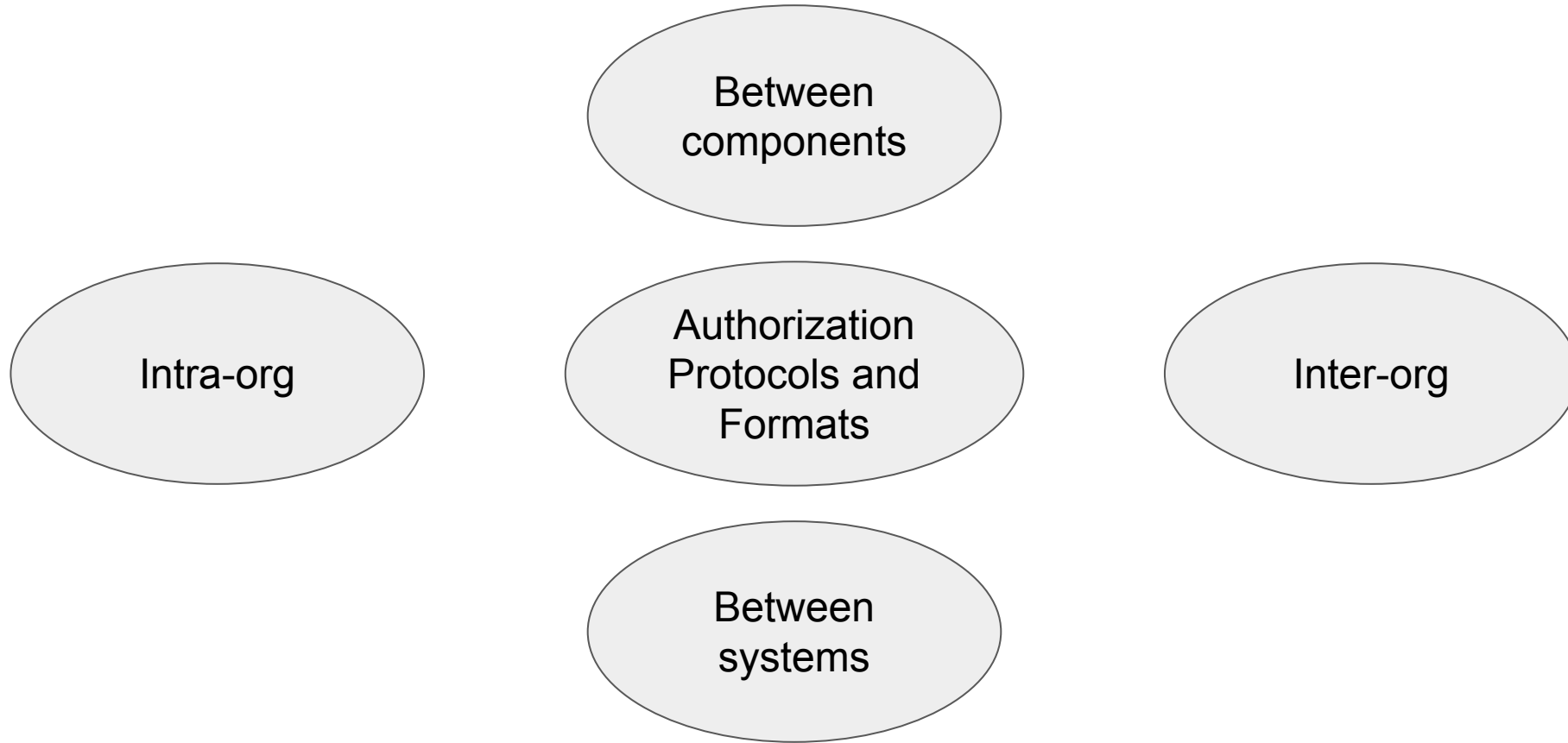
Why We Need an Authorization Working Group

- Majority of cyber attacks exploit identities
- Most attacks are successful because of over-permissioned users
- Turns even a single identity compromise into a potential catastrophe
- The #1 issue on OWASP's Top 10 is **A01:2021-Broken Access Control**
 - 94% of apps were tested for some form of broken access control.

Why We Need an Authorization Working Group (Contd.)

- Authorization is hard to manage in today's organizations
 - Authorization is siloed
 - Too many places to manage authorization
 - Each application “does its own thing”
 - There are clear gaps between silos
 - SaaS and cloud complicate matters
- No standardized widely-adopted way for AuthZ components to communicate
 - NIST ABAC and XACML are timid precursors
 - SaaS, COTS, and cloud services cannot talk to external AuthZ systems

Proposed Working Group Purpose



Scope and Objectives

- Increase interoperability between existing standards and approaches to authorization
 - Policy-based e.g. ALFA, Cedar, OPA (Rego), and IDQL,
 - Graph-based e.g. 3Edges and SGNL,
 - Zanzibar-inspired systems such as OpenFGA, Topaz and SpiceDB
- Standardize interoperable communication patterns between major authZ components
 - PAP, PDP, PEP, and PIP
 - See NIST ABAC's architecture
- Establish and promote the use of externalized authZ as the preferred pattern

Proposed Specifications

- Description of standard authorization patterns, use cases, communications patterns, and integration patterns
- An API to communicate authorization requests and decisions between Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) (which may be implemented by different parties)
- An API to communicate authorization policy and data from PAP to PDPs (which are implemented by different parties)

Anticipated Audience or Users

- Authorization developers and architects
- SaaS vendors (Multi client hosting)
- Cloud platforms
- Application vendors
- Enterprise implementers/practitioners who integrate authorization products





Proposers

- Alex Babeneau, 3Edges, alex@3edges.com
- Allan Foster, allan@macguru.com
- Atul Tulshibagwale, SGNL, atul@sgnl.ai
- David Brossard, Axiomatics, david.brossard@axiomatics.com
- Gerry Gebel, Strata Identity, gerry@strata.io
- Mike Kiser, SailPoint, mike.kiser@sailpoint.com
- Omri Gazitt, Aserto, omri@aserto.com
- Pieter Kasselmann, Microsoft, pieter.kasselmann@microsoft.com
- Steve Venema, ForgeRock, steve.venema@forgerock.com

Co- Chairs

- David Brossard (Axiomatics)
- Allan Foster
- Gerry Gebel (Strata Identity)
- Sean O'Dell (Disney)

Where to find us

- <https://openid.net/wg/authzen/>
 -  [Mailing List](#)
- Meeting notes & Design Documents
 -  HackMD: <https://hackmd.io/@oidf-wg-authzen>
- Github
 -  <https://github.com/openid/authzen>
- Slack
 -  [#wg-authzen](#)

January 2024 Update

- Prior Art Document
 - Deep dive into XACML, ALFA, Cedar, and OAuth
 - Comments welcome here: <https://hackmd.io/@oidf-wg-authzen/prior-art-pep-pdp>
- AuthZEN Interop Scenarios
 - <https://hackmd.io/@oidf-wg-authzen/InteropScenarios>
- Next steps
 - Panel submission at Identiverse 2024
 - Interop at Identiverse 2024 or EIC 2024

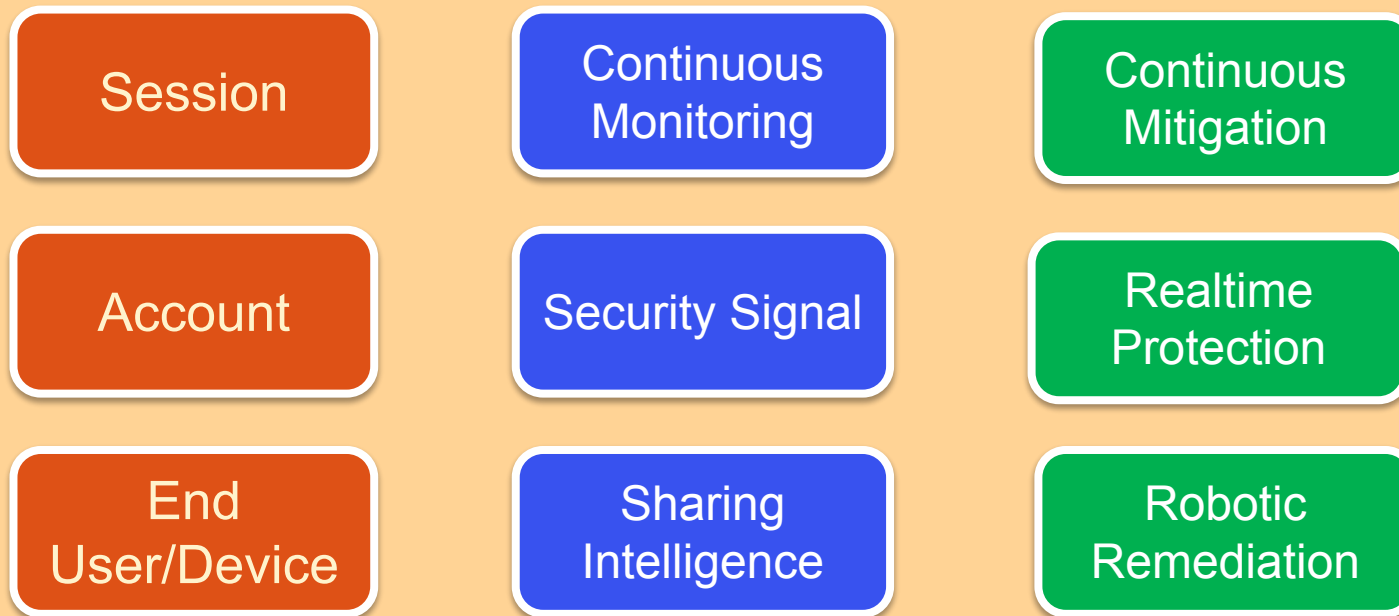


Shared Signals Working Group Update

Tom Sato, Shared Signals WG

Problem: Authentication only happens at the time of login

Shared Signal Framework



Shared Signal Framework Technical Overview



CAEP

RISC

CAEP :- Session control
RISC :- Account protection

Shared Signal Framework ID 2

Secure multi stream Webhook
communication layer

PUSH based SET
Delivery RFC 8935

POLL based SET
Delivery RFC 8936

Sub-ID for SET
RFC 9493

Security Event Token (SET) RFC 8417

IETF technology standards
used by the SSF Framework



JSON Web Token
RFC 7519

JSON Web Key
RFC 7517

JSON Web
Encryption RFC
7516



Working Group Activities Overview



Specifications Under Development

- Dec 2023 : Implementer's Draft 2 of Shared Signals Framework Approved
 - What's New in Shared Signal (Nov 2023)
 - SSF ID2 Spec Doc
 - Updates planned for CEAP, RISC Specs



Interoperability

- Shared Signals Framework InterOp Profile (On going)
 - CAEP Interoperability Profile 1.0 - draft 01
 - Call for Participation: Demonstrate Interoperability of your CAEP Implementations
 - Gartner Identity & Access Management Summit will be held in London on March 4-5th, 2024



Developer Events

- OpenID Summit Tokyo 2024 (SSF Technical breakout session) Jan 19th
- IIW Silicon Valley April 16-18
- Indenterverse May 28-31 2024 Las Vegas
- European Identity and Cloud Conference 2024 June 4-7 Berlin

Industry Updates and Progress

- Apple announcement “SSF with Managed Apple ID” Video– June 2023 WWDC
Third party Identity providers can now connect to Apple Business Manager by supporting OpenID Connect, SCIM and OpenID SSF. Currently Apple supports Microsoft Entra ID, Google Workspace and will open to other Identity providers.
- Okta announcement –June 2023
Okta's account security events (SSF) will allow Okta to notify Apple Business Manager whenever an important account security event (such as password reset) occurs.
- SGNL CAEP Transmitter announcement - caep.dev June 2023
Launch of a free, non-commercial online Continuous Access Evaluation Protocol / Profile (CAEP) Transmitter
- Microsoft Entra ID CAE updated developers guide released Oct 2023
The mechanism for this conversation is continuous access evaluation (CAE), an industry standard based on Open ID Continuous Access Evaluation Profile (CAEP)
- CISA/NSA report “Developer and Vendor Challenges Dec 2023
“These protocols (RISC and CAEP) enable identity providers and relying parties to exchange signaling around risk of particular sessions. Broad support for and development of these standards in the enterprise ecosystem will enable a variety of security use cases, ranging from limiting access to managed devices to quickly revoking access when accounts are compromised.”
- UK Digital Identity and Attributes Trust Framework Beta July 2023
WG submitted a set of recommendation to the UK Gov.
- SharedSignal Guide by Cisco
Developers guide to implementing SSF. Very thorough and easy to understand with set of sample codes for developers.

What's new in SSF ID 2 : Multi Stream Support Improved

Subjects

- Top-level sub_id claim. The draft now complies with the SubIds recommendation of using sub_id as the subject name and places it at the top-level of the SET.
- Format in complex subjects: "format": "complex"

Transmitter Metadata

- Well Known URL: The well-known URL of the Transmitter is now at /.well-known/ssf-configuration
- Spec Version: A Spec version field is now added to the Transmitter Configuration Metadata (TCM).
- Authorization Scheme: An authorization scheme has been added to the TCM to specify how the Transmitter authorizes Receivers.
- Optional jwks_url: jwks_url is now optional

Streams

- Multi-Stream Support: The draft now supports multiple streams between the same Transmitter and Receiver. The API has been modified to support creating such streams.
- Poll Delivery URL: The draft clarifies that the Transmitter must supply the endpoint_url field in the stream creation process. It also defines how the Transmitter can specify the poll URL.
- Status Restriction: The stream status methods now do not allow subjects to be included in Stream Status methods.
- Receiver Supplied Description: The Stream now includes a receiver supplied description
- “Control Plane” Events Always Included: Clarified language the control plane events (Verification and Stream Updated) are always delivered in the stream regardless of the stream configuration
- Events Delivered: The draft specifies that events_delivered is a subset (not necessarily a proper subset) of the intersection of events_supported and events_requested. Earlier, it was required to be the intersection.
- Reason in Status: The stream status now includes an optional reason string

Stream Events

- No Subjects in SSF “Control Plane” Events: The Stream Verification and Stream Updated events restrict the subject in these events to only reference the stream as a whole.

Authorization Scheme

- Authorization scheme is agnostic to the SSF. You can discover via TCM.
- InterOp recommends OAuth 2.0.



SSF Inter-Operability Event at Gartner IAM Summit UK

- Demonstrate standards-based interoperability with SSF, CAEP and RISC
- Commit to participate by Feb 2nd
- Pre-conference InterOp room on Mar 3rd
- Breakout session on Mar 4th - Erik Wahlstrom (Gartner) and Atul Tulshibagwale (OpenID SSWG)
- InterOp room available for appointments and demo
- Free booth within the InterOp room for participants
- Contact SSF WG for more details.

How to participate

- SSF WG HP
- <https://openid.net/wg/sharedsignals/>
- Subscribe to WG Mailing List
- Attend our WG Weekly meeting
- View our Specs
- Attend OpenID Workshop events
- We are at most IAM industry events



OpenID Foundation 2024 Strategic Initiatives

Gail Hodges & Dima Postnikov

OpenID Foundation 2023 Highlights

Gail

Specifications

- FAPI moving to FINAL imminently
- eKYC moving to final imminently
- OID4VCI moving to 1st Implementor's draft
- OID4VC Errata to Final, PAS submission

Certifications

- 692 certifications in 2023 vs 2,880+ since program start
- 500 certs for Brazil; 7 recertifications for OBIE UK
- 67 new certifications (Saudi, OPIN)
- 22 certifications of FAPI 2.0 completed by OPs & RPs

Adoption

- Billions of users, millions of applications use OIDC
- Millions of users hundreds of implementations of FAPI
- OID4VC named in EU ARF, selected by CA DMV
- Shared signals selected by Apple and named in CISA/NSA paper

“Lead the Community”

- Human-Centric Digital Identity (13 entities)
- Privacy-Preserving Digital Identity Credentials & Government Landscape (7 co-brand entities)
- GAIN in 2023 (6 cobrand partners)
- Open Banking Crossing Borders

Requests for Comment

- NIST SP 800-63-4 comments
- US CFPB Comments
- UK DIATF Comments
- ISO eKYC comments, ISO mDL liaison

Operations

- 60 net new memberships, of which 3 new Board members
- \$624k net contribution to cash
- OIDF Website refreshed, bylaws passed
- Kim Cameron Award-> DIAF

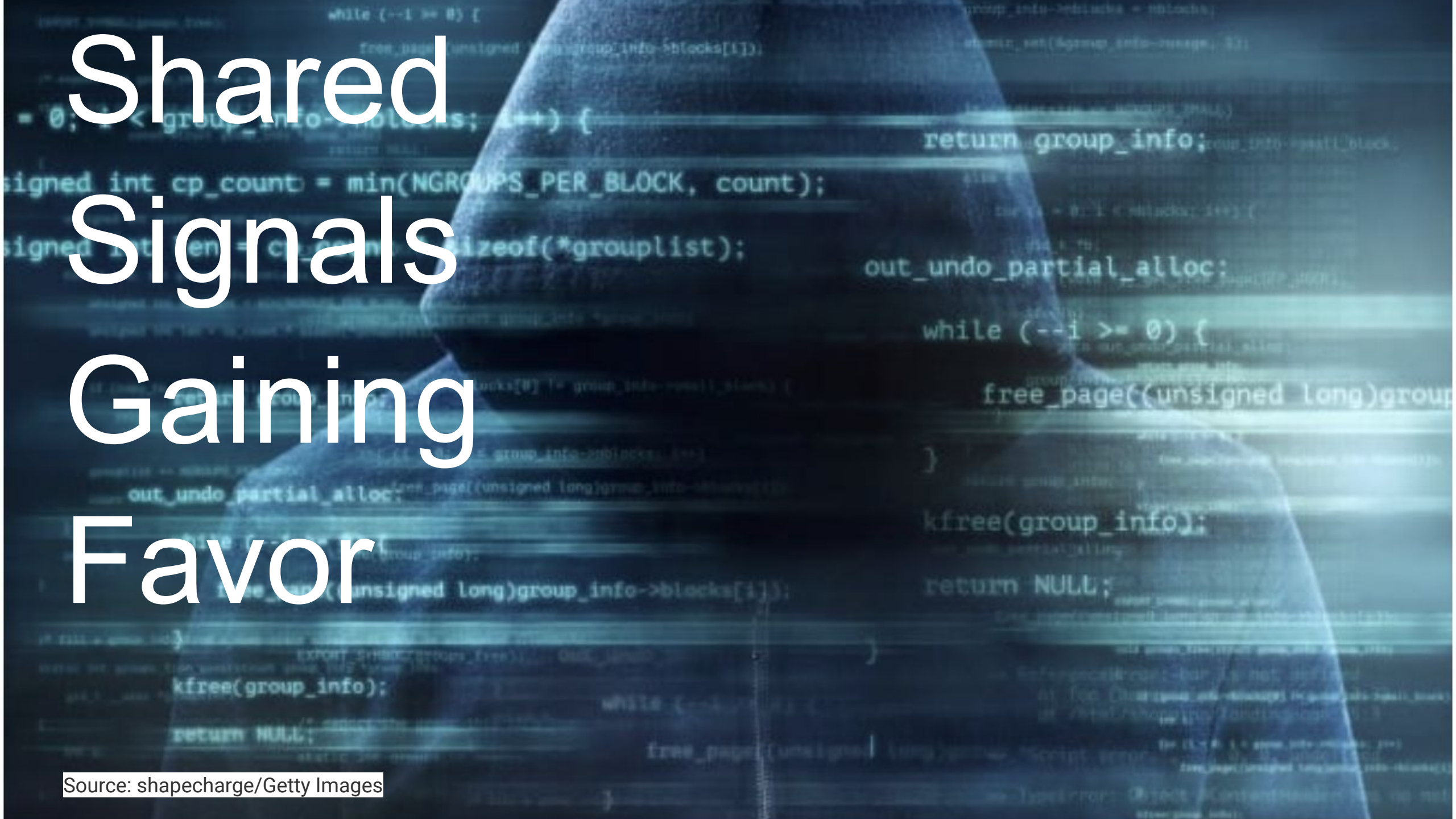




Can identity
be as easy to
transact with
as Currency?

A digital tunnel made of binary code (0s and 1s) leading to a bright light at the end. The tunnel is formed by concentric rings of binary digits, creating a perspective effect. The digits are in various colors like blue, green, and yellow. The light at the end is a bright, glowing circle.

Open
Data
Everywhere



Shared Signals Gaining Favor

Source: shapecharge/Getty Images

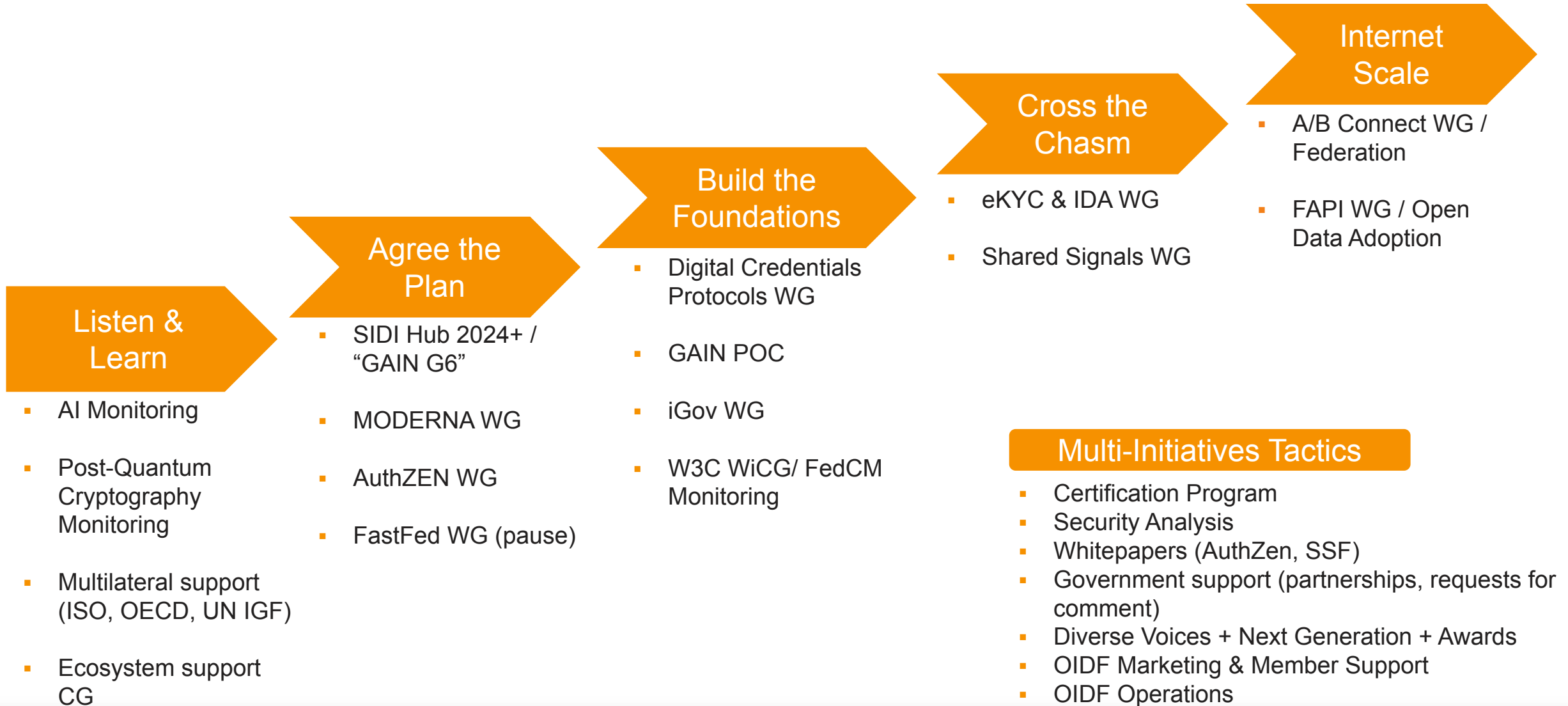


OIDF Connecting Ecosystems

sonian Magazine. "Do trees talk to each other?" Richard Grant, March 2018. A British Columbia rainforest, where Douglas firs soar
than 160 feet, supports 23 native tree species. Diàna Markosian.

2024 Initiatives

Dima





OpenID Foundation Japan Updates

Naohiro Fujie

OpenID Foundation Japan

Overview

- Established in 2008 to support the growth of the open API ecosystem in Japan through promoting of OpenID-related technologies. Aiming to enable Japanese industries to develop secure and privacy preserving digital identity environment.

Structure

- Board members
 - Naohiro Fujie, Masaru Kurahayashi, Yusuke Karasawa, Satoru Kanno
- Executive Director
 - Hiroko Soga
- Evangelists
 - nov, kura, ritou

members

6 Corporate members



Japan Digital Design



46 Members

ARIGATOBANK



未来のあたりまえをつくる。



信頼される安心を、社会へ。



OIDF-J activities - overview

- Local working groups
 - KYC WG
 - Translation and education WG
- Global and local events
 - OpenID Summit Tokyo 2024
 - OpenID BizDay, OpenID Technight, OAuth Immersion Workshop
- Other activities
 - Support the Japanese government initiative
 - Support higher education initiative

Local working groups activities: KYC WG

- Over 30 participants from Telco, Financial institutes, Japanese government, FIDO alliance Japan WG, etc.
- Focus on find out Japan specific use-cases for IDA adoption.
 - KYC for individuals
 - Adopt IDA spec for industries which are controlled by Japanese laws.
 - Adopt IDA spec for industries which are *NOT* controlled by Japanese laws.
 - KYC for legal entities
 - Find out requirement of KYC/KYB in B2B business.
 - Intent to enhance the Authority Claims profile in future.

KYC WG hosted event: OpenID BizDay #15

1月
10

[ハイブリッド開催] OpenID BizDay #15
OpenID Connect関連仕様の最新動向、KYC WG活動報告からGビズIDまでお届けします！

**OpenID BizDay
#15**

OpenID Connect 関連仕様の最新動向
KYC WG 活動報告から Gビズ ID までお届けします！



ハッシュタグ : #OpenID

募集内容	現地参加枠 (OIDF-J会員企業優先) 無料	先着順 (抽選終了) 56/100人
	リモート参加枠 無料	先着順 337/350人
参加者への情報	(参加者と発表者のみに公開されます)	

Agenda

- OpenID Foundation / OpenID Foundation Japan Activities Overview
- KYC WG Results Presentation ①: Consideration status on Next-Generation KYC
- Consideration status on Corporate KYC
- Latest information on OpenID Connect for Identity Assurance, DID, Verifiable Credentials specifications
- Latest information on Financial-grade API (FAPI)
- Latest developments on G-Biz ID (Digital Agency)

The number of participants
Offline : 56
Online : 337

Reference : Connpass Registration

Digital Identity Verification Guidelines for private enterprises

- A guideline which was developed through collaboration with the Digital Agency, and experts from over 10 member organizations.
- The guideline envisions enterprises to choose identity verification methods tailored to their own services.
 - Mainly focus on private enterprises which are not controlled by laws.
- The Digital Agency has released a similar guidelines for government services.
 - They are updating their guidelines and refers our guideline.
 - Nat and Naohiro are supporting the Digital Agency for update.

Local working groups activities: Translation&Education WG

- Translated NIST SP800-63-4 draft into Japanese
- Hosted event to introduce NIST SP800-63-4 in Japanese
- In 2024, OIDF-J decided divide this WG into two WGs
 - Translation WG
 - Translate OpenID related specs or guidelines into Japanese language.
 - Digital Identity Talent Development WG
 - Cultivate and educate individuals who would be an expert in the identity space.

Translation&Education WG hosted event: OpenID BizDay #15

3月
16

OpenID BizDay #16 – NIST SP800-63-4 (Draft)

OIDF-J 翻訳WGによる NIST SP800-630-4 (draft) 翻訳版公開記念

ハッシュタグ : #sp800_63_4

フォロー参加者



募集内容	現地参加枠 (会員企業優先) 無料	先着順 (抽選終了) 40/80人
	リモート参加枠 無料	参加者数 372人

参加者への情報

(参加者と発表者のみに公開されます)

この度は「OpenID BizDay #16 – NIST SP800-63-4 (Draft)」へお申込みいただきありがとうございます。

▼開催日時▼
2023年3月16日 (木) 19:00 – 21:00 @東京ミッドタウン

▼当日オンサイトで参加される方▼
18:30から受付開始しますので connpass の受付票を持って会場へお越しください。
[東京ミッドタウンカンファレンス](#) (東京ミッドタウン4F)

▼YouTube Live 配信 (限定公開) で参加される方▼
https://youtube.com/live/_li3a0VYRnc

みなさまのご参加お待ちしております。

OpenIDファウンデーション・ジャパン

- SP800-63-4 Digital Identity Guidelines
 - Noboru Kurumai / Transmit Security
- SP800-63A - Enrollment & Identity Proofing
 - Tatsuya Katsuhara / Amazon Web Services Japan G.K.
- SP800-63B - Authentication & Lifecycle Management
 - Hitomi Kimura / Trend Micro Inc. (United States)
- SP800-63C - Federation & Assertions
 - Nov Matake / OpenID Foundation Japan Evangelist and Translation WG Leader

The number of participants

Offline : 40

Online : 372

Reference : Connpass Registration

OpenID Summit Tokyo 2024

Tomorrow! In person only, recordings will be on Youtube after while.

OpenID Summit TOKYO 2024

Summary

Program

OpenID Foundation Hybrid Workshop

X Post

Like

Beyond the Decade: The Evolution and Future of OpenID

It's been 10 years since OpenID Connect 1.0 was specified, and four years have passed since the OpenID Summit Tokyo 2020, through the challenges of the COVID-19 pandemic.

During this time, how have digital IDs changed our lives, and how will they shape our world in the present and future?

Digital ID specialists from both within Japan and abroad will extensively discuss the latest profiles of OpenID Connect, from both business use-case and technology perspectives.

We warmly invite all those interested in digital ID to join us.

Registration: register today (<https://openidsummittokyo2024.peatix.com/>)

Capacity: 270 (Admission free)

Event date and time: Friday, January 19, 2024, 10:00 - 18:00

Event Location: Shibuya Stream Hall Shibuya 3-21-3, Shibuya-ku, Tokyo, Japan

Other activities: supporting Gov, academic initiatives

- The Japanese government
 - The Cabinet Secretariat of Japan
 - Trusted Web Promotion Council Taskforce, I14N Sub Working Group
 - The Digital Agency
 - Identity verification guideline taskforce, Digital Identity Wallet project
- Standardization support organization
 - JIPDEC(Japan Information Processing and DEvelopment Center)
 - Blockchain Standardization Investigation Committee
- Higher education institutes
 - National Institute of Informatics
 - The next generation academic federation and trust framework working group
 - AXIES(Academic eXchange for Information Environment and Strategy)
 - VC on educational sector standardization working group(planned)

Trusted Web Promotion Council

- An Initiative following to the concept of the DFFT(Data Free Flow with Trust) agreement at G7/G20.
- Aims to build a new trust framework in digital society and enable various parties to create new values.
- Published a white paper through PoC projects, mainly using OpenID for Verifiable Credentials related specs.
- OIDF-J supports their activities by participating in meetings and promoting the application of the latest specifications.
- The Japanese government is going to present their initiative at the OpenID Summit Tokyo tomorrow.



OpenID Foundation Working Group Updates



OpenID Connect Working Group

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 Federation, and is the home of OpenID for Verifiable Credentials
- Transfer of the OpenID4VC specs to the newly formed Digital Credentials Protocols (DCP) working group is anticipated after OpenID Connect WG Implementer's Drafts are approved
- See the list of specs with descriptions at <https://openid.net/wg/connect/specifications/>

Final 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 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 October

- WGLC for first proposed Implementer's Draft of OpenID for Verifiable Credential Issuance
- Multiple OpenID Connect Federation drafts published
 - Working towards final Implementer's Draft
- Updated OpenID4VC drafts published (described in a different presentation)
- Second set of OpenID Connect Errata drafts published!
- Submitted OpenID Connect specs for ISO Publicly Available Specification (PAS) status

Challenges and opportunities facing the working group

- OpenID Federation deployments
 - Production use in Italy, both for national federations and EU wallet ecosystem
 - Proof-of-concept deployment in Sweden
 - Possible deployments in other nordic countries
- Relationships with digital wallet initiatives and national identity systems worldwide
- Finish Implementer's Drafts of all OpenID4VC specs
 - Enabling transfer to Digital Credentials Protocols (DCP) working group

Working Group Roadmap

DATE	DELIVERABLES	ASPIRATIONS	NOTES
Q1 2024	Next Federation Implementer's Draft	Bring text up to OpenID Connect quality standards	We can discuss specifics this week
Q1 2024	OpenID4VCI Implementer's Draft	First Implementer's Draft	Following 45-day review and vote
Q2 2024	Other OpenID4VC Implementer's Drafts	Lock in IPR within Connect WG	Enabling transfer to DCP WG
Q3 2024	Final Federation Spec	Trust establishment for broad set of use cases	Having Final spec will accelerate deployments

Discussion

What do you want the OpenID Connect working group to accomplish during our time in Japan?



eKYC & IDA Working Group

Mark Haine

Working Group Overview

Objective of the Working Group

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

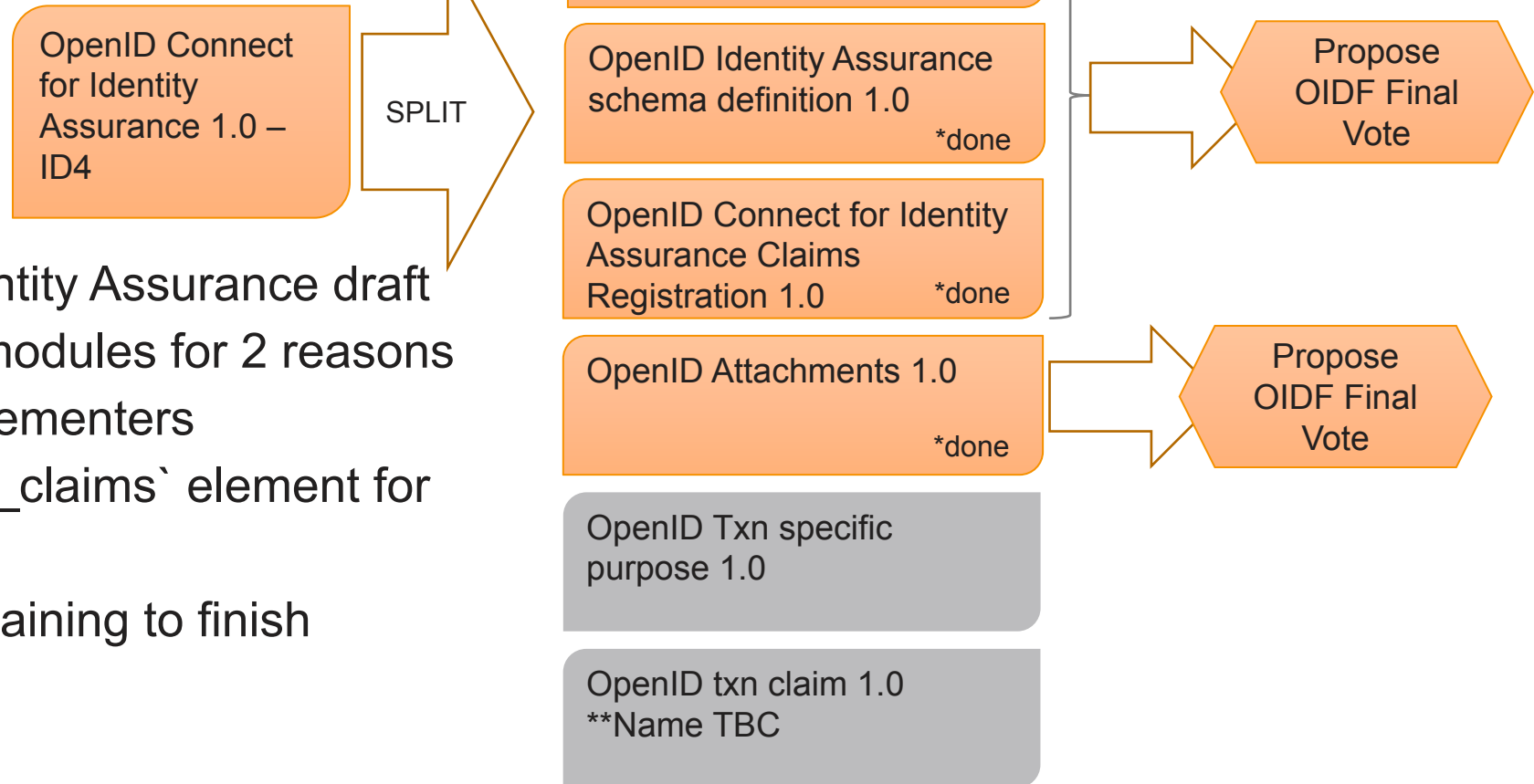
Published Specifications

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

Working group deliverables since last workshop in April

- We took a big decision to modularize the OpenID Connect for Identity Assurance draft
- More on next page

Working Group Progress



Modularization

- The Current OpenID for Identity Assurance draft is being split into separate modules for 2 reasons
- Easier consumption by implementers
- Easier reuse of the `verified_claims` element for example by OID4VC drafts
- Small number of issues remaining to finish

External achievements

- OIX recommendation to base Identity Assurance standards for interoperability on the work of the eKYC & IDA WG

Link: [OIX Data Standards recommendation](#)



MODRNA Working Group

Bjorn Hjelm

Working Group Overview

Objective of the Working Group

- **Support** Mobile Network Operator (MNO) community and the identity ecosystem by developing technical standards to **enable** MNOs to become Identity Providers as well as exposing applicable APIs by **developing** (1) a profile of and (2) an extension to OpenID Connect for use by MNOs providing identity services.

Published Specifications

- Final – CIBA Core
- Implementer's Draft – MODRNA Authentication Profile, Account Porting, User Questioning API

Specifications Under Development

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

Working Group Progress & New Opportunities

The Working group is working on new documents including **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**.

The Working Group is actively engaged in **outreach** activities including the following:

- Updates (to increase the engagement between the organizations) to the liaison agreement with **ETSI** (European Telecommunications Standards Institute) completed and approved.
- Based on the liaison agreement with **CAMARA Project**, a Linux Foundation project, engagement to assist in the development of APIs (to enable seamless access to Telco network capabilities) has started with FAPI specifications overview presentation (to Identity and Consent Management SP) and forthcoming eKYC-IDA WG overview presentation (to KnowYourCustomer SP).
- Continue to work on establishing a formal liaison agreement with **GSMA** to facility the open exchange of information between the organizations across working groups.

Current Working Group Roadmap

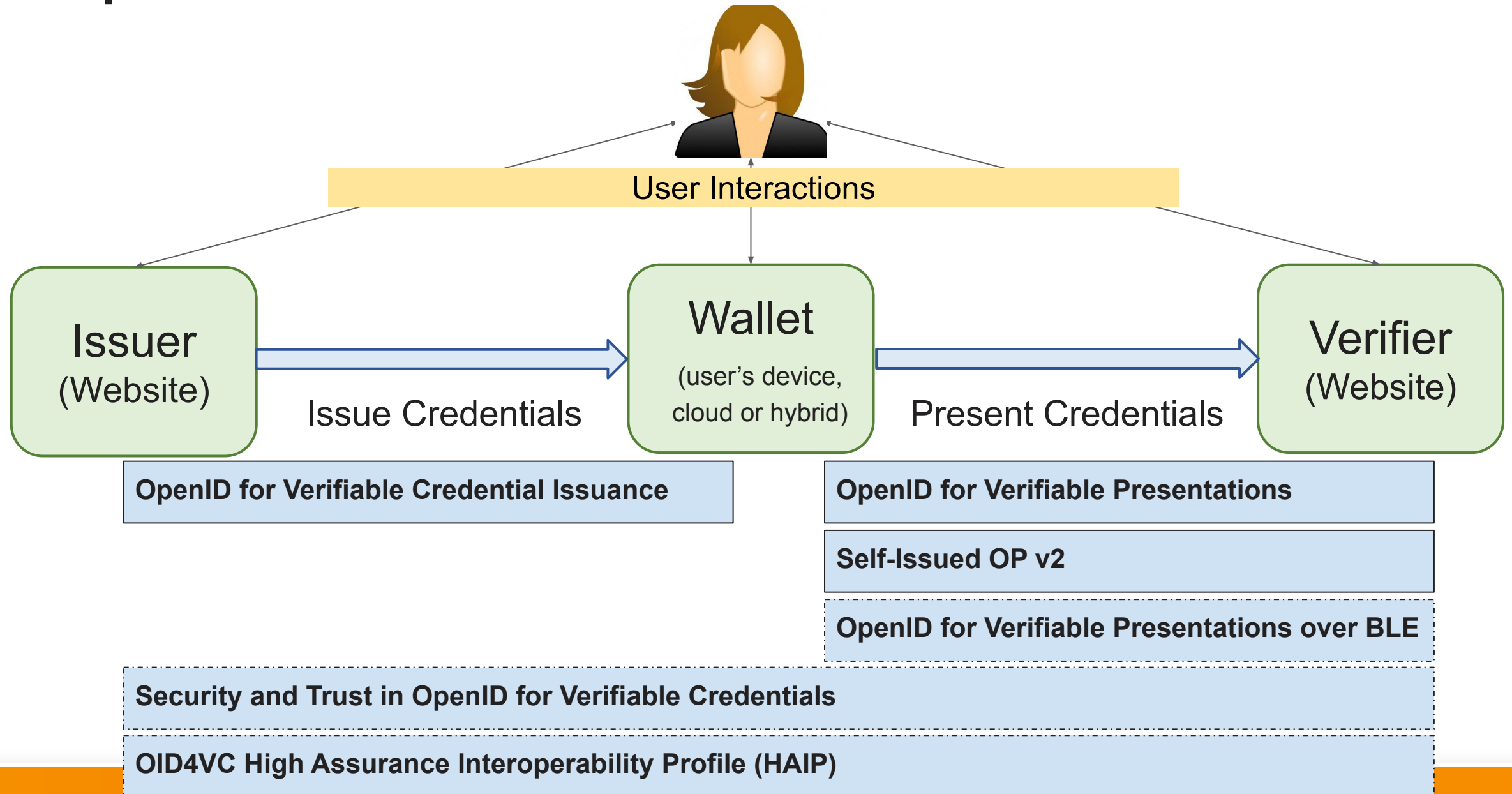
DATE	DELIVERABLES	ASPIRATIONS	NOTES
Q1 2024	<ul style="list-style-type: none">▪ IETF draft (IANA Registry)▪ MODRNA CIBA Profile (Implementer's Draft)▪ MODRNA Discovery Profile (Implementer's Draft)	<ul style="list-style-type: none">▪ Liaison Agreement with GSMA	<ul style="list-style-type: none">▪ Active engagement with CAMARA Project
Q2 2024	<ul style="list-style-type: none">▪ MODRNA Registration Profile (Implementer's Draft)▪ CIBA Errata draft▪ CIBA Extension draft		
Q3 2024			



Digital Credentials Protocols (DCP) Working Group Deeper Dive

Torsten Lodderstedt

OpenID for Verifiable Credentials



Progress

- We have a new Working Group and migrated to Github ;-)
- We have the first conformance tests
 - OID4VP baseline with SD-JWT VC
- OID4VP mdoc profile successfully tested
 - ISO 18013-5/-7 Test Event (SpruceID)
- Formal Security Analysis completed
- Supported eIDAS ARF/Expert Group
- WG adopted OID4VC High Assurance Interoperability Profile (HAIP)
- Incorporated almost all implementers feedback into OID4VCI

Implementations

- Lots of new implementations
 - e.g. Aries JavaScript Framework (AJF), .NET Wallet Framework (previously Aries .NET Framework), eIDAS 2.0 Reference Wallet Implementation, Bundesdruckerei, Impierce Technologies, AltMe, Italian Government.
- Increasing number of open source projects
 - e.g. Ping Identity, .NET Wallet Framework, MOSIP (OWF) and AJF (Hyperledger Aries)
- OID4VC Due Diligence Task Force at OWF
- Lot of implementers feedback

Next Steps

- Start Implementers Draft process for OID4VCI after WGLC
- Evolve OID4VP and HAIP
- OID4VCI: full lifecycle support for unlinkable credentials
- Extend conformance tests
- Continue eIDAS support, e.g. through contribution of HAIP to eIDAS expert group
- Support NIST NCCoE
- Contribute to Browser API discussions at W3C WICG



FAPI Working Group Update & Ecosystem Engagement

Nat Sakimura, Mike Leszcz & Elcio Calefi

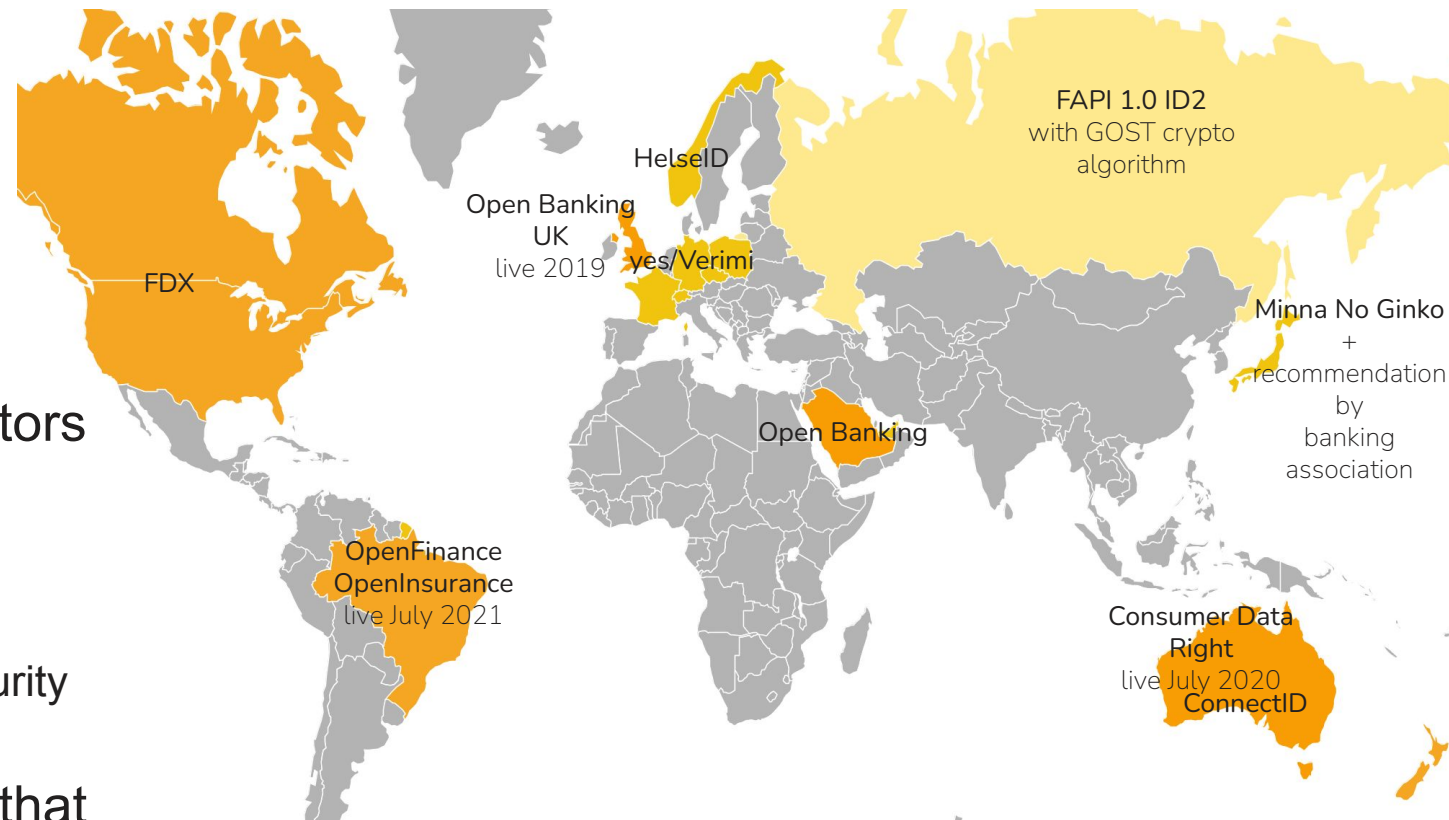
Working Group Overview

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, FDX, KSA, Canada/US
 - Thanks to Australia sponsoring FAPI2 security analysis!
- 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
- [FAPI 2.0 Message Signing](#) – an extension of the baseline profile that provides non-repudiation for all exchanges including responses from resource servers
- [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

Working Group Progress & Opportunities

White Papers

- "Open Banking, Open Data, and the Financial Grade API" - 2022
- "Open Banking and Open Data: Ready to Cross Borders?" - 2023

Formal Analysis

- FAPI 2.0 Security Profile analysis complete
- FAPI 2.0 Message Signing, CIBA, DCR / DCM (Dynamic Client Registration/Management) complete

Certification

- Thriving for FAPI 1.0.
- FAPI 2.0 tests delivered, certification gaining momentum
 - Multiple vendors / banks / fintechs certified
 - Existing and prospective implementors encouraged to consider FAPI 2.0 in roadmap

Working Group Roadmap

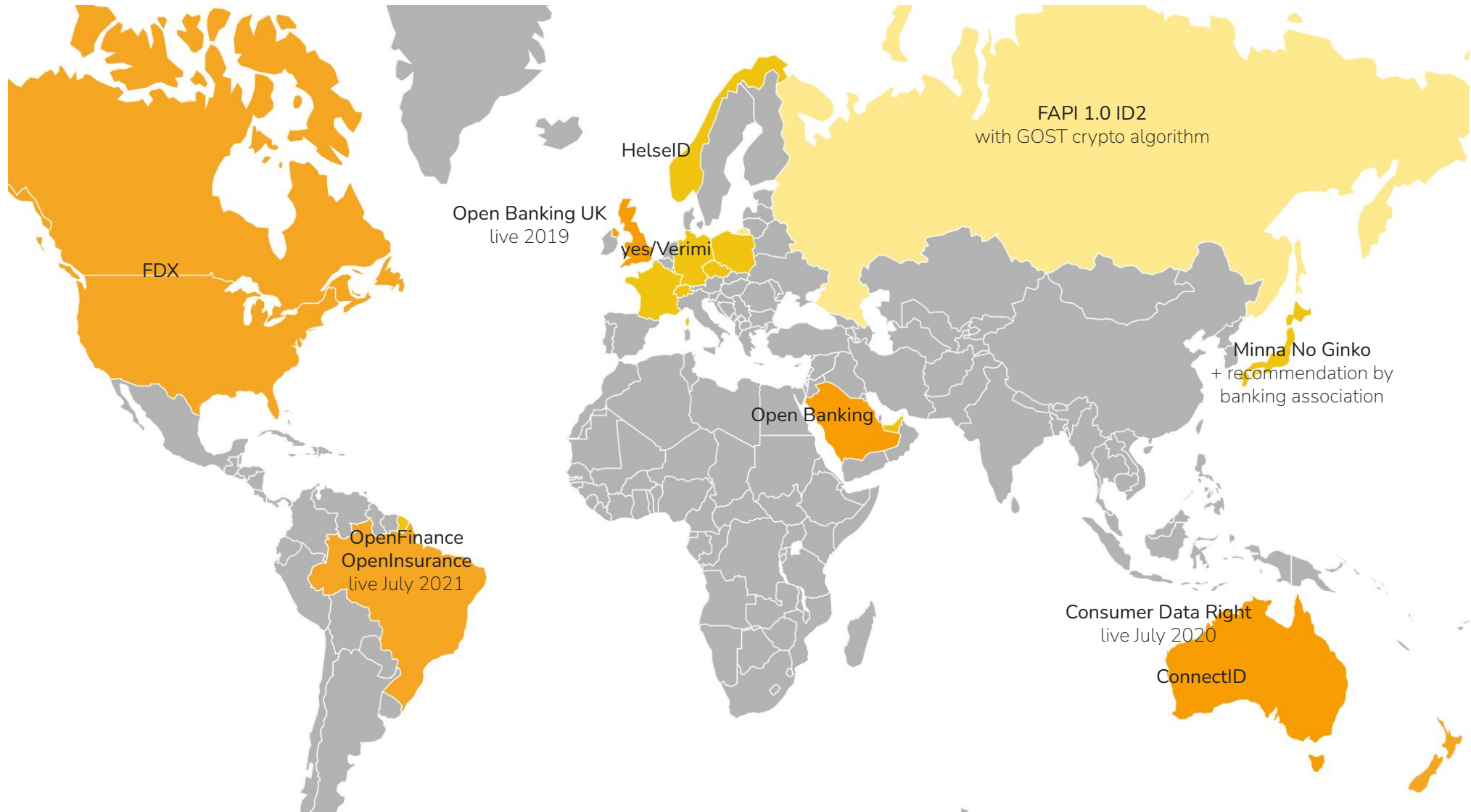
DATE	DELIVERABLES	ASPIRATIONS	NOTES
Q4 2023	Formal Verification for FAPI 2.0 Message Signing, DCR, and CIBA FAPI 2.0 Message Signing -- 2 nd Implementer's draft	End Oct WG Signoff Australian Gov't notification of WG sign-off	
Q1 2024		FINAL for FAPI 2.0 specs.	









FAPI Ecosystem Engagement

Mike Leszcz

The Evolving Landscape



FAPI Landscape Update

 OBIE (Gov't)	 Open Finance (Gov't)	 Open Insurance (Gov't)	 CDR (Gov't)	 ConnectID (Private)	 SAMA (Gov't)
<ul style="list-style-type: none">▪ OIDF Certification (partial mandatory CMA9, annual)▪ Local profile▪ 64 IdP entities certified	<ul style="list-style-type: none">▪ OIDF Certification (mandatory, annual)▪ Local profile▪ Board member▪ Community group pilot▪ Hundreds of IdP & RP entities certified▪ 2024 recertification in Q1	<ul style="list-style-type: none">▪ OIDF Certification (mandatory)▪ Local profile▪ 47 IdP and 45 RP entities certified	<ul style="list-style-type: none">▪ Selected FAPI 1.0, moving to FAPI 2.0▪ Co-funded mathematical Security Analysis by Stuttgart University FAPI 2.0 Baseline complete▪ FAPI Message Signing and CIBA completed - awaiting FAPI WG feedback	<ul style="list-style-type: none">▪ ConnectID, co-funded conformance tests via directed funding▪ OIDF pilot to bundle specifications▪ Board member▪ 5 IdP and 9 RP entities certified to ***FAPI 2.0***	<ul style="list-style-type: none">▪ OIDF Certs. (Mandatory)▪ Local KSA profile▪ 17 IdP and 12 RP entities certified

FAPI Landscape Update



Open Banking Canada (Gov't)

- Open Banking Canada Feedback
- FDX selected FAPI 1.0
- Report completed and is under review. Will be released soon.
- FDX discussions renewed on combined certification to streamline FDX member journey



Norway Norsk Helsenett (Gov't)

- Selected FAPI 2.0
- Deployed in to nearly all healthcare personnel (250k) and providers (7.5k)
- OIDF Workshop presentation @ EIC & OAuth Workshop



Japan Minna Bank (Private)

- Selected FAPI for Minna Bank to x-sell of Insurance with partners



Germany (Private)

- yes.com - private-sector open banking ecosystem
- Selected FAPI 2.0



CFPB / FDX (Gov't / Private)

- CFPB feedback
- FDX selected FAPI 1.0 Advanced, considering path to FAPI 2.0
- FDX discussions renewed on combined certification to streamline FDX member journey
- Awaiting initial rulemaking to review and comment – anticipated this week

FAPI Landscape Update



Open Banking
UAE
(Gov't)

- Selected FAPI
- Requested certification program support



Open Banking
Colombia
(Gov't)

- Draft regulations confirm FAPI 2.0 selected
- Briefed a leading bank, requested regular contact


Note: Local entities in New Zealand (live, small scale) and Nigeria also selected FAPI.





Open Finance Brazil FAPI Adoption

Elcio Calefi



Enabling an digital economy in Brazil

Innovation, Security and inclusion

Elcio Calefi

AGENDA SLIDE

1

The Brazilian Scenario

2

Open Finance Brazil

3

Security Agenda (FAPI, Profile Simplification)

Innovation in the financial system

Convergence



Financial innovation



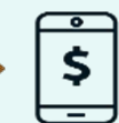
Intensive use of
clouding



Innovation in the SFN



- Simplification
- Internationalization
- Convertibility



Digital
currency

Brazil Financial Initiatives



20 Billions

Api calls since 2022

27 Millions

of given consents

**550
thousands**

Payments done
since Sept. 2022

+ 800

registered financial
institutions

17 PISPs

Certified Payment
Initiation Providers

+ 500

People from various
institutions



687 Millions

of registered keys

4,1 Billions

of transactions in
out/23, against 2,4
billions in out/22,
growth of **67,8%**.

144 Millions

of people using PIX

13,3 Millions

of companies PIX

R\$ 169

Millions

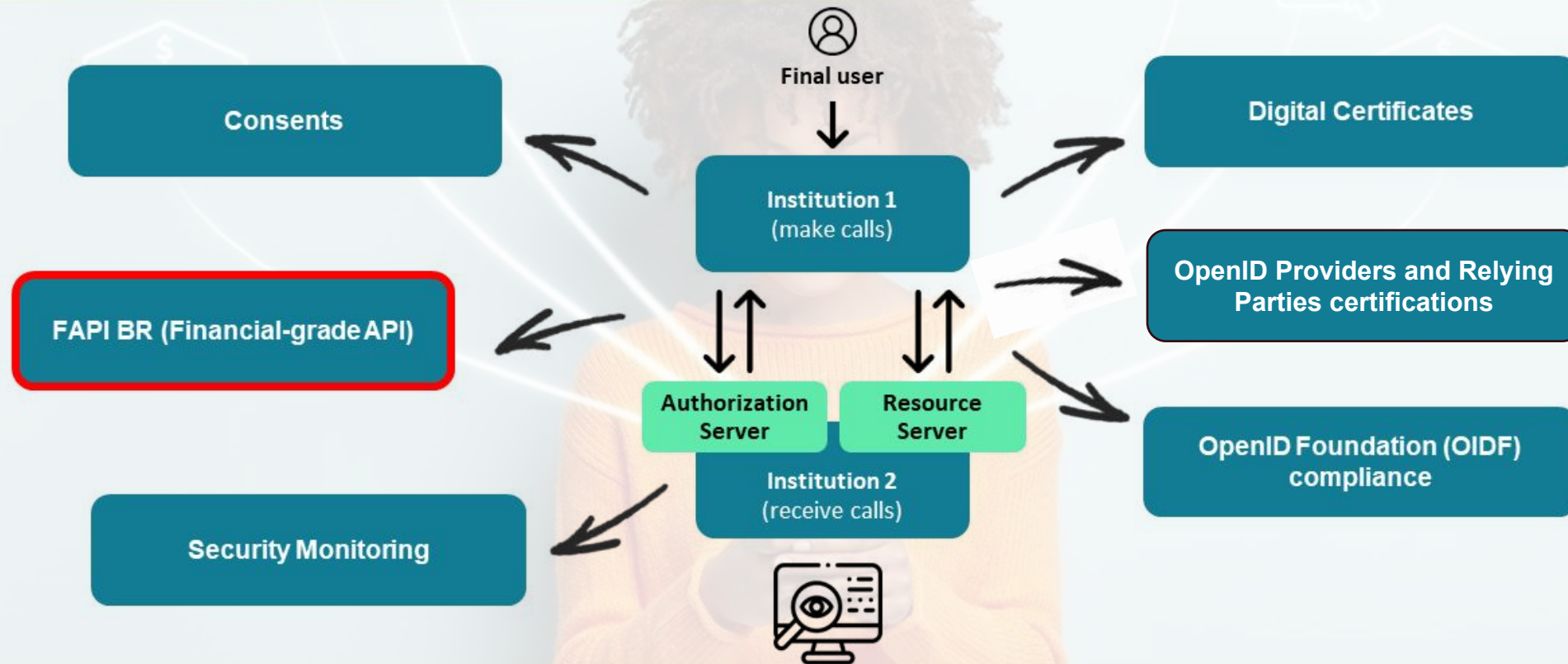
Daily operations



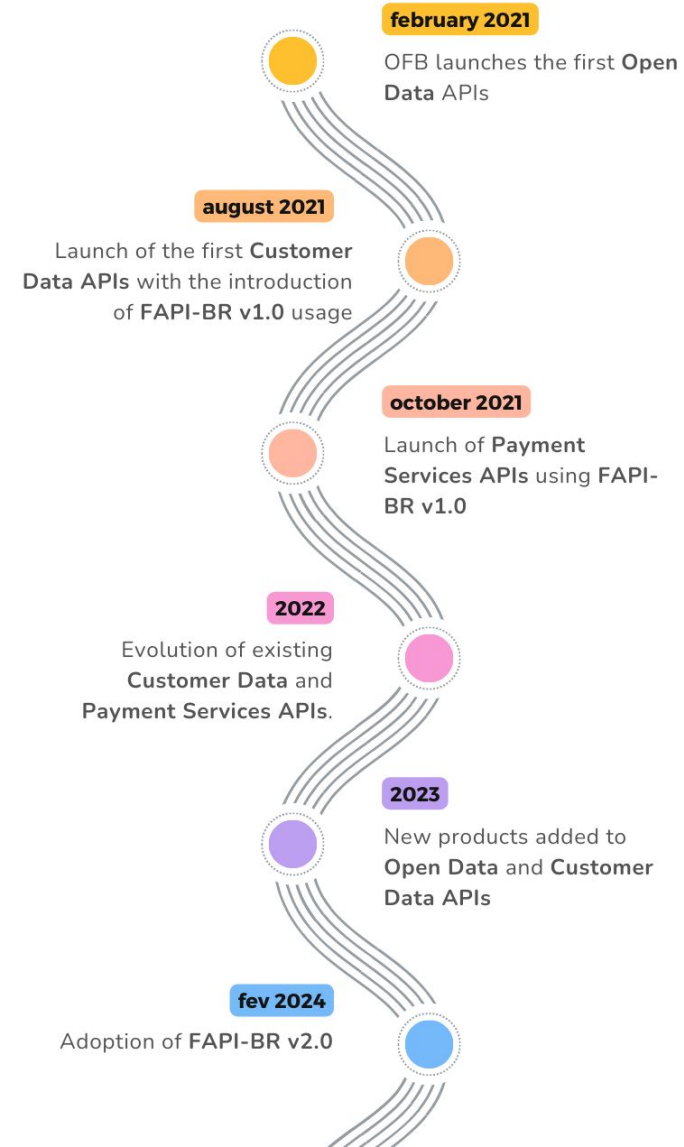
The Banco Central do Brasil (BCB) is developing Drex, the Brazilian real in a digital format, so that more people would have access to:

1. Transactions of traditional products and services, such as investment and financing, with higher safety
2. Smart contracts – which implement intermediation protocols for the purchase and sale of financial products and services – in an easy and innovative manner
3. New types of digital financial products and services.

Open Finance – Cybersecurity components



Roadmap – FAPI-BR



What is FAPI-BR?

FAPI-BR profile describes security and features provisions for a server and client that are necessary for the Brazil Open Finance Programme by defining the measures to mitigate or address:

- attacks that address privacy considerations identified in clause 9.1 of [FAPI1 Advanced]
- the requirement to support fine-grained access to resources for data minimisation purposes
- the requirement to convey the Authentication Context Request that was performed by an OpenID Provider to a Client to enable a appropriate client management of customer conduct risk.

FAPI-BR v1 Features

- Uses [FAPI1 Advanced] as base
- Focus on reducing the entry barrier for the participants.
- Offered 8 FAPI profiles (variations with mtls, private-key, PAR, and JARM), allowing multiple alternatives to enable most technology providers
- **Consequence:** greater implementation effort for RPs, as they need to be capable of integrating with various distinct profiles, resulting in interoperability issues among institutions.

FAPI-BR v2 Features

- Uses [FAPI1 Advanced] as base
- Focus on simplifying the ecosystem and easing interoperability.
- Adopts a single FAPI profile: private-key-jwt with the use of PAR.
- Seeks changes that move towards FAPI 2.0, such as mandatory use of PAR and PKCE.



THANK YOU!

**ANY
QUESTIONS?**



Certification Program Update

Joseph Heenan

Certification Overview

Objective

- Encouraging interoperable and secure implementation of OpenID Foundation specifications through open-source testing tools & self certification

Current Certification Programs

- OpenID Connect, OpenID Connect Logout, FAPI1-Advanced, FAPI2 Security Profile ID2, FAPI2 Message Signing ID1 (partial), FAPI-CIBA ID1

Tests Under Development

- OpenID For Verifiable Presentations (beta available)
- OpenID Connect For Identity Assurance (beta available)
- FAPI2 DPoP, HTTP Signatures
- OpenID For Verifiable Credential Issuance

Future Roadmap

- OpenID Federation (directed funding received from ConnectID, thank you!)
- FAPI2-CIBA
- OIDF-J/ Japan Gov collaboration (directed funding anticipated for OID4VC tests)

Progress & Opportunities

Working group deliverables last 6 months

- FAPI1-Adv New, simplified OpenFinance Brazil profile
- FAPI1-Adv KSA OpenBanking profile
- FAPI-CIBA RP tests
- FAPI2 OP & RP tests
- FAPI2 ConnectID Profile
- Tackling some technical debt & bringing many dependencies up to date

USA & Canada OpenBanking reports from government due to drop during 2024

- Expected to endorse FAPI & FDX in some way
- Waiting to see what they might say about certification



SIDI Hub Brief

Gail Hodges & Mark Haine



SIDI HUB

Sustainable & Interoperable Digital Identity

January 18, 2023

Sustainable Digital & Interoperable Digital Identity © 2023 SIDI Hub Community is licensed under CC BY 4.0.
To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>

International interoperability transcends from domestic models of digital identity



Country A

Country B

Country C

Country D

Country E

Context

Material benefits to domestic and cross-border digital identity

Complexity of standards, policies, use cases, and organizations

Domestic led model on a divergent path from interoperability

Cross-Border governance model lacking



Hypothesis

Experts can accelerate interoperability

Non-Profit led, multi-stakeholder supported

Identify gaps between standards and other barriers

Determine if there is appetite to continue work

Sponsors:



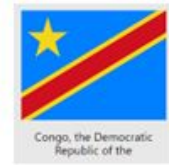
Non-Profit Organizers:



Multilaterals, standards, development organizations and academic institutions:



Government Experts:



In addition to the Paris Summit attendees, the following entities were unable to attend but requested to be on the SIDI HUB dissemination list. Others may join the dissemination list at <https://sidi-hub.community/>

Non-Profits:

American Association of Motor Vehicle Administrators (AAMVA)
Digital Equity
Nordic Institute of Interoperability Solutions
Bill & Melinda Gates Foundation
MOSIP
GLEIF

Multilaterals, standards, development organizations and academic institutions, Private companies:

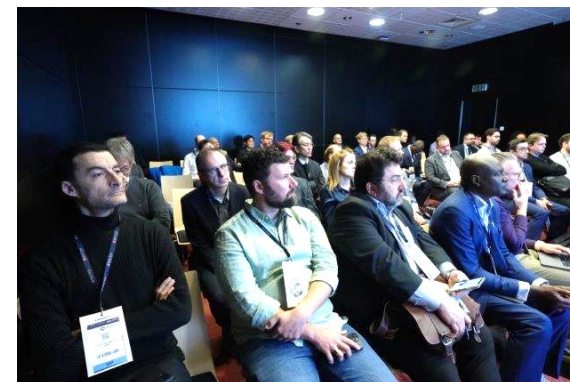
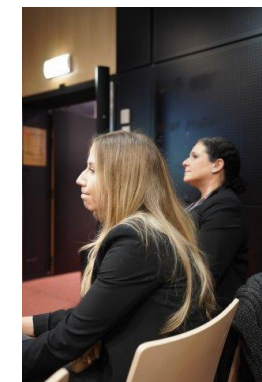
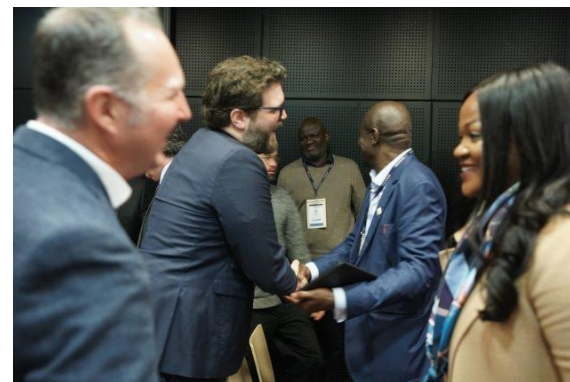
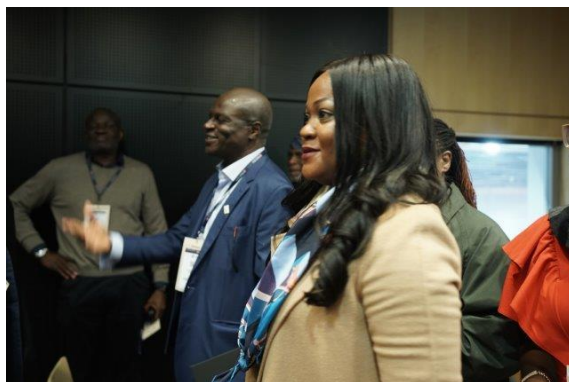
Amazon Web Services
CVS Health
George Washington University
Oxford University
UN World Food Programme
UN UNCITRAL
UN International Organization for Migration

Governments:

India
Germany - BSI, Bundesdruckerei
New Zealand
Norway - NORAD
Japan MIC
Sierra Leone
Spain - Digital
Sweden DIGG
UK DIATF
US - Treasury, FinCEN, TSA, California DMV

SIDI Paris Participants (11/28/23)

SIDI PARIS
2023



92% of Summit Attendees want to continue the work into 2024.

SIDI HUB Objective:

To define what we need to achieve global interoperability for digital identity.

Multilaterals

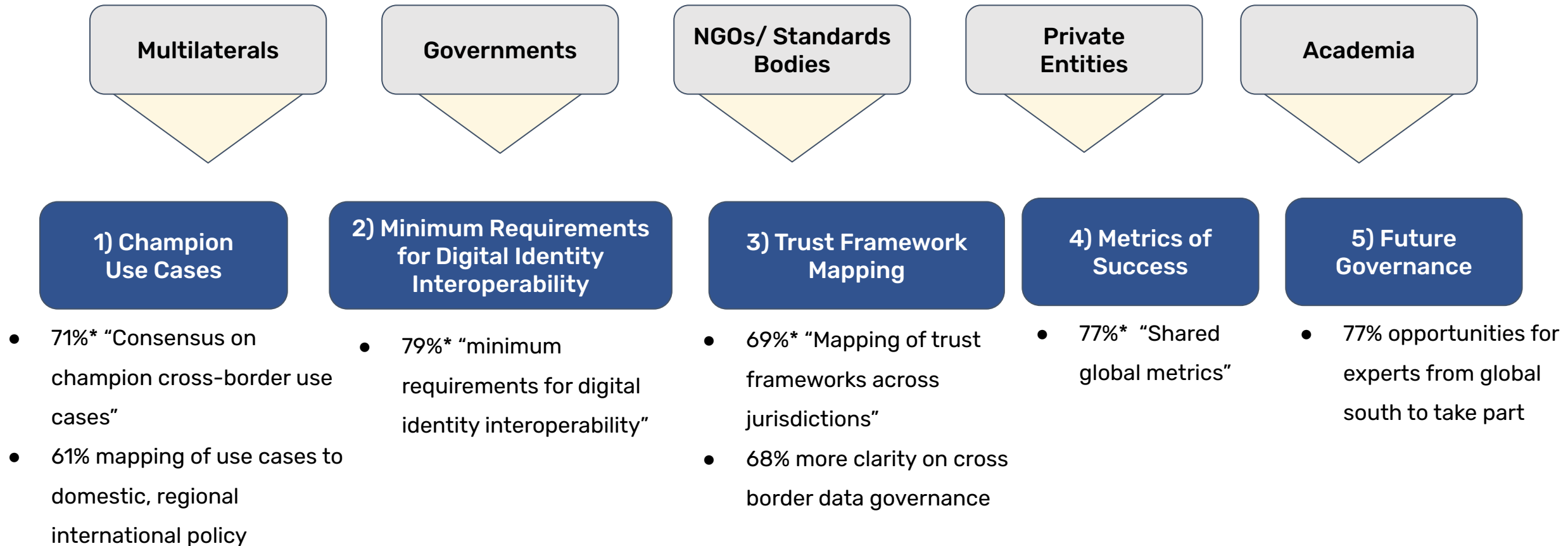
Governments

**NGOs/
Standards
Bodies**

**Private
Entities**

Academia

In the first SIDI Hub Summit in Paris on 11/28/23, we asked the attendees what we need to enable digital identity interoperability and five areas resonated the most



* % Participants in Exit poll who voted "yes" this is a high priority tactic to enable digital identity interoperability

SIDI Paris discussions & exit poll highlighted other tactics the community should pursue to deliver results

Organisational Alignment

e.g. roles, gap closure

Strategy

e.g. Vision + Roadmap

Funding

e.g. EU NGA Sargossa

Events & Outputs

e.g. ID4Africa, EIC, AAMVA, etc

Collaboration

e.g. Meeting cadence consensus

Communications

e.g. website, PR, briefs

Governance

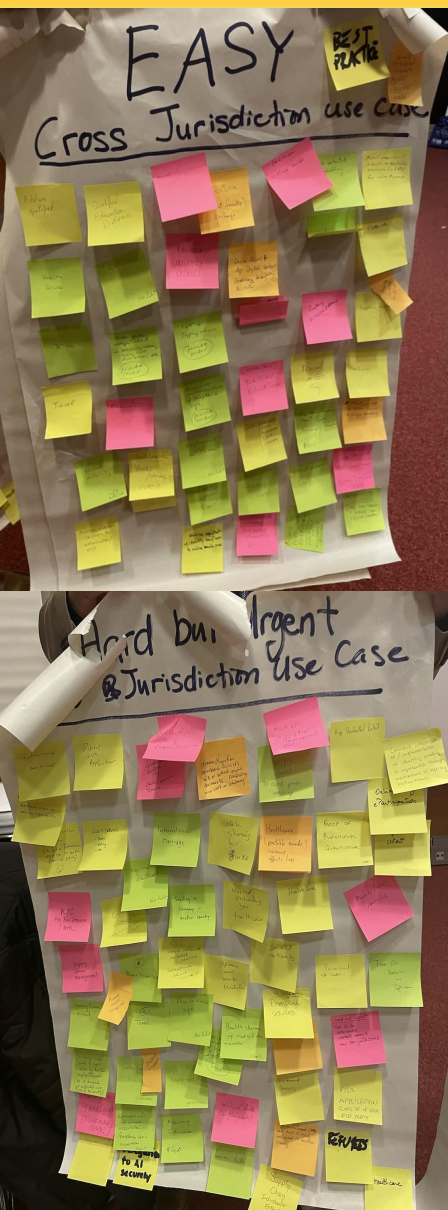
e.g. MOU, interop participation

Certification and Conformance

e.g. tests

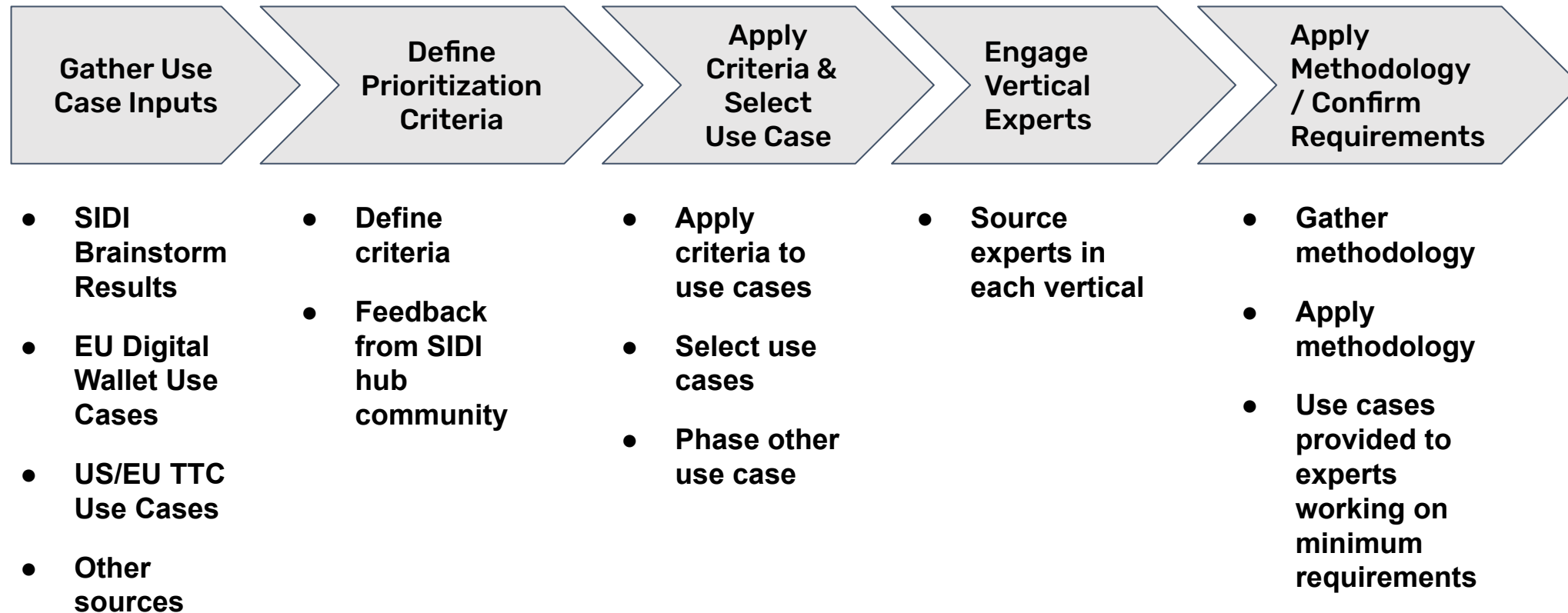
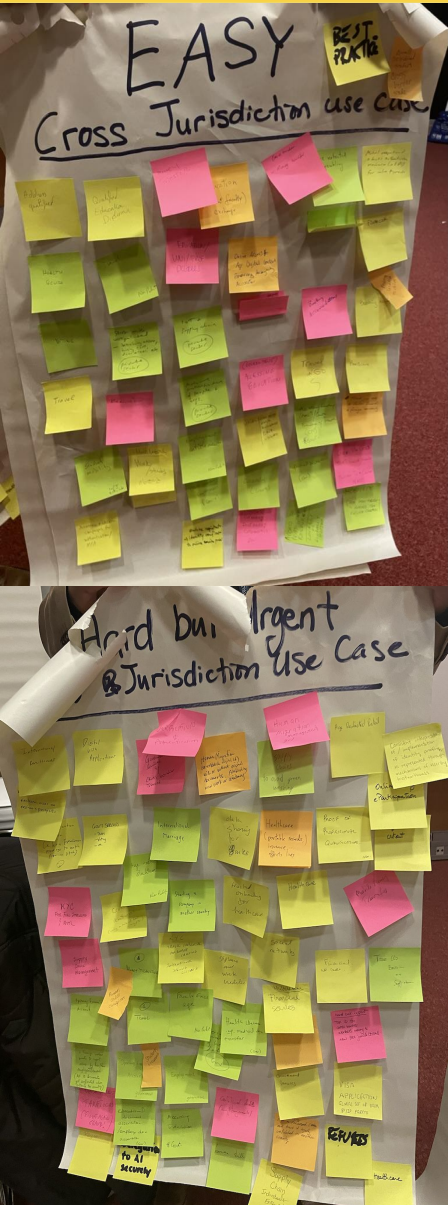
"Champion Use Case" SIDI Summit "Voting" Results

SIDI PARIS
2023

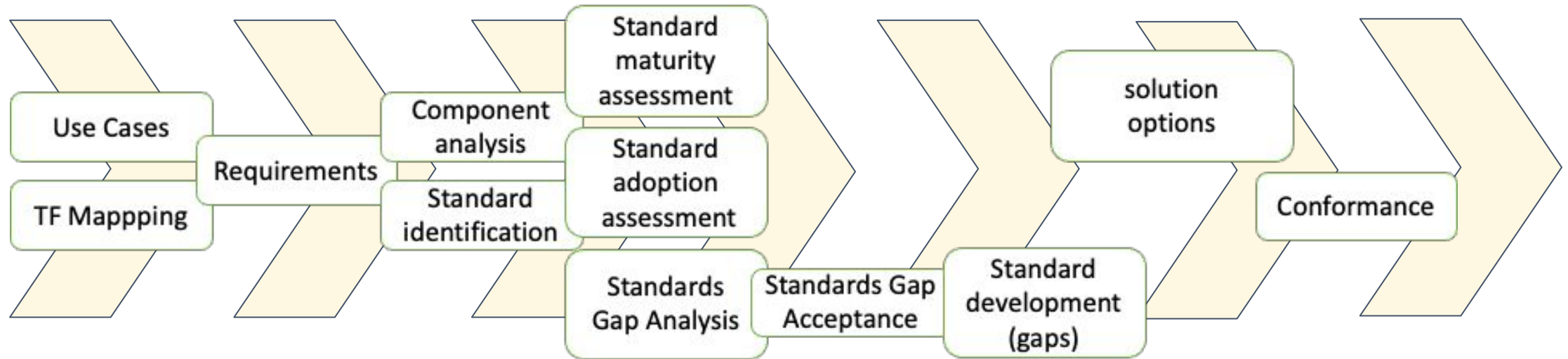


"Easy"	"Hard but Urgent"
<ul style="list-style-type: none"> • Qualifications (10) • Travel (8) • Financial Services (6) • Government Services (6) • Access to restricted resources online (3) 	<ul style="list-style-type: none"> • Financial services (11) • Qualifications (11) • Healthcare Services (7) • Government Services (7) • Travel (7) • Age verification (6) e.g. adult content in Utah, face to face age • Supply chain management (4) • Human migration (3)
<ul style="list-style-type: none"> • Healthcare (2) • Supply Chain (2) • Address qualified (1) • IoT (1) • Unregulated cases (1) 	<ul style="list-style-type: none"> • Social networking (1) • Parent/ child/ caregivers (1) • AI delegation Securely (1) • International Marriage (1) • Start a company in another country (1) • Foreign worker wants to report abuse(1)

“Champion Use Case” Selection Process



Minimum Requirements & Trust Framework Mapping - DRAFT



Policy requirements, gap analysis, bilateral/multi-lateral agreement requirements

Communications / Feedback / Distribution & Conformance of Comments

Metrics of Success

2024 Roadmap- In Development

SIDI PARIS
2023 /

Kick Off
2H 2023

Q1 2024

Q2

Q3

Q4

- **Summit 11/28**
 - **Validate the problem**
 - **Explore minimum requirements**
 - **Prioritize tactics**
 - **Confirm interest to continue in 2024**
 - **Draft 2024 strategy**
- **Public briefing**
 - **Confirm 2024 summits**
 - **Kick-off workstreams**
 - **Align roadmaps (standards, OECD, World Bank, UN, EU)**
 - **Participant roles**
 - **Draft G7 Report (TBD)**
- **Progress workstreams**
 - **MOUs for non-profits on contributions**
 - **G7 (June, TBD)**
 - **Draft G20 Report**
- **Progress workstreams**
 - **Conform comments on G20 Report**
- **Progress workstreams**
 - **Conform comments on G20 Report**
 - **Present G20 Report on progress and recommendations for 2025-2030**

2024 Roadmap- In Development

SIDI PARIS
2023 /

Kick Off
2H 2023

Q1 2024

Q2

Q3

Q4

2024 SIDI
Summits

1. **Africa** (~ID4AFrica,
Cape Town, 5/21)

2. **Europe** (~EIC, Berlin,
6/3)

3. **TBC: North
America** (~AAMVA
AIC, Atlanta, 9/27)

4. TBC: **Asia** (Tokyo,
Oct)

5. **L.A.** / G20 (Rio,
11/15 + 11/20)

SIDI Brief +
Surveys

Tokyo 1/19 (OIDF-J)
D.C. 1/XX (BIC)
Addis Ababa
(MOSIP)
Asia (Identity Week)

Las Vegas
(Identiverse)
London (Identity
Week June)

U.S. (Authenticate)
D.C. Identity Week
(Sep)
London OIX (Sep)
Other...

Closing Remarks & Open Q&A



Visit: www.OpenID.net

Thank you.



Visit: www.OpenID.net