Internet Architecture Board (IAB)

Wholistic Human-Oriented Discussions on Identity Systems (WHODIS)

Chris Wood, Cullen Jennings,
Rifaat Shekh-Yusef, Dick Hardt
Pam Dingle, Hannes Tschofenig, Pieter Kasselman

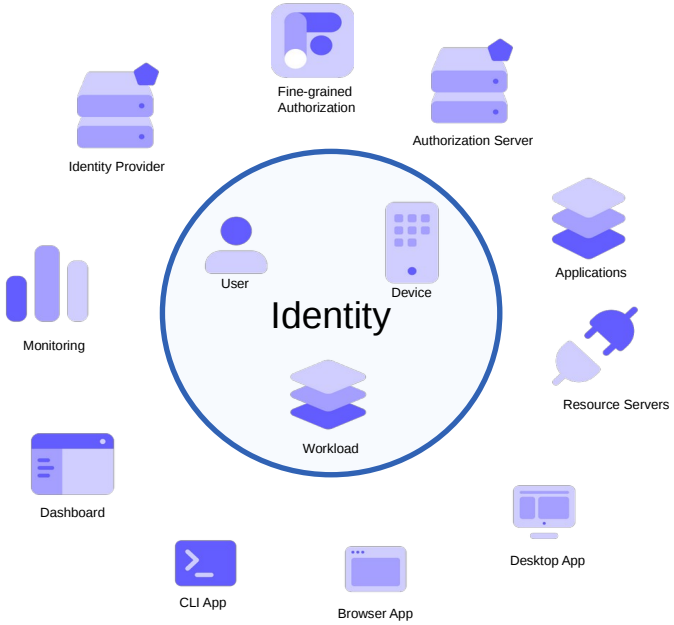
WHODIS

- An IAB Program to explore the **Internet Identity** space, which has a **very large surface area**.
  - You can learn more about the program here
    - https://github.com/intarchboard/proposed-program-whodis/blob/main/README.md
    - identity-discuss@iab.org

- Our goal with this presentation is to provide some **background** on the motivation for this work and explore an **initial achievable scope** to this program to make sure we are not boiling the ocean.

Internet Identity

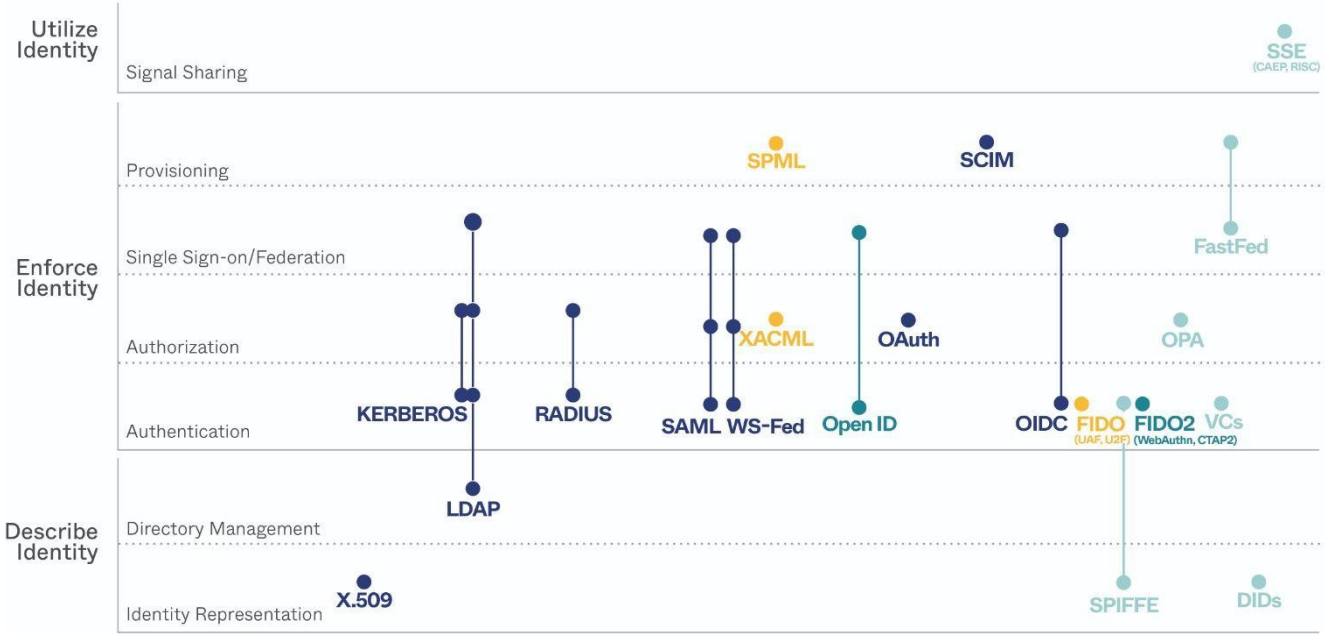
- Identity is a **fundamental** part of the Internet, and a **critical** part of any secure cloud-based solution, including the **end to end security** story.

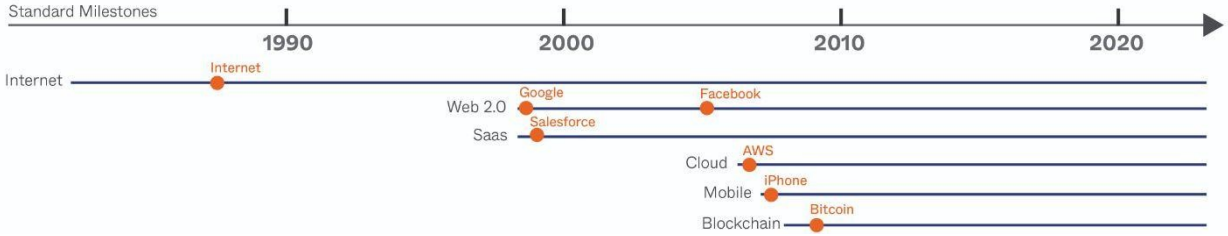


Organizations doing Identity Work

- Cloud Native Compute Foundation (CNCF)
- Decentralized Identity Foundation (DIF)
- FIDO Alliance
- ID Pro
- IETF
- Internet Identity Workshop (IIW)
- ISO
- OpenID Foundation
- W3C

A Map of Open Identity Standards





Level of Adoption

- Emerging
- Limited Implementation
- Some Implementations
- Widely Implemented

- Megatrends
- Major Triggers

Acronyms

SSE - Shared Signals and Events
CAEP - Continuous Access Evaluation Protocol
RISC - Risk Incident Sharing and Coordination
SPML - Service Provisioning Markup language
SCIM - System for Cross-domain Identity Management
SAML - Security Assertion Markup Language
WS-Fed - Web Services Federation
FastFed - Fast Federation
XACML - eXtensible Access Control Markup Language
OAuth - Open Authorization
RADIUS - Remote Authentication Dial-In User Service
OIDC - OpenID Connect
FIDO - Fast IDentity Online
OPA - Open Policy Agent*
SPIFFE - Secure Production Identity Framework for Everyone*
UAF - Universal Authentication Framework
U2F - Universal 2nd Factor
WebAuthn - Web Authentication
CTAP2 - Client-to-Authenticator Protocol
VCs - Verifiable Credentials
LDAP - Lightweight Directory Access Protocol
DIDs - Decentralized identifiers
**Open Source Projects*

Identity is more than Authentication

- Attestations
- Audit
- Authentication
- Authorization
- Compliance
- Federation
- Identifiers
- Incident Response
- Monitoring
- Provisioning
- Policies
- Tokens
- … and many more

User Identity

- IETF OAuth
- OpenID Connect - An Identity layer on top of OAuth
- FAPI (aka Financial-grade API)
  - FAPI 1.0 is based on OpenID Connect
  - FAPI 2.0 is based on OAuth artifacts defined by the OAuth WG
- IETF SCIM
- IETF SecEvents
  - OIDF Shared Signals and Events
- FIDO Alliance
  - WebAuthn
  - PassKeys
- W3C WebAuthn API
- CNCF Open Policy Agent (OPA)
- W3C Decentralized Identifiers (DIDs)
- OpenID for Verifiable Credentials

Device Identity

- IETF OAuth Token Exchange
- IETF JWTs
- IETF SCIM
- IETF TEEP
- FIDO Device Onboard Specification
- OASIS KMIP (secrets management)
- HOPT and TOTP
- IETF Remote Attestation
- IETF SCITT
- IETF MADINAS
- IETF EAP
- IETF SASL
- IETF ACE

Workload Identity

- IETF MTLS
- CNCF SPIFFE
- IETF OAuth Identity Chaining
- IETF OAuth Token Exchange
- IETF JWT
- W3C Decentralized Identifiers (DID)
- CNC OPA/Rego

Gaps & Challenges

- **Identity is part of most systems**
  - Implementors need to have a basic understanding of identity.
  - They do not need to be experts, but there is not a common vocabulary on what terms such as identity, credentials etc. mean
- **Why No Common Vocabulary?**
  - Many different SDOs have identity requirements and are developing standards to meet their own requirements.
  - Each frames identity in the context of a problems requirements and often use terms in slightly different ways.

Possible Initial Work?

1. Create **Identity Vocabulary** document
   - Provides an overview of terms used across documents
   - Some terms will have different meanings

2. Identify overlapping work between IETF WGs (& other SDOs?)
   - Reduce duplicated work
   - Align vocabulary in future standards

3. Tutorials about identity technologies
   - OAuth, OpenID Connect, SCIM to start with

https://www.iab.org/mailman/listinfo/identity-discuss