The Future of Identity and Authentication

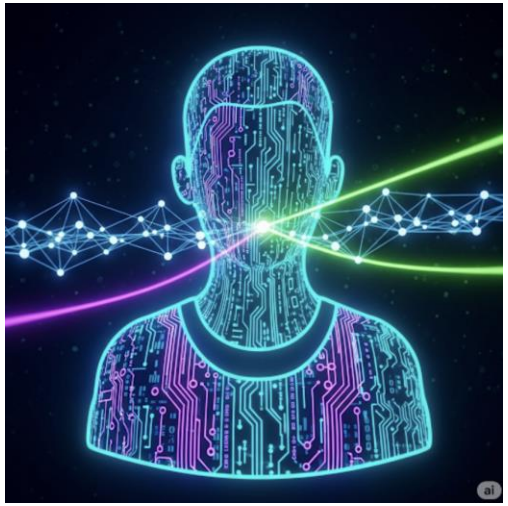
Phil

Identity

- You (person) have a **real-world**, **physical**, **identity**
  - You interact with other people who have their own real-world identities
  - You distinguish different real-world identities (people) by:
    - their physical/biological characteristics
    - their legal documents (passports etc. which obviously are also digital)
- When you **interact** with a **machine**, it wants to know **who** you are. **Why**?
  - **Security**
    - To know what you can access (**authorisation**)
      - To know what you are allowed 'to do'.
  - To **track** what you do (although **privacy** is important here)
  - To **personalize** your experience
  - This is your **digital identity**

Jisc

Digital Identity?



- Your digital identity is?
  - One or more unique **identifiers**
    - To distinguish between your digital identity and other digital identities (noting not all digital identities belong to humans)
    - Different identifiers are used in different contexts e.g. researcher identifier, student identifier, enterprise (organizational) identifier.
  - **Attributes**
    - That describes you (name etc).
    - That describes your roles e.g. I am a student, I am a staff member
    - Many other things
    - (Noting, when verified by an identity provider, these become claims or assertions intended for a given audience e.g. these are the claims I want to present to Salesforce).

Authentication?

- Connect your real-world identity to your digital identity?
  - To verify your digital identity, you need to provide **proof** that you own it
    - **Credentials** can be used as something you present to verify your digital identity. There are many types (none provide definitive proof you own your digital identity).
      - **Passwords**
      - Physical **keys (passkeys, FIDO2)**
      - **Biometrics**
      - A **combination** (Multi-factor)
  - This is **MY** digital identity, and these are **MY** unique identifiers, and these are **MY** attributes
  - If the connection is successful, you have an authenticated identity

Managing Identity

- There are different ways to **manage digital identity**
  - Centralised Per Service
    - Each service creates, manages, and stores your digital identity (account)
    - This dates back to the 1960s, mainframes etc.
    - Used on the web in the 90s and still today
      - A website manages your digital identity (account) on your behalf
  - Federated
    - Cross-domain identity and authentication
    - This dates back to the early 2000s
      - Services do not want responsibility for identity and credential management
      - Delegate that to another party (a federated Identity Provider)
      - User only wants one password and identity to access all services, SingleSignOn.
  - Decentralised
    - This has emerged in the last 10 years, and is part of the Web3 model for the decentralized web (including cryptocurrency)
    - Is user-controlled, not controlled by organisations
      - Is part of self-sovereign identity

Jisc

Trust Federation?

- If a Service Provider wants ‘somebody’ else to authenticate a user, why would they trust it?
  - They could do this bilaterally, or multilaterally (via a trust federation)
- Trust is established using trust federations, an important component of federated or decentralized authentication
- Enables multilateral trust at scale
  - Technical and governance policy frameworks etc.
- The Research and Education community run large scale multi-lateral trust federations
  - Identity providers and services provides agree on a trust framework that allows scalable multilateral trust
  - Described technically by metadata
  - Are **currently SAML** based
- Exist at the national level e.g. The UK Access Management Federation
- Exist at the global level via eduGAIN

The protocols that enable federated identity?

- For authentication, single-sign on, and authorization
- Current R&E Federations are SAML based
  - That is, IdPs and SPs in our federations communicate identity assertions via SAML and XML
- SAML has many applications beyond R&E including governments, enterprises (Salesforce etc) etc.
- Over the past 10 years, OpenID Connect (OIDC) has become a popular protocol for making bilateral SSO identity connections.
  - Especially for mobile applications, APIs and single page applications
  - Popular with developers…that is where the modern skillset is?

Jisc

Timeline of protocols for federated identity

- 2002:
  - SAML 1.0: Driven by the need for federation in academia and enterprise, starting around 1999.
- 2003:
  - **SAML 1.1**: Bug fixes to 1.0, and artifact binding.
- 2005:
  - **SAML 2.0**: consolidation of features from other specifications and implementations, including Shibboleth.
- 2006:
  - UK Access Management Federation went live!
- 2014:
  - **OpenID Connect** (OIDC): An identity layer on top of OAuth. Provides identity and authentication assurances.
- 2025?:
  - **OpenID Federation**: Support third-party trust relationships in protocols (including OpenID Connect) to support multilateral trust.
- 2025?:
  - OpenID for Verifiable Credentials. Issuing credentials to digital wallets (holders) and presenting credentials to verifiers (RP/SP)

Long Live SAML?

- Maybe, maybe not
- The SAML technical committee was closed in 2023
  - No changes to the core SAML specification expected
- SAML is not suitable for certain applications e.g. HTTP APIs
- XML based skills are decreasing, JSON and other technologies are now favored by deployers and developers?
- New technologies are based on OAuth and OpenID Connect/OAuth, not SAML. For example, OpenID For Verifiable Credential Issuance
- A post quantum world
  - NCSC guidance to migrate to PQC by 2035
  - Changes to XML digital security needed. Can this happen and be rolled out in an interoperable way? W3C have been discussing.

https://trustandidentity.jiscinvolve.org/wp/2025/05/16/will-quantum-computing-topple-saml/

And then what, OpenID Connect?

- OpenID Connect (OIDC) provides an identity layer on top of OAuth 2.0
  - OAuth authorizes a third-party to access either some other entities resources, or their own.
  - OIDC supplies the identity of the End-User that authenticated.
    - Identifiers and attributes (claims)
    - Can therefore be used as a replacement for SAML
- Developer friendly?
  - JSON over XML
  - Bilateral static registration via a web portal is easy
- More use cases?
  - Mobile clients, HTTP APIs, microservices…
- Security?
  - Arguably the JOSE standard used for JWTs (e.g., identity tokens) is less complicated and easier to get right than XML security
- Needs multilateral support to be used in large scale federations

Jisc

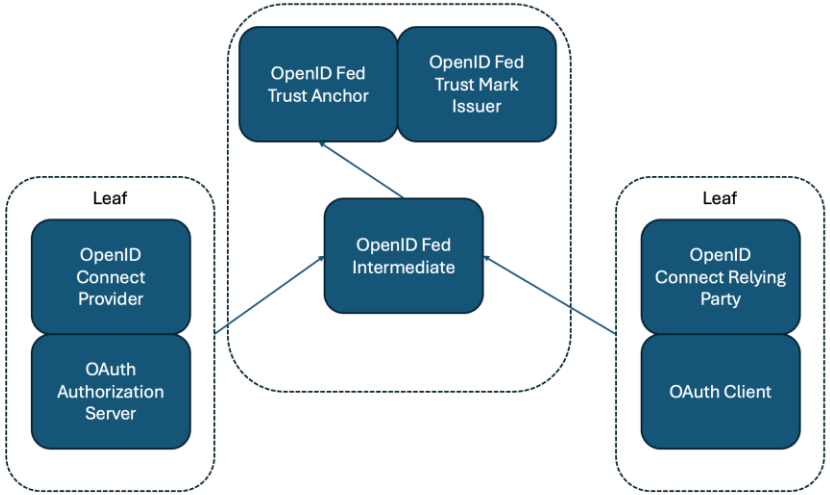
OpenID Federation?

- Pre 2016, OpenID Connect has no formal federation model
  - Noting that, neither does SAML. It is a model based on SAML specifications and SAML metadata.
  - OpenID Connect works using a simple ‘federated’ model that requires bilateral trust between RPs and OPs.
    - This is seen as an advantage to developers, as registration is simpler
    - But a disadvantage to identity provider operators: it is much harder to manage at scale.
- Roland Hedberg started a federation model for OpenID Connect in around 2016.
  - Aim, to establish scalable multilateral trust via a trusted third-party
  - It was specifically for OpenID Connect. But struggled to gain traction.

Jisc

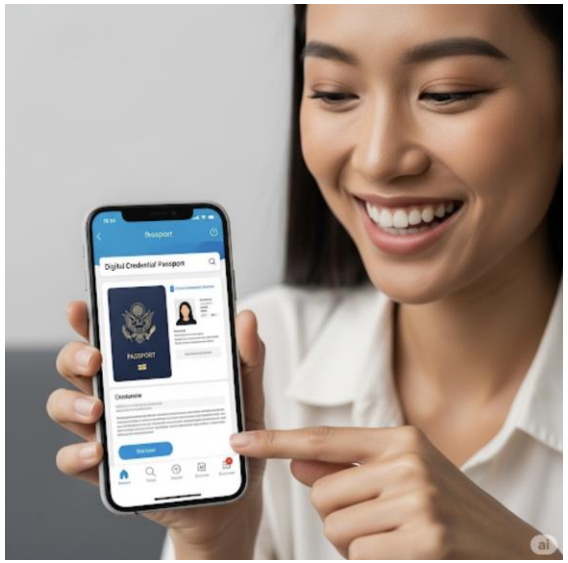
OpenID Federation

- The OpenID Foundation set up the OpenID Connect Federation Working Group in 2018 [1]
  - Mike Jones, Roland Hedberg, John Bradley et al.
  - Part of the AB/Connect Working Group [1]
- ‘Connect’ was dropped from the name to represent the broader capability of the federation specification in 2023 [2]
  - Not just for OpenID Connect. Digital Wallets are also a driver for this specification.



Jisc

There is more? Digital Credentials



- Should the end-user hold and issue their own credentials?
- Digital credentials represent a four-party model
  - *Issuer* (IdP)
  - **Holder** (Digital Wallets)
  - *Verifier* (Service Provider or Relying Party)
  - *Trust framework*
- This allows the holder, typically the human end-user, to decide what credentials to present, not the IdP
  - Self-sovereign identity (kind of)
- In the EU, driven by eIDAS
  - Personal Identification Data (PID) information
  - Give back control to their citizens from Google, Apple, Microsoft etc?
    - Governed by EU-Law.

Digital Credentials

- eIDAS 2.0 (electronic identification, authentication, and trust services)
  - DC4EU – Digital Credentials for Europe Pilot. Issuing professional and educational credentials
  - wwwWallet – an implementation (GUnet, Sunet, and Yubico).
- Project Titan
  - Student learner record
- GOV.UK digital wallet initiative
  - Not education focused to start? Driving license etc.

Digital credentials in research and education

- Right now, verifiable credentials could be used in R&E for:
  - Educational qualifications
    - Including ‘microcredentials’
  - Student Identifiers
    - Useful to integrate with digitised campus services
  - Admissions or student enrolment:
    - using a student learner identifier
    - with a verified set of credentials on who they are and what qualifications/attainments they have at a given point in time
  - Authentication to e-resources
  - Student mobility
    - cross-border education by allowing cross-border data exchange
    - Univeristy alliances

Web browser mediate authentication?

- Existing identity flows utilize basic web primitives in a way that is ‘unseen’ to the web browser.
- Google started work on their Federated Credential Management web browser APIs in 2019.
- They want to mediate all federated authentication
  - To help solve the problem third-party cookie tracking problem? Or to become a first-class citizen of the process?
  - Part of their privacy sandbox
- They also want to mediate all digital credential interactions
- They already mediate passwordless (passkey) authentication

In the future, what are the options?

Now.....

.....future

1. **SAML** based federations
    1. Supported by WebAuthn, or phishing resistant authentication
2. **OpenID Connect** based federations
    1. Supported by WebAuthn, or phishing resistant authentication
3. Federated authentication **mediated** by the **browser** using OpenID Connect
    1. Multilateral trust provided by OpenID federation
4. **Verified Credential** transactions
    1. Possibly mediated by the web browser
    2. Trusted by OpenID Federation, or trust lists
    3. Potentially providing authentication
5. All or some of the above?

In the future, what are the options?

future

1. We’ve not explore much on authentication, passkeys etc.
2. Other things I’ve no idea of…
    1. **AI** for…all the things including Identity and authentication