okta

Blog

An Exploration of Open Identity Standards

Fei Liu
Emerging Technology Researcher

October 31, 2022

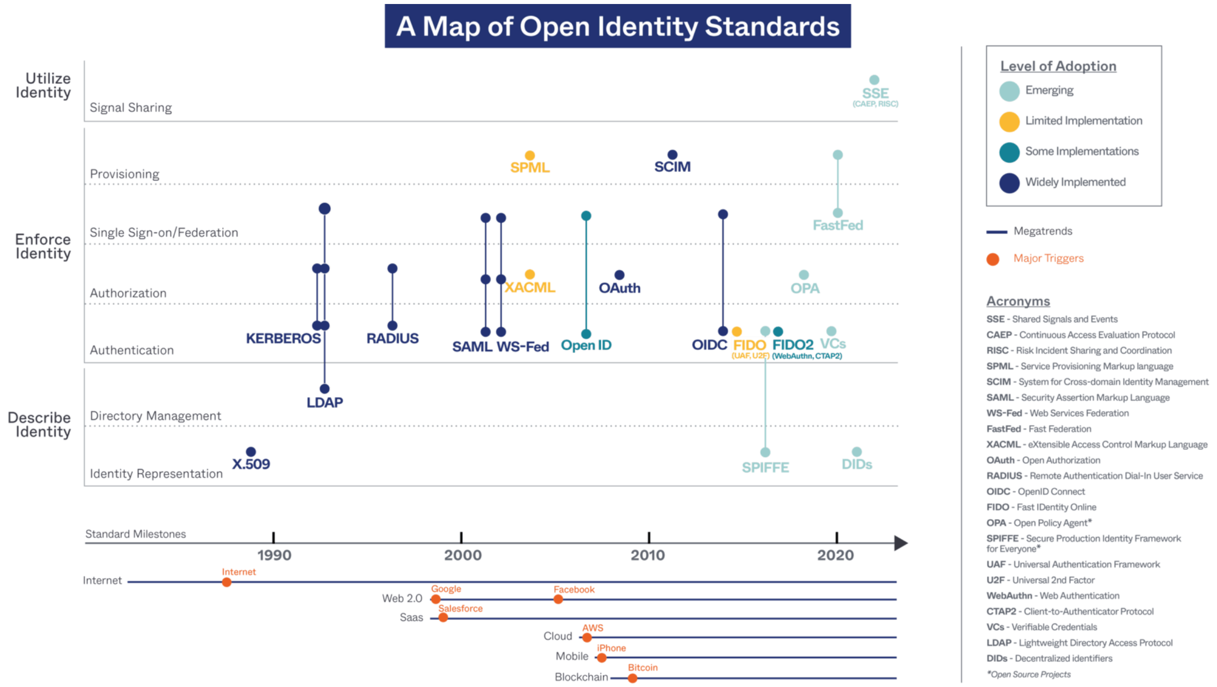
You may be curious to find out how products and solutions are developed, implemented, adopted, and operated. The history of standards is a fascinating place to start.

Standards are well-defined, abstract interfaces that enable industries to develop and thrive. These interfaces ensure ecosystem players with different roles can work together and enable compatibility and interoperability of products built by different vendors. Standards reflect the needs, interests, and pain points of technologies at the time during which they were conceived and developed.

Similar to case studies in law and business, standards can serve as a learning tool for technologists, offering domain understanding from technical and business perspectives. Studying standards history allows us to explore why certain standards emerged, what technical and business challenges they solved, and what the considerations and capabilities were during their developments.

When I joined Okta, one of the first topics our CEO Todd McKinnon tasked me with researching was the history of identity standards, and my insights here emerged from that research. Studying this history has given me a foundation to understa the identity field, identity products, and emerging trends. What follows are my lessons so far.

Register now


A Map of Open Identity Standards

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*

How open identity standards are put to use

We created a chronological map of open identity standards to represent capabilities that describe, enforce, and utilize identity.

- **The "Describe Identity" layer** is responsible for defining identity representation and performing directory management for that representation.
  - *Identity representation* can be in the form of credentials or certificates. We often use usernames and passwords to represent user identities. We use certificate-based identity representation to describe devices, applications, workloads, and even people. The certificate-based identity representation offers better security than usernames and passwords but adds complexity.
  - *Directory management* is used to access and manage an identity directory. This directory is the repository of the identity information of users, systems, networks, services, and applications. Directory management defines the overarching directory structure, schema, and operation.

  - *Authorization* is the process of verifying what someone or something has access to. In this layer, we include coarse-grained and fine-grained authorization, like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC).
  - *Single sign-on (SSO) and federation* give users a single set of credentials or certificates to access multiple systems within a single organization (SSO), or across federated organizations (federation).
  - *Provisioning* is the process of creating, syncing, exchanging, managing, and deleting digital identities. In this layer, we include the techniques for both user and group provisioning, as well as application configuration provisioning.
- **The "Utilize Identity" layer** is responsible for exploring the value propositions of identities that go above and beyond identity itself. One example is signal sharing. Risk signal sharing correlates identity information with other contextual data to assess security risk, provide continuous adaptive risk and trust assessment (CARTA), mitigate security breaches, and offer comprehensive Zero Trust capabilities.

Next, we mapped the most relevant open identity standards into the three layers with a timeline. The three-layer timeline graph describes the functions and evolution of standards.

Open standards:

- X.509
- Kerberos
- Lightweight Directory Access Protocol (LDAP)
- Remote Authentication Dial-In User Service (RADIUS)
- Security Assertion Markup Language (SAML)
- Web Services Federation (WS-Federation)
- Service Provisioning Markup language (SPML)
- eXtensible Access Control Markup Language (XACML)

- Fast IDentity Online (FIDO)
- Verifiable Credentials (VCs)
- Decentralized Identifiers (DIDs)
- Fast Federation (FastFed)
- Shared Signals and Events (SSE)

Open-source projects:

- Secure Production Identity Framework for Everyone (SPIFFE)
- Open Policy Agent (OPA)

The placement of colored dots on the three-layer timeline shows the capabilities and relationships of the standards and projects.

We've color-coded each of the open standards and open-source projects to indicate four levels of adoption: emerging (turquoise color), limited implementation (yellow color), some implementation (teal color), and widely implemented (navy blue color). Since it takes time and effort for standards to reach broad adoption, the assessments of recent standards and projects are opinionated and subject to changing circumstances.

A Brief History of Open Identity Standards and Why They Matter

It is essential to note that identity plays a crucial role in technological advancement. Identity is the lynchpin of technological advancement.

A timeline illustrates the initial development of these underlying technologies in chronological order from the late 1980s to the current day, providing historical context for the evolving landscape. Below the timeline, we've plotted megatrends and aligned them with the major triggers that generated the paradigm shifts.

Megatrends are powerful and transformative, with global technological, economic, and societal impacts. Over the last three decades, key megatrends include the

Next-generation identity standards appear whenever megatrends happen. These new standards address the gaps and challenges unresolved by the previous generations. Successful open standards solve the biggest pain points that come with the adoption of these megatrends. To gain traction, open identity standards must attract participation from identity providers and applications, and be practical to implement. As new generation identity standards are successfully adopted, earlier identity standards do not disappear overnight. They can coexist with the new ones. Early identity standards like Kerberos, RADIUS, and LDAP, are still widely used and supported.

Here are some examples of how identity standards and technologies advance interactively.

In the identity representation layer, passwords are the most ancient and still the most widely used way to authenticate users. Passwords were invented by **Fernando Corbató** in 1960 to allow different users to access a shared mainframe, when he worked with the Compatible Time-Sharing System (CTSS) at MIT. With the birth of the internet in 1983, users needed a way to communicate over an untrusted network. The X.509 certificates were introduced at the end of the 1990s to provide a secure way to verify the identities of websites, businesses, and devices on the websites. Bitcoin and Ethereum were launched in 2009 and 2015, along with the concept of the blockchain, the underlying technology of cryptocurrencies. Blockchain consists of a ledger system of cryptographically secured linked records. Blockchain is considered a new way of establishing trust without central authorities. Due to the interest in using blockchain as a decentralized peer-to-peer network, decentralized identifiers (DIDs) were introduced around 2020 as a verifiable, decentralized digital identity, stored on a distributed ledger or off-chain.

In the directory management layer, cloud-based directory implementations emerged from their on-premises directory predecessors in the late 2000s and early 2010s as cloud and SaaS adoption continued to grow.

For authenticators in the authentication layer, hardware token products based on One-Time Passwords (OTPs) were implemented at the end of the 1980s as a second factor to enhance **identity security**. X.509-based Smart Cards were introduced in the late 1990s when Congress directed the Secretary of Defense to **implement smart card technology** for the Department of Defense (DoD) to increase efficiency, security, and readiness. To balance security and ease of use, In the authentication and single sign-on federation layers, we began with centralized identity, storing usernames and passwords in machines or databases and performing user authentication directly. With the increasing adoption of the internet and networked computers, federated identity emerged to allow users to log in to different resources with the same set of credentials. SSO provides login convenience and migrates password reuse and weak password problems. Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) are the most popular standards to support federated identity. However, social media giants previously leveraged one type of federated identity implementation—social login—to track user behavior for targeted advertising. Social login became associated with the aggressive and unscrupulous collection of personal data. Due to the awareness of blockchain and user privacy concerns, the concept of decentralized identity began to emerge. Verifiable Credentials (VCs) were introduced at the end of the 2010s, putting credential holders at the center of the identity ecosystem by giving them control of their identities.

In the realm of federated identity, several transitions were underway. Kerberos and LDAP emerged in the 1990s as tools to authenticate users and allow single sign-on for internal company resources. Kerberos and LDAP were based on the client-server model and used Abstract Syntax Notation One (ASN.1) data encoding. As the internet, SaaS, and the cloud rose to prominence, SAML and WS-Federation gained traction to allow secured federation and management of identities across different organizations with different security domains in the 2000s. These standards were based on Simple Object Access Protocol (SOAP) and used Extensible Markup Language (XML) assertions. Alongside the adoption of mobile devices and web technologies, OIDC was introduced in the 2010s to allow single-page applications (SPA), native, and mobile apps to authenticate users. OIDC was based on Representational State Transfer (REST) with JavaScript Object Notation (JSON) web tokens, abbreviated JWT.

In the authorization layer, as Web 2.0 became popular in the first decade of the century, OAuth was introduced to allow users to share information about their accounts with third-party applications and interactive websites. In addition, open-source projects like OPA emerged in the late half of the 2010s in response to the adoption of the cloud.

In the provisioning layer, the need to easily federate an identity provider and an application led to the development of FastFed in recent years, to ease the use of prevent and mitigate security breaches.

An Overview of Open Identity Standards

In this section, we'll provide a concise overview of individual identity standards. It aims to cover what these standards were built for, and why, as well as key players, major milestones, how successful the efforts have been, and why. However, we won't get into the details of each standard. For more thorough discussions, we'd recommend **Identity, Unlocked**, where Vittorio Bertocci invites identity standard experts to discuss identity specs and trends meticulously, or Aaron Parecki's **OAuth 2.0 Simplified**, which provides comprehensive descriptions of OAuth and OIDC.

X.509

An X.509 (pronounced "ex five oh nine") certificate binds an identity to a public key using a digital signature. It includes a digital certificate containing a **public key** for a given entity and a unique name for that entity, together with other information rendered unforgeable by a digital signature for the certificate issued by a certificate authority.

X.509 was defined by the International Telecommunications Union (ITU) and was initially designed as the secure access method for updating electronic directory services. It provides users with secure access to digital resources and helps systems avoid cryptographic man-in-the-middle attacks. The initial version of **X.509** was published in 1988, followed by version 2 in 1993, and version 3 in 1996.

Nowadays, X.509 certificates allow websites, users, businesses, and devices to prove their identities. X.509 certificates are widely used as an essential part of the international X.509 public key infrastructure (PKI). An X.509 certificate is natively embedded in multiple well-known modern security technologies, such as the Transport Layer Security (TLS) protocol, Secure Multipurpose Internet Mail Extensions (S/MIME) protocol, and IP Security (IPsec) Virtual Private Networks (VPN).

information services over an IP network. LDAP allows clients to perform a variety of operations in a directory server, including storing and retrieving data, searching for data that match a given set of criteria, authenticating clients, and more. The standard TCP ports for LDAP are 389 for unencrypted communication, and 636 for LDAP over a TLS-encrypted channel.

The protocol was created by the University of Michigan. LDAP was originally intended to be a lightweight alternative protocol for accessing X.500 directory services through the simpler and widespread TCP/IP protocol stack. **LDAPv2** was the first standard version of LDAP published in 1993 and was obsoleted by **LDAPv3**, published as IETF RFC 2251 in 1997.

LDAP influenced subsequent internet protocols and was the basis for Microsoft's Active Directory. **Open-source implementations of LDAP** include **OpenLDAP**, ApacheDS, OpenDJ, and 389 Directory servers. Major cloud providers and many modern technologies still provide integrations to LDAP.

Kerberos

Kerberos (generally pronounced "kur-bur-ohs") is a network authentication protocol. It provides mutual authentication by enabling users and service systems to authenticate each other. **Kerberos uses secret-key cryptography** and a trusted third party, a Key Distribution Center (KDC), for authenticating client-server applications and verifying user identities.

Kerberos was initially developed by the Massachusetts Institute of Technology (MIT) in the late 1980s. Kerberos V5 was published in 1993 as Internet Engineering Task Force (IETF) RFC 1510, which was then made obsolete by RFC 4120 in 2005. MIT released its implementation of Kerberos as **Open Source software** in 1987 and has been enhancing it ever since. Kerberos achieved widespread adoption in both UNIX-like and Windows systems. Windows 2000 and later versions use Kerberos as their default authentication method. Kerberos implementations also exist for other operating systems like macOS, FreeBSD, UNIX, and Linux.

Remote Authentication Dial-In User Service (RADIUS)

initially based on the User Datagram Protocol (UDP) on ports 1812 and 1813, and later supported Transmission Control Protocol (TCP) as a transport layer, with TLS encryption for enhanced security. The protocol supports credential- and certificate-based authentication.

In 1991, Livingston Enterprises developed RADIUS as a National Science Foundation Network (NSFnet) request for proposal (RFP), which Merit Network then sent out. Livingston Enterprises and Merit worked to gain industry acceptance for RADIUS as a protocol. In 1997, RADIUS was published as IETF RFC 2058 and RFC 2059. Current versions are **RFC 2865** and **RFC 2866**, published in 2000.

Since the 2000s, Microsoft has implemented RADIUS in Internet Authentication Service (IAS) and Network Policy Server (NPS). RADIUS is still used to authenticate users to many applications and devices, such as WiFi access, VPNs, Virtual Desktop Infrastructure (VDI), network routers, and controllers. There are plenty of open-source implementations, including FreeRADIUS, and daloRADIUS.

Security Assertion Markup Language (SAML)

Security Assertion Markup Language (**SAML** (pronounced "sam-el")) is an XML-based framework for communicating user authentication, entitlement, and attribute information. It is used to enable web browser SSO, allowing a service provider to contact a separate enterprise identity provider to authenticate users.

SAML was introduced to allow secured federation and management of identities across different organizations with different security domains. The standard was developed initially in 2001 under the Organization for the Advancement of Structured Information Standards (OASIS). OASIS announced the SAML V1.0 specification as an OASIS Standard in November 2002. SAML V1.1 was then announced in September 2003. SAML 2.0 was introduced in 2005 and remains the current version of the standard.

By 2008, **SAML had gained momentum in financial services**, higher education, government, and other industry segments. Support appeared in major application server products and was commonly found among web services management and

Web Services Federation (**WS-Federation** or WS-Fed) enables identity, account, attribute, authentication, and authorization federation across different trust realms. WS-Federation was created in 2003 as a part of **the larger WS-Security Framework**, which included WS-Authorization, WS-Trust, and WS-Policy.

WS-Federation was created by BEA, IBM, Microsoft, RSA Security, and VeriSign. It has since been codified as an OASIS standard. WS-Federation v1.0, v1.1, and v1.2 were released in July 2003, December 2006, and May 2009, respectively.

WS-Federation was primarily championed by Microsoft, which invested heavily in incorporating WS-Federation into its products, such as Active Directory, Active Directory Federation Services (ADFS), and Windows Identity Foundation (WIF). However, Microsoft did not use WS-Federation on Azure cloud architecture.

Service Provisioning Markup Language (SPML)

Service Provisioning Markup language (**SPML**) enables the exchange of user-, resource-, and service-provisioning information between cooperating organizations. **SPML is an XML-based** provisioning request-and-response protocol between requestors, such as enterprise applications, and providers, such as identity management systems. SPML v1.0 and v2.0 were **standardized by OASIS** in October 2003 and April 2006, respectively. Today, **few SPML implementations exist** due to the complexity of the v2 standard and the lack of interoperability across SPML implementations.

eXtensible Access Control Markup Language (XACML)

eXtensible Access Control Markup Language (**XACML** (pronounced “exac-mil” or “zack-mil”)) is a declarative fine-grained, attribute-based access control policy language, an architecture, and a processing model describing how to evaluate access requests according to the rules defined in policies. XACML is an XML-based markup language designed specifically for ABAC, but also compatible with RBAC. The XACML model supports and encourages the separation of enforcement from

OpenID and OpenID Connect (OIDC)

OpenID (pronounced "open eye dee") allows users to sign in to multiple websites with an existing account, without needing to create new passwords. The original OpenID authentication protocol was developed in May 2005. The **OpenID Foundation** was formed in June 2007, and **OpenID 2.0** was published in December 2007.

OpenID Connect (**OIDC**) is the third generation of OpenID technology, introduced in February 2014. But OIDC was not backward compatible, so the original OpenID protocols (OpenID 1.0 and 2.0) are essentially gone. OIDC is **an authentication layer on top of the OAuth 2.0 authorization framework**. It uses REST/JSON message flows, and is more API-friendly than OpenID 2.0, allowing SPA, native, and mobile apps to request and receive information about users and authenticated sessions. OIDC enables SSO across applications and APIs. OIDC and OAuth 2.0 are suitable for native mobile and browser-based JavaScript apps, and they are lightweight compared to SAML 2.0.

By 2016, over one billion OpenID-enabled accounts and over one million websites accepted **OpenID** for logins. **Several large organizations issued or accepted OpenID**, including Google, Facebook, Yahoo!, Microsoft, AOL, MySpace, Sears, Universal Music Group, France Telecom, Novell, Sun, and Telecom Italia. Today, OIDC and OAuth 2.0 are the most popular identity standards with wide adoption by identity providers and applications.

Open Authorization (OAuth)

Open Authorization (**OAuth** (pronounced "oh auth")) is an open standard for secure designated access. Users grant applications and application programming interfaces (APIs) access to their information with tokens. OAuth provides authorization flows for web applications, desktop applications, mobile devices, servers, constrained devices, and APIs.

OAuth was developed for use with internet applications and on mobile platforms. Google and Twitter started the OAuth discussion in 2006. IETF decided to formally accounts with third-party applications or websites. Nowadays, OAuth 2.0 is a popular identity standard with widespread adoption by identity providers and applications.

System for Cross-domain Identity Management (SCIM)

System for Cross-domain Identity Management (**SCIM** (pronounced "skim")) is a standard for automating the exchange of user identity information between identity domains, or IT systems. SCIM is used to automatically add or delete accounts for users in external systems, and share information about users, groups, and other resource types. SCIM uses a REST API with data formatted in JSON. Historically, it also supported payloads with an XML format.

SCIM was designed to make identity management easier in cloud-based applications and services. SCIM 1.0 was released in 2011 by a SCIM standard working group organized under the Open Web Foundation. SCIM 2.0 was released as IETF RFC in 2015. **SCIM has been adopted by identity providers** and applications as more and more organizations rely on a growing offering of SaaS applications.

Fast IDentity Online (FIDO), Universal Authentication Framework (UAF), Universal 2nd Factor (U2F), Client-to-Authenticator Protocol (CTAP2), Web Authentication (WebAuthn)

Fast IDentity Online (FIDO (pronounced "Fido")) is authentication technology designed to standardize the use of authenticators. The **FIDO Authenticator** is a set of hardware and software that implements the authenticator portion of the FIDO protocols. **FIDO aims** to address the lack of interoperability among strong authentication technologies and remedy problems users face when dealing with passwordless and multi-factor experience for users. UAF 1.0, 1.1, and 1.2 were released in December 2014, February 2017, and November 2017, respectively.

- Universal 2nd Factor (U2F) was a model of authentication that enabled users to use a credential stored on a second-factor authenticator in addition to a password. Solutions built with U2F utilized authenticators to create a simpler second-factor authentication (2FA) experience. U2F 1.0 and 1.2 were released in October 2014 and April 2017, respectively.

The World Wide Web Consortium (W3C) and the FIDO Alliance started a joint effort on FIDO 2.0, which includes CTAP and WebAuthn. CTAP, a merger of UAF and U2F use cases, addressed both FIDO's passwordless and second-factor experiences. The CTAP specification refers to two protocol versions, the CTAP1/U2F protocol, and the CTAP2 protocol. CTAP2 Proposed Standard and Implementation Draft were published in September 2017 and February 2018, respectively.

WebAuthn (pronounced "web auth en") is a browser-based API that allows web applications to simplify and secure user authentication via strong authenticators. WebAuthn supports two types of authenticators: *platform authenticators*, such as built-in biometric authenticators in phones or laptops; and *roaming authenticators*, such as hardware security keys. For both types, WebAuthn uses public key cryptography to protect users from phishing attacks.

The Working Draft of the WebAuthn standard was published in May 2016. The **WebAuthn Level 1 standard became a W3C recommendation** in March 2019, and the Level 2 specification was recommended in April 2021. A Level 3 specification is currently a First Public Working Draft. **WebAuthn is supported in Chrome, Firefox, Edge, Safari, and Brave web browsers**, as well as the following platforms: Android 7+, iOS 14.5+, Windows 10, macOS Catalina, and macOS Big Sur. Combining WebAuthn and CTAP 2.0 provides a strong authentication solution for web applications.

Secure Production Identity Framework for Everyone (SPIFFE)

Distributed design practices such as micro-services, container orchestrators, and cloud computing have led to production environments that are increasingly dynamic and heterogeneous. A first-class identity framework for workloads in an organization becomes necessary. SPIFFE was proposed in 2016, joined the **Cloud Native Computing Foundation** (CNCF) in early 2018 at the sandbox level, and graduated in September 2022. Since its creation, SPIFFE has been implemented by projects such as Envoy, gRPC, Istio, Kubernetes, Sigstore, and Tekton.

Open Policy Agent (OPA)

Open Policy Agent (**OPA** (pronounced "opa!" like the Greek expression)) is an open-source, general-purpose policy engine that enables unified, context-aware policy enforcement across an entire software stack. OPA provides declarative fine-grained control for cloud-native environments. It specializes in infrastructure authorization, and integrates with modern-day systems and platforms like Kubernetes, Envoy, Kafka, SQL, Terraform, and Linux Pluggable Authentication Modules (PAM). The project was accepted into the CNCF sandbox in April 2018 and graduated in February 2021. **Maintainers primarily come from** Google, Microsoft, VMware, and Styra.

Verifiable Credentials (VCs)

Verifiable Credentials (**VCs**) are an emerging open standard for digital credentials. They can represent information found in physical credentials, like a passport or license, as well as types of information that have no physical equivalent, like ownership of a bank account. VCs are claims and metadata that are digitally signed, cryptographically verifiable, and tamper-resistant. VCs place credential holders at the center of the identity ecosystem, giving individuals control of their identity attributes. Verifiable Credentials Data Model 1.0 and 1.1 were published as a W3C Recommendation in November 2019 and March 2022, respectively.

Decentralized identifiers (DIDs)

Decentralized identifiers (**DIDs** (pronounced either "dids" or "dee-eye-dees")) are an emerging type of identifier that enables verifiable, decentralized digital identity.

Recommendation in August 2021.

Fast Federation (FastFed)

Fast Federation (**FastFed**) aims to simplify the administrative effort required to configure identity federation between an identity provider and a hosted application. The specification defines metadata documents, APIs, and flows, enabling an IT administrator to quickly connect two providers that support common standards such as OIDC, SAML, and SCIM. It also allows configuration changes to be communicated directly between the identity provider and the hosted application on a recurring basis. FastFed is a working group under the OpenID Foundation, with participants including Amazon Web Services (AWS), Google, Microsoft, Okta, and SGNL. **FastFed Core 1.0** draft was published in March 2020.

Shared Signals and Events (SSE), Continuous Access Evaluation Protocol (CAEP), Risk Incident Sharing and Coordination (RISC)

Shared Signals and Events (**SSE**) aims to improve API efficiency and security by providing privacy-protected, secure webhooks. It communicates security alerts and status changes of users, continuously and securely, to prevent and mitigate security breaches. SSE is currently leveraged by the CAEP and RISC specifications to achieve this result. The **OpenID Shared Signals and Events Framework Specification 1.0** was published in June 2021.

SSO is a common way of enforcing access control. Widely used identity standard protocols such as SAML and OIDC enable identity providers to assert the validity of access at the time of user login. However, these sessions may last over long durations of time, during which user properties, such as location, authentication, or organizational membership, may change. Relying on information asserted only at the time of login creates security issues due to unauthorized access provided based on the old information.

enables providers to prevent attackers from compromising linked accounts across multiple providers and coordinate in restoring accounts in the event of compromises.

Final Thoughts

Identity plays a critical and influential role in technology evolution. In fact, identity is more crucial than ever before as we become more reliant on myriad digital products and services. Nowadays, corporations build their infrastructure using cloud providers and proprietary data centers. Employees access scores of cloud apps and on-prem resources. Professional and personal lives blur as we work from home and use personal devices to access corporate resources. Identity connects siloed resources and services and clarifies different use-case scenarios.

The best approach to building identity technology is neutral and interoperable, facilitating choice and flexibility while enhancing security, reducing risk, and enabling people to use any technology they choose. Open identity standards facilitate neutrality and interoperability. They are built with wisdom from the entire industry by bringing identity ecosystem players together. I am impressed and inspired by the contributions of identity providers, app providers, browser providers, operating system providers, and device manufacturers in the journey of identity advancements.

Studying open identity standards has been a great learning experience for me. Thank you so much for reading. I look forward to hearing your thoughts and feedback.

Acknowledgments

Thanks to Stephen Lee, Karl McGuinness, Vittorio Bertocci, Joël Franusic, Aaron Parecki, Moushmi Banerjee, Lee Tschetter, Katie Ryan O'Connor, Havi Hoffman, Desirae Latorre, and Jess Bagherpour for valuable contributions, guidance, and feedback to this article.