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!
# Workshop Agenda

<table>
<thead>
<tr>
<th>TIME</th>
<th>TOPIC</th>
<th>PRESENTERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:30-12:35pm</td>
<td>Welcome</td>
<td>Nat Sakimura</td>
</tr>
<tr>
<td>12:35-12:50pm</td>
<td>eKYC &amp; IDA WG Update</td>
<td>Mark Haine</td>
</tr>
<tr>
<td>12:50-1:05pm</td>
<td>AuthZEN WG Update</td>
<td>David Brossard &amp; Omri Gazitt</td>
</tr>
<tr>
<td>1:05-1:20pm</td>
<td>AB/Connect WG Update</td>
<td>Michael Jones</td>
</tr>
<tr>
<td>1:20-1:35pm</td>
<td>FAPI WG Update</td>
<td>Nat Sakimura</td>
</tr>
<tr>
<td>1:35-1:50pm</td>
<td>MODRNA WG Update</td>
<td>Bjorn Hjelm</td>
</tr>
<tr>
<td>1:50-2:05pm</td>
<td>DCP WG Update</td>
<td>Kristina Yasuda &amp; Joseph Heenan</td>
</tr>
<tr>
<td>2:05-2:20pm</td>
<td>Shared Signals WG Update</td>
<td>Tim Cappalli</td>
</tr>
<tr>
<td>2:20-2:30</td>
<td>BREAK</td>
<td></td>
</tr>
<tr>
<td>TIME</td>
<td>TOPIC</td>
<td>PRESENTERS</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2:20-2:30</td>
<td>BREAK</td>
<td></td>
</tr>
<tr>
<td>2:30-2:40</td>
<td>OIDF Certification Program Update + Roadmap</td>
<td>Joseph Heenan</td>
</tr>
<tr>
<td>2:40-2:55pm</td>
<td>Death &amp; the Digital Estate Community Group</td>
<td>Dean Saxe</td>
</tr>
<tr>
<td>2:55-3:05pm</td>
<td>Sustainable &amp; Interoperable Digital Identity (SIDI) Hub Update</td>
<td>Gail Hodges</td>
</tr>
<tr>
<td>3:05-3:30pm</td>
<td>Listening Session: Post-Quantum Computing &amp; Identity. What are your concerns? What is OIDF’s role?</td>
<td>Gail Hodges, Nancy Cam-Winget, John Bradley, Rick Byers, Andrea D’Intino</td>
</tr>
<tr>
<td>3:30-3:55pm</td>
<td>Listening Session: AI &amp; Identity. What are your concerns? What is OIDF’s role?</td>
<td>Nancy Cam-Winget, Kaelig Deloumeau-Prigent, Mike Kiser, Geraint Rogers</td>
</tr>
<tr>
<td>3:55-4:00pm</td>
<td>Closing Remarks</td>
<td>Nat Sakimura</td>
</tr>
</tbody>
</table>
OpenID Foundation
Work Group Updates
eKYC & IDA Work Group

Mark Haine
eKYC & IDA 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
- OpenID Connect for Identity Assurance modularization complete
eKYC & IDA Working Group Progress - IDA drafts

- IDA Final reviews well underway

  "OpenID Connect for Identity Assurance 1.0" - openid-connect-4-identity-assurance.md

  "OpenID Identity Assurance schema definition 1.0 draft" - openid-ida-verified-claims.md

  "OpenID Connect for Identity Assurance Claims Registration 1.0 draft" - openid-connect-4-ida-claims.md

With particular thanks to Taka, Kosuke, Nat, and Dima for their detailed review and Hodari for hard work on PRs
eKYC & IDA Working Group Progress - other Activities

- Profiles/registry - under discussion
- IDA related JSON Schemas updated
- Long term home for JSON schemas discussion underway

Next Steps

- IDA specs to final - really!
- Update beta Conformance test to “final”
- Attachments Draft - next in line for move to “final”
- Advanced Syntax for Claims Draft - moving towards “Implementers Draft 1”
- Authority Draft - moving towards “Implementers Draft 1”
- Possible registry establishment for “evidence” and “assurance_process” types
Working Group external achievements

- IDA Implementations operational in:
  - Germany, Scotland, Australia, Czech republic, Japan
- Projects underway in:
  - UK, US,
- Collaboration with Digital Agency of Japan
- Presentations to CAMARA Working Group about IDA specs and ASC - facilitated by Kosuke & Bjorn
- Included IDA drafts in consultation feedback to UK Department of Science, Innovation and Technology (DSIT) and Ofcom (communications regulator)
- Presented OIDC, OIDC4IDA, OID4IDA & ASC for discussion at ISO SC27 WG5 in the context of ISO 27566 - Age Assurance
- Curity Tutorial Post: https://curity.io/resources/learn/verified-claims-identity-assurance/
AuthZEN Work Group Update

David Brossard, Omri Gazitt
Motivation: why authorization is critical

- 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 (2021) is A01:2021-Broken Access Control
  - 94% of apps were tested for some form of broken access control.
- The #1, 3, 5 issues on OWASP’s Top 10 API security risks (2023) are all related to broken authorization
  - Broken Object-Level Authorization, Broken Object Property-Level Authorization, Broken Function-Level Authorization
Motivation: why standards are needed

- 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

- Intra-org
- Authorization Protocols and Formats
- Between components
- Between systems
- Inter-org
AuthZEN WG Scope and Objectives

- Increase interoperability between existing standards and approaches to authorization
  - Policy-based e.g. ALFA, Cedar, OPA (Rego), Topaz, and IDQL,
  - Zanzibar/Graph-inspired systems such as OpenFGA, Topaz, SpiceDB, SGNL
  - NGAC-inspired systems e.g. 3Edges

- Standardize interoperable communication patterns between major authZ components
  - PAP, PDP, PEP, and PIP
  - See NIST ABAC’s architecture (NIST SP 800-162)

- Establish and promote the use of Externalized AuthZ as the preferred pattern
Deliverables and Specifications

- Description of standard authorization patterns, use cases, communications patterns, and integration patterns (in progress)

- 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 (in progress, interop scenario defined)

- An API to communicate authorization policy and data from PAP to PDPs which may be implemented by different parties (not started)
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 Kasselman, Microsoft, pieter.kasselman@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/](https://openid.net/wg/authzen/)
  - 📩 Mailing List

- Meeting notes & Design Documents
  - 📝 HackMD: [https://hackmd.io/@oidf-wg-authzen](https://hackmd.io/@oidf-wg-authzen)

- Github
  - 🌟 [https://github.com/openid/authzen](https://github.com/openid/authzen)

- Slack
  - 📚 #wg-authzen
April 2024 Update

- Prior Art Document
  - Deep dive into XACML, ALFA, Cedar, Topaz, and OAuth
  - Comments welcome here: https://hackmd.io/@oidf-wg-authzen/prior-art-pep-pdp
- PEP-PDP API draft
  - https://openid.github.io/authzen/
- AuthZEN Interop Scenarios
  - https://hackmd.io/@oidf-wg-authzen/InteropScenarios: focused on a simple “Todo” app
  - Interop website: https://authzen-interop.net | Sample payload Postman collection
  - 4 implementations are already conformant: Aserto (Topaz), Cerbos, Kogito, SGNL
  - At least 3 more implementations are in the works: Axiomatics (XACML REST/JSON), Permit.io, OPA
- Next steps
  - AuthZEN Panels at Identiverse 2024 and EIC 2024
  - Interop events at both Identiverse 2024 and EIC 2024
OpenID Connect Work Group

Michael B. Jones
OpenID Connect Working Group Overview

Initiatives of the Working Group

▪ Created the OpenID Connect protocol, enabling login and logout
▪ Incubated OpenID Connect for Identity Assurance work
  ▪ Now in the eKYC-IDA WG
▪ Developing OpenID Federation, enabling trust establishment among cooperating parties
▪ Incubated OpenID for Verifiable Credentials specifications
  ▪ Transfer of the OpenID4VC specs to the Digital Credentials Protocols (DCP) working group is anticipated after OpenID Connect WG Implementer’s Drafts are approved
▪ See the list of specs and descriptions at https://openid.net/wg/connect/specifications/
OpenID Connect Working Group 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)
- OpenID 2.0 to OpenID Connect Migration
- Error Code unmet_authentication_requirements
- Initiating User Registration via OpenID Connect

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 2023

- Second Errata Set for OpenID Connect specifications published, December 2023
- ISO Publicly Available Submission (PAS) submission accepted, January 2024 (see next slide)
- First Implementer’s Draft of OpenID for Verifiable Credential Issuance specification, April 2024
- Multiple OpenID Federation drafts published
  - Federation Operators section rewritten for clarity
  - Working towards final Implementer’s Draft
- Multiple OpenID4VC drafts published (described in the DCP WG presentation)

Challenges and opportunities facing the working group

- OpenID Federation in production use
  - In Italy, both for national federations and EU wallet ecosystem
  - In Australia, for FAPI trust establishment
  - In Sweden, for national federations
- Relationships with digital wallet initiatives and national identity systems worldwide
ISO Publicly Available Submission (PAS) for OpenID Connect

Submission of OpenID Connect specs for republication by ISO/IEC JTC 1

- Will enable use of OpenID Connect in jurisdictions requiring specs by treaty organizations
- Submission accepted, January 2024
- No changes were made to the submitted specifications, other than adding ISO title pages
- ISO spec numbers assigned, February 2024
  - ISO/IEC CD 26131: Information technology — OpenID Connect Core 1.0
  - ISO/IEC CD 26132: Information technology — OpenID Connect Discovery 1.0
  - ISO/IEC CD 26133: Information technology — OpenID Connect Dynamic Client Registration 1.0
  - ISO/IEC CD 26134: Information technology — OpenID Connect RP-Initiated Logout 1.0
  - ISO/IEC CD 26135: Information technology — OpenID Connect Session Management 1.0
  - ISO/IEC CD 26136: Information technology — OpenID Connect Front-Channel Logout 1.0
  - ISO/IEC CD 26137: Information technology — OpenID Connect Back-Channel Logout 1.0
  - ISO/IEC CD 26138: Information technology — OAuth 2.0 Multiple Response Type Encoding Practices
  - ISO/IEC CD 26139: Information technology — OAuth 2.0 Form Post Response Mode
- Publication as ISO specs expected after five-month ISO balloting period
## Working Group Roadmap

<table>
<thead>
<tr>
<th>DATE</th>
<th>DELIVERABLES</th>
<th>ASPIRATIONS</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q2 2024</td>
<td>Final OpenID Federation Implementer’s Draft</td>
<td>Finish bringing text up to OpenID Connect quality standards</td>
<td>Can discuss specifics this week</td>
</tr>
<tr>
<td>Q3 2024</td>
<td>ISO PAS specifications for OpenID Connect published</td>
<td>Make OpenID Connect specs available to those with treaty-based procurement processes</td>
<td>ISO publication expected after conclusion of five-month ballot period</td>
</tr>
<tr>
<td>Q4 2024</td>
<td>Final Federation Spec</td>
<td>Trust establishment for broad set of use cases</td>
<td>Having Final spec will accelerate deployments</td>
</tr>
</tbody>
</table>
Tenth Anniversary of OpenID Connect

- OpenID Connect specifications were approved in February 2014
- Three celebrations are being held
  - January 2024 at Japan OpenID Summit in Tokyo
  - May 2024 at Identiverse in Las Vegas
  - June 2024 at EIC in Berlin
- Presentations from first celebration published at https://self-issued.info/?p=2481
- During the celebrations, we are sharing our perspectives on
  - How we developed OpenID Connect
  - Why it succeeded
  - Lessons we learned along the way
- Lessons learned
  - “Keep simple things simple”
  - Repeated interop testing and incorporating resulting feedback from developers was critical
  - Certification enables an ecosystem of interoperable implementations
What the Working Group Plans to Accomplish at IIW This Week

What sessions do you plan to hold?

What hallway/table conversations do you want to have?

What demos are you presenting?

Logistics:
- Today’s OpenID Connect working group call cancelled in favor of this workshop
- Do we want to hold Thursday’s 7am working group call?
FAPI Work Group Update

Nat Sakimura
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

<table>
<thead>
<tr>
<th>DATE</th>
<th>DELIVERABLES</th>
<th>ASPIRATIONS</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q2 2024</td>
<td></td>
<td>FINAL for FAPI 2.0 Security Profile</td>
<td></td>
</tr>
<tr>
<td>Q3 2024</td>
<td></td>
<td>FINAL for FAPI 2.0 Message Signing</td>
<td></td>
</tr>
</tbody>
</table>
MODRNA Work 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

Preparing the MODRNA Discovery Profile to Implementer’s Draft review and vote.

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:

- Continuing engagement with the CAMARA Project, a Linux Foundation project, with Identity and Consent Management SP and KnowYourCustomer SP.
- Review in proposed draft formal liaison agreement with GSMA in order to facility the open exchange of information between the organizations across working groups.
- Established relationship and liaison agreement with ETSI (European Telecommunications Standards Institute).
<table>
<thead>
<tr>
<th>DATE</th>
<th>DELIVERABLES</th>
<th>ASPIRATIONS</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q2 2024</td>
<td>▪ MODRNA CIBA Profile (Implementer’s Draft)</td>
<td>▪ Liaison Agreement with GSMA</td>
<td>▪ Active engagement with CAMARA Project</td>
</tr>
<tr>
<td></td>
<td>▪ MODRNA Discovery Profile (Implementer’s Draft)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q3 2024</td>
<td>▪ IETF draft (IANA Registry)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ MODRNA Registration Profile (Implementer’s Draft)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q4 2024</td>
<td>▪ CIBA Errata draft</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ CIBA Extension draft</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Digital Credentials Protocols (DCP)
Work Group Update

Kristina Yasuda
Joseph Heenan
OpenID for Verifiable Credentials

User Interactions

Issuer (Website)
Issue Credentials
OpenID for Verifiable Credential Issuance

Wallet (user’s device, cloud or hybrid)
Present Credentials
OpenID for Verifiable Presentations
Self-Issued OP v2
OpenID for Verifiable Presentations over BLE

Verifier (Website)

Security and Trust in OpenID for Verifiable Credentials

OID4VC High Assurance Interoperability Profile (HAIP)
Progress

- New working group chair added (Joseph Heenan)
- Added an additional WG slot on Tue 9 pm CET/noon PT/9am NZ to facilitate attendance from US West Coast & NZ
- OID4VCI
  - First implementer’s draft now published!
- Conformance tests have been updated
  - OID4VP tests now support ISO 18013-7 mDL as well as SD-JWT VC (wallet-side)
- OID4VP
  - Preparing the third implementer’s draft of OID4VP (WGLC next month?)
    - request_uri extension
    - SD-JWT VC profile added
  - PR in progress with draft of profile of Browser API for OID4VP
  - gathering requirements to address implementation feedback for OID4VP query language
Implementations

- 100+ companies will test OpenID4VC protocols with mdocs and SD-JWT VC at the EU’s POTENTIAL Large Scale Pilot’s interop event
- 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, GAIA-X, CA DMV
- Increasing number of open source projects
  - e.g. Ping Identity, .NET Wallet Framework, MOSIP and Aries JavaScript Framework
- OID4VC Due Diligence Task Force at OWF
- Lot of implementers feedback
Next Steps

- **OID4VCI**
  - Updates to batch API to support issuing copies of credentials (full lifecycle support for unlinkable credential)
  - Update terminology to differentiate multiple instances of a credential

- **OID4VP**
  - Complete/continue Browser API discussions at W3C WICG
  - Address implementer feedback for the query language in OID4VP

- Extend conformance tests (to be used in various interop tests/hackathons)

- Continue eIDAS support, e.g. through evolving HAIP

- Support NIST NCCoE
Shared Signals Work Group Update

Tim Cappalli
Problem: Authentication only happens at the time of login

Shared Signal Framework

- Session
- Continuous Monitoring
- Continuous Mitigation
- Account
- Security Signal
- Realtime Protection
- End User/Device
- Sharing Intelligence
- Robotic Remediation
Shared Signal Framework Technical Overview

CAEP :- Session control
RISC :- Account protection

Secure multi stream Webhook communication layer

IETF technology standards used by the SSF Framework

Shared Signal Framework ID 2

PUSH based SET Delivery RFC 8935
POLL based SET Delivery RFC 8936
Sub-ID for SET RFC 9493

Security Event Token (SET) RFC 8417

JSON Web Token RFC 7519
JSON Web Key RFC 7517
JSON Web Encryption RFC 7516
Two New Chairs

Shayne Miel
Cisco

Sean O’Dell
The Walt Disney Company
The Chairs

Atul
- Interop spec
- Certification

Shayne
- SSF ID-2 to final

Tim
- New events for CAEP
- Liaising with other standards bodies

Sean
- Use cases whitepaper
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 CAEP, RISC Specs

Interoperability
- Shared Signals Framework Interop Profile (ongoing)
  - CAEP Interoperability Profile 1.0 - draft 01

Developer Events
- IIW Silicon Valley April 16-18
- Indentiverse 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 through 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 Interoperability Event at Gartner IAM Summit, London

• March 4-5th
  – Breakout session with OpenID speaker
  – 3 demo sessions

• 8 participating implementations achieved interoperability

• Focus on event-level interoperability

• Event-types used:
  – Session Revoked, Credential Change, Token Claims Change
### CAEP Interoperability Event Results

#### Demo Session In Action

#### Interop participants

<table>
<thead>
<tr>
<th>Participants</th>
<th>Transmitter</th>
<th>Receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Duo</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Sgnl</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>SailPoint</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Okta</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Webex by Cisco</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Heliosoft</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Caep.dev</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Vericlouds</td>
<td>🟢</td>
<td></td>
</tr>
</tbody>
</table>
How to participate

- WG Landing: openid.net/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
BREAK
10-minutes

Visit: www.OpenID.net
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, now includes ISO mDL, participating in EU LSP)
- OpenID Connect For Identity Assurance (beta available)
- FAPI2 DPoP
- OpenID For Verifiable Credential Issuance

Future Roadmap
- OpenID Federation (directed funding received from ConnectID, thank you!)
- FAPI2: CIBA, HTTP Signatures
- New UAE FAPI profile
Progress & Opportunities

Deliverables last 6 months
- FAPI1-Adv New, simplified OpenFinance Brazil profile launched
- Brazil OpenFinance ecosystem recertified on new profile
- Ecosystem support
- Tackling some technical debt & bringing many dependencies up to date

USA & Canada OpenBanking regulatory updates due to drop during 2024
- Expected to endorse FAPI & FDX in some way
- Waiting to see what they might say about certification
Death & the Digital Estate Community Group

Dean Saxe
The Problem

• Death is the forgotten state transition in identity systems
The Problem

• Death is the forgotten state transition in identity systems

• Individuals lack clear, consistent tools to enable them to determine the disposition of their digital estate
The Problem

• Death is the forgotten state transition in identity systems

• Individuals lack clear, consistent tools to enable them to determine the disposition of their digital estate
  – Delegate access
The Problem

• Death is the forgotten state transition in identity systems

• Individuals lack clear, consistent tools to enable them to determine the disposition of their digital estate
  – Delegate access
  – Provide credentials to designated heirs
The Problem

• Death is the forgotten state transition in identity systems

• Individuals lack clear, consistent tools to enable them to determine the disposition of their digital estate
  – Delegate access
  – Provide credentials to designated heirs
  – Delete data / account
The Problem

• Death is the forgotten state transition in identity systems

• Individuals lack clear, consistent tools to enable them to determine the disposition of their digital estate
  – Delegate access
  – Provide credentials to designated heirs
  – Delete data / account
  – Evidentiary requirements
The Problem is International

- There’s an interplay between local laws, customs, and international systems
  - Not all problems can be solved by standards, nor should they be
The Digital Estate Community Group

• Goal: Establish an OIDF Community Group
The Digital Estate Community Group

• Goal: Establish an OIDF Community Group
  – Provide a space to bring together experts and interested parties
The Digital Estate Community Group

• Goal: Establish an OIDF Community Group
  – Provide a space to bring together experts and interested parties
  – Develop use cases, broad data flows, and guidance for service providers
The Digital Estate Community Group

• Goal: Establish an OIDF Community Group
  − Provide a space to bring together experts and interested parties
  − Develop use cases, broad data flows, and guidance for service providers
  − Identify out of scope issues – legal, political, social
The Digital Estate Community Group

• Goal: Establish an OIDF Community Group
  – Provide a space to bring together experts and interested parties
  – Develop use cases, broad data flows, and guidance for service providers
  – Identify out of scope issues – legal, political, social

• Long Term Goal: Establish an OIDF Working Group to develop protocols based on the output of the proposed CG
The Digital Estate Community Group

• Charter is in an early draft state
The Digital Estate Community Group

• Charter is in an early draft state

• Collaborators needed to develop the draft in Q2 2024
The Digital Estate Community Group

• Charter is in an early draft state

• **Collaborators needed to develop the draft in Q2 2024**

• Want to help? Contact me – deansaxe@amazon.com
Sustainable & Interoperable Digital Identity (SIDI) Hub Update

Gail Hodges
Strategy

• “SIDI Hub 2024 Strategy”

• OIDF SIDI Hub Draft Objectives, as per Task Force & EC feedback
  https://docs.google.com/document/d/1pJwT57YfxQaStdIHtqvt6qnnPOzk_H4PluDw_sE_sl/edit

• OIDF SIDI Hub Subgroup participants (to date):
  Ben, Ian, Mike, Gail, Mark, Nick Thorne

• Co-operative agreement between the 17 non-profit co-organizers underway, target to sign in May
SIDI Hub OIDF Board Update

**Summits**
- May 20\(^{th}\) Cape Town
- June 3\(^{rd}\) Berlin (German Gov)
- Sep 10\(^{th}\) Washington D.C.
- Oct 25\(^{th}\) Tokyo (Japanese Gov)
- Mid-Nov Rio or Sao Paulo

**Workstreams**
- Champion Use Cases
- Min Requirements (*charter drafted*)
- Trust Framework Mapping
- Metrics (*charter drafted*)
- Governance (SIDI Hub+ gaps in ecosystem governance)

**Staffing**
- Co-organizers (non-profit leaders)
- Co-chairs volunteers (14 co-chairs identified to date, OIDF has two)
- Nick Thorne as Advisor (March – June)
- Key staff person identified for contract with SIA or OIDF

**Funding**
- ~$110k Non-Profits
- $110k EU NGI Sargasso
- ~28k Japan Gov (in kind venue, food)
- ~$15k German Gov (in kind venue)

$220k direct + ~$43 indirect

~~$263k Total Funding (OIDF 19%)~~

**Structure**
- Community group, not a legal entity
- Cooperative Agreement between key co-organizers including OIDF underway

**Communications**
- Ongoing survey
- Summit Reports
- Public events (IIW Sessions, Identiverse, EIC (keynote, masterclass), FedID, Identity Week D.C. panel), Identity Week Singapore, Trust Tech, +others
# DRAFT: OIDF’s KPIs for SIDI Hub (Subgroup)

<table>
<thead>
<tr>
<th></th>
<th>1Q 2024</th>
<th>2Q 2024</th>
<th>2H 2024</th>
</tr>
</thead>
</table>
| 1. Community thought leadership | **OIDF led SIDI Hub 2024 Strategy & in partnership with 17 non-profits SIDI Hub communications**  
**OIDF one of 5 parties to EU NGI Sargasso Grant**  
**Co-chairs two workstreams** | **OIDF thought leadership approach to 2 events**  
**Workstream progression in all 5 workstreams** | **OIDF thought leadership approach to 2-3 events**  
**In person workshops inform WG/CG development**  
**Workstream progression in all 5 workstreams** |
|   | **Gap analysis on OIDF specifications to enable interoperability**          | **Gap analysis on OIDF specifications to enable interoperability (Cont).**  
**Gather requirements to close the gaps in OIDF specs**                       | **Close gaps on liaison agreements**  
**20 new contributors to OIDF WGs, CGs**  
**4 SIDI Hub participants use OIDF standard**  
**2 SIDI Hub Participants confirm they will use OIDF certification** |
| 2. OIDF WG & CG benefits     | **50+ new relationships since November**  
**Insight on development domain and other jurisdictions.** | **EU NGI Saragasso award brings coaching and support to SIDI/OIDF**  
**German, Brazil and Japanese govl considering hosting event** | **Align SIDI Roadmap to OECD, World Bank, UN, EU roadmaps**  
**Align SIDI Roadmap to data sharing/open banking roadmaps** |
| 3. New strategic relationships | **EU NGI Sargasso fund of $100k and $45k other non profits scales $50k from OIDF**  
**OIDF prospects engaged (Apple, Idemia)**  
**Retain Nick Thorne to derisk program** | **$50k + travel in SIDI Hub is scales OIDF reach**  
**Onboard new OIDF members** | **Further extend OIDF reach by SIDI Hub fundraising**  
**SIDI Hub informs 2025 OIDF Strategy and Investment**  
**OIDF members** |
| 4. Optimize OIDF investment  |                                                                                           |                                                                           |                                                                           |
OIDF/ SIDI Advisor Nick Thorne

• Career diplomat with 15 years experience at the UN

• UK Ambassador to all United Nations, WTO (Geneva 2003-8), UN Advisory Committee, Deputy Ambassador (Helsinki)

• Expert in Internet Governance. Experienced International Advisor with a demonstrated history of working in the civic & social organisation industry

• International Relations Adviser to the President and CEO of ICANN, Elected Oversight Committee Red Cross, other advisory roles.

• Personally involved in the governance process of developing the internet and balancing power amongst ecosystem participants, and risk mitigation plans for many other global initiatives

• Nick has the perspective to inform the digital identity community of what is required to identify and mitigate risks, and refine our plans to achieve globally interoperable digital identity across different layers from standards to geopolitics.

EC resolution to retain Nick for 3 months, to revisit in June Board (SIDI Hub funded extension and/or OIDF extension)
Listening Session: Post-Quantum Computing & Identity

Gail Hodges, Nancy Cam-Winget, John Bradley, Rick Byers and Andrea D’Intino
Listening Session: PQC + Identity

Key Questions:
What concerns you about the intersection of AI + Post Quantum Cryptography? What is OIDF’s role (if any) to support the community?

1) Andrea intro Slides:
https://docs.google.com/presentation/d/16g1NqI_g_d3oDljs1vY4hE_chXpJHDZvj77ecTi-KmM/edit#slide=id.p

Discussants:
- Andrea D’Intino, Dyne.org Project Manager
- John Bradley, Yubico, OIDF Board Member
- Nancy Cam-Winget – CISCO Fellow, OIDF Board Member
- Rick Byers – Web Platform Area Tech Lead, Chrome, Google & W3C Standards
Listening Session: AI & Identity

Gail Hodges, Kaelig Deloumeau-Prigent, Mike Kiser, and Geraint Rogers
Listening Session: AI + Identity

Key Questions:
What concerns you about the intersection of AI + Identity? What is OIDF’s role (if any) to support the community?

1) Deutche Telekom July 2023, 2.4M Vies: [https://youtu.be/F4WZ_k0vUDM?si=nVyN7IO1kr6DZuNo](https://youtu.be/F4WZ_k0vUDM?si=nVyN7IO1kr6DZuNo)

2) LLM Prompt

Discussants:
- Nancy Cam-Winget – CISCO Fellow, OIDF Board Member
- Geraint Rogers – Daon, Customer Success, Market SME Identity & Risk
- Kaelig – Netlify Principal Engineer/ W3C Design Tokens CG CoChair
- Mike Kiser- Sailpoint, Director Strategy and Stanards

(Geraint, Timothy M reposts, Deutche Telekom July 2023)
LLM Prompt to implement OIDC in JS

How do I implement openID connect in JS

Implementing OpenID Connect in JavaScript for a web application typically involves several steps. OpenID Connect (OIDC) is built on top of OAuth 2.0 and enables clients to verify the identity of the end-user based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the end-user.

Here's a simplified guide to help you implement OpenID Connect in a JavaScript web application:

1. Choose a Library
First, choose a JavaScript library that supports OIDC. Libraries like `oidc-client-js` are popular for client-side applications. This guide will use `oidc-client-js` for demonstration purposes.

2. Create an OIDC Client
Register your application with your OpenID Provider (OP) to obtain a client ID and client secret. Configuration varies by provider (Google, Auth0, Okta, etc.), but generally, you'll need to provide a callback URL to which the OP will redirect after authentication.

3. Configure oidc-client-js
Install the `oidc-client-js` library and configure it with your client's details:

```
npm install oidc-client
```

```
import { UserManager } from 'oidc-client';
const config = {
```

[Other steps inbetween…. but no step to use OIDF tests or certify]

Additional Notes
- The `redirect_uri` must match one of the URLs you registered with your OP.
- Ensure you handle errors and edge cases, such as token expiration.
- Consider security implications, such as using HTTPS for production environments.

This is a basic guide to get started. Depending on your specific requirements (e.g., using a Node.js backend, SPA frameworks like React, Angular, or Vue), you might need to adapt and extend this implementation. Always refer to the documentation of the library you're using and your OpenID Provider for more detailed information.
Closing Remarks & Open Q&A
Thank you.

Visit: www.OpenID.net