*DRAFT* W3C Strong Authentication and Identity Workshop Report  
**Now finalized and posted to** <https://www.w3.org/Security/strong-authentication-and-identity-workshop/report.html>

*December 10th-11th, Redmond, WA*

Table of Contents

[**​1.​ Introduction**](#_sj4s2qtqbbgb) **3**

[**​2.​ Workshop Agenda**](#_q154d76f0amf) **3**

[**​3.​ Presentations**](#_xrjdert8slqh) **5**

[​3.2.​ Understanding Verifiable Credentials](#_vyqkcwdqeclz) 5

[​3.3.​ Understanding Decentralized Identifiers (DIDs)](#_90wkfpbv4d8) 5

[​3.4.​ Understanding DID Authentication](#_sgl36fitmngc) 5

[​3.5.​ Understanding WebAuthentication, CTAP, EAT, FIDO, and Authenticators](#_oncnjhqhookg) 6

[​3.6.​ Understanding JWT/CWT, OpenID, and IndieWeb](#_vnijbo7et7p8) 7

[​3.7.​ Current and Future Challenges:](#_mn50z3his3zp) 7

[3.7.1 Government](#_vy58is43p0mp) 7

[​3.7.2 Healthcare](#_9nvrjewdo8cc) 7

[​3.7.3.​ Market Verticals: Supply Chain](#_5jrp0e4n5apa) 7

[​3.7.4​ Market Verticals: Legal](#_jdx1n1w455) 8

[​3.7.5​ Enterprise: Once Upon a Time](#_v6zngzianpdc) 8

[3.8 Exploring Cultural and Economic Perspectives](#_jl17xkohed91) 8

[3.8.1 Current Situation of Japanese fragmented ID Platforms](#_g06tlm4irt1v) 8

[3.8.2 Automatic Identification Standards](#_fixizo9vscam) 8

[3.8.3 Law and Borders](#_qz36gm2dh86c) 8

[​3.9.​ Trusted Identity](#_p4bfv7wg3cp5) 9

[​3.10. Avoiding Mistakes and Minefields](#_emcvlvfjv72c) 9

[​3.11.​ Roadmap: Attestations](#_y94gyyp19fh) 9

[​3.13.​ Roadmap: Decentralized Identifiers and Verifiable Credentials (VC)](#_jdxfpqb7cfdh) 9

[​3.14.​ Roadmap: Biometrics](#_encrgce3351w) 9

[​3.14.​ Roadmap: Payment Authentication](#_iplkt8ghexmb) 9

[**4.​ Data Produced by Workshop**](#_avy2kwt9zu0g) **10**

[**​5.​ Identified Trends**](#_tdmdaw6d538d) **10**

[​5.1.​ Integration of WebAuthn with Legacy Systems](#_p1g0huocvdht) 10

[​5.2.​ Decentralized Identifiers](#_j3gqoilu1w02) 10

[**​6.​ Community Next Steps**](#_ag34wpxg2nl2) **10**

[**​7.​ W3C Next Steps**](#_yq0zufgrd5wt) **10**

# ​1.​ Introduction

The W3C Strong Authentication and Identity Workshop gathered experts in the space to explore the existing standards landscape, examine existing technology roadmaps, and identify potential future work for how strong identity and strong authentication should work on the web. The workshop explored aligning recent W3C specifications (WebAuthn, Verifiable Claims, Web Payments) and work that is ongoing in the W3C Credentials Community Group (DID, DIDAuth) along with the IETF and ISO, as well as other existing community standards such as IndieAuth, Open ID Connect, OAuth, and SAML.

# ​2.​ Workshop Agenda

Minutes: <https://www.w3.org/Security/strong-authentication-and-identity-workshop/minutes.html>

|  |  |  |
| --- | --- | --- |
| **Time** | **What** | **Presenter** |
| **Monday, December 10th** |  |  |
| 8:30 AM | Registration / Settling | Program Committee / W3C Staff |
| 9:00 AM | Welcome and Procedural | Wendy Seltzer |
| 9:30 AM | Understanding Verifiable Credentials | Dan Burnett |
| 9:50 AM | Understanding DIDs | Kim Duffy |
| 10:10 AM | Understanding DID Auth | Markus Sabadello |
| 10:30 AM | Break |  |
| 11:00 AM | Understanding WebAuthn, CTAP, EAT, FIDO and Authenticators | Tony Nadalin  Dirk Balfanz  Rae Hayward |
| 11:30 AM | Understanding JWT/CWT, OpenID, and related ecosystem | John Bradley  Mike Jones  Aaron Parecki |
| 11:50 AM | Explanation of Breakout Sessions (Goals/Output) | Kaliya Young |
| 12:10 PM | Lunch |  |
| 1:30 PM | Breakout #1: Positions on Presented Technologies / Concerns / Potential Work Items | All |
| 2:00 PM | Breakout #2: Positions on Presented Technologies / Concerns / Potential Work Items | All |
| 2:30 PM | Report Out to Entire Group on Concerns and Potential Work Items | Kaliya Young |
| 3:00 PM | Break |  |
| 3:30 PM | Market Verticals - Understanding current and future problems  \* Government - Peter Watkins  \* Healthcare - Allen Brown  \* Supply Chain - Jim Masloski  \* Legal - Scott David  \* Once upon a time - John Fontana | Industry |
| 4:30 PM | Wrap up / Agenda Gardening | Wendy Seltzer |
| 5:00 PM | Close |  |
|  | Afterhours: Zeitgeist of concerns and potential work items | Program Committee |
| 6:00 PM | Group Dinner | On Campus - |
|  |  |  |
| **Tuesday, December 11th** |  |  |
| 9:00 AM | Procedural / Agenda Gardening | Wendy Seltzer |
| 9:30 AM | Dot voting: Concerns and Potential Work Items | Kaliya - All |
| 9:45 AM | Exploring Cultural and Economic Perspectives | Takashi Minamii  Shigeya Suzuki  Pindar Wong |
| 10:15 AM | Avoiding mistakes and minefields | Jeff Hodges |
|  | Trusted ID | Mary Hodder  Tom Jones |
| 10:45 AM | Morning Break |  |
| 12:00 PM | Lunch |  |
| 2:15 PM | 5 Year Roadmap: DIDs, VCs, and Attestations | Christopher Allen  Mathias Brossard  Greg Kidd |
| 2:45 PM | 5 Year Roadmap: Authenticators | John Bradley  John Callahan  Marie Lathière |
| 1:30 PM | Entire Group: Discussion | Wendy Seltzer - All |
| 2:00 PM | Afternoon Break |  |
| 3:45 PM | Breakouts |  |
| 4:00 PM | Finish |  |

# ​3.​ Presentations

## ​3.2.​ Understanding Verifiable Credentials

A Verifiable Credential is an object a Holder can present to a Verifier showing assertions made by an Issuer. The Verifiable Credential contains one or more claims, metadata, an optional identifier, and a cryptographic proof that makes the digital document tamper-evident. W3C’s Verifiable Claims Working Group is preparing to recommend version 1.0 of the [Verifiable Credentials Data Model](https://w3c.github.io/vc-data-model/) in 2019.

[slides: Understanding Verifiable Credentials](https://www.w3.org/Security/201812-Auth-ID/02_-_Day_1_-_Understanding_Verifiable_Credentials.pdf)

## ​3.3.​ Understanding Decentralized Identifiers (DIDs)

Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority. DID implementations, or “methods”, must specify create, read, update, and delete operations against a target ledger. DIDs “resolve” to DID Documents, which enable operations such as authentication, and DID management through its list of service endpoints and cryptographic key material.

The W3C Credentials Community Group has incubated a draft community group report, [Data Model and Syntaxes for Decentralized Identifiers (DIDs)](https://w3c-ccg.github.io/did-spec/). As a next step, the W3C Credentials Community Group has proposed to [form a W3C DID Working Group](https://w3c-ccg.github.io/did-wg-proposal/).

Related documentation:

* [DID Working Group Charter Proposal](https://w3c-ccg.github.io/did-wg-proposal/)
* [DID Use Cases](https://w3c-ccg.github.io/did-use-cases/)
* [DID Specification](https://w3c-ccg.github.io/did-spec/) (published by W3C CCG)

[slides: Understanding DIDs](https://www.w3.org/Security/201812-Auth-ID/03_-_Day_1_-_Understanding_DIDs.pdf)

## ​3.4.​ Understanding DID Authentication

In the Decentralized Identifiers (DIDs) community, the term "DID Auth" has been frequently used in various contexts, without a clear understanding whether it is meant as a high-level concept, or as a set of concrete protocols. If we consider what DIDs and their Decentralized Public Key Infrastructure (DPKI) inherently provide, it seems that "proving control of a DID" for authentication purposes is both very useful and relatively straightforward.

In order to prove such control of a DID, the general approach is as follows: 1. A relying party sends a challenge to a DID controller, 2. The DID controller constructs a signed response and sends it to the relying party, 3. The relying party resolves the DID to its DID Document, 4. The relying party verifies the signed response using the public key discovered from the DID Document.

Beyond this basic flow however, many different projects are currently implementing the high-level concept in different ways, using different data formats, transport mechanisms, and protocols. In order to introduce some clarity, a [report](https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/blob/master/final-documents/did-auth.pdf) was written by the Rebooting-the-Web-of-Trust community to describe the scope as well as different incarnations of the "DID Auth" concept.

Given that "DID Auth" is at this point still a relatively new and unproven idea, there is now much discussion on how it relates to existing authentication technologies such as OIDC and WebAuthentication, which are mature and proven, and which have strong anti-correlation, anti-phishing, and key management properties.

Suggested next steps:

1. Continue to mature the DID and DID Resolution specifications, as a baseline for "DID Auth" and other DID-based protocols and applications.
2. Continue to explore how to re-use existing, mature authentication frameworks such as OIDC and WebAuthentication, and how to combine the strengths of these protocols with new features provided by DIDs.

[slides: Understanding DID-Auth](https://www.w3.org/Security/201812-Auth-ID/04_-_Day_1_-_Understanding_DID_Auth.pdf)

## ​3.5.​ Understanding WebAuthentication, CTAP, EAT, FIDO, and Authenticators

Modern Authentication: “FIDO 2” is an umbrella term for CTAP and WebAuthn. CTAP (client-to authenticator protocol) is developed at FIDO; [Web Authentication](https://www.w3.org/TR/webauthn/), an API by which the browser authenticates to a relying party (web application), is a W3C Recommendation. Together, the two enable strong passwordless authentication for the Web.

EAT: Entity Attestation Tokens, under discussion at the IETF, provide device attestation about provenance. Such attestation can be used in WebAuthn and FIDO to require proof of authenticator strength.

FIDO and Authenticators. FIDO Alliance oversees a certification program to validate the security characteristics of authenticator implementations, at Level 1 through 3+.

[slides: Understanding WebAuthentication, CTAP, EAT, FIDO, and Authenticators](https://www.w3.org/Security/201812-Auth-ID/05_-_Day_1_-_Understanding_WebAuthn,_CTAP,_EAT,_FIDO_and_Authenticators.pdf)

## ​3.6.​ Understanding JWT/CWT, OpenID, and IndieWeb

JSON Web Token (JWT), representation of claims in JSON; can be signed with JWS. Used by OpenID Connect, among others. [OpenID Connect](https://openid.net/connect/) is an identity layer on top of OAuth 2.0.

<https://openid.net/connect/>

[IndieAuth](https://indieauth.net/): Bring your own identity, via URL. Prompt the user for identity, discover the authorization endpoint from the URL, send user there for permission, on the redirect back, exchange authorization code for access token and user’s canonical URL.

[slides: Understanding JWT/CWT, OpenID, and IndieWeb](https://www.w3.org/Security/201812-Auth-ID/06_-_Day_1_-_Understanding_JWT_CWT,_OpenID,_and_Related_Ecosystem.pdf)

## ​3.7.​ Current and Future Challenges:

### 3.7.1 Government

Peter Watkins, Government of British Columbia, shared some identity needs and challenges. Multiple levels of jurisdiction, administration and contexts (individual and corporate, legal title, professional credentials, health, education, justice…). “Damned if we do, damned if we don’t” provide authentication/identity tokens, because there’s high value/infrequent usage of a government-specific identity; but there are privacy and accountability concerns with relying on third parties for government identification.

[slides: Government, Supply Chain, Legal](https://www.w3.org/Security/201812-Auth-ID/08_-_Day_1_-_Market_Verticals_-_Understanding_Current_and_Future_Problems.pdf)

### ​3.7.2 Healthcare

Allen Brown described challenging situations for coalescing health and medical information with identity, including military field hospitals or civilian patients who seek only sporadic emergency care. Identity is needed by payers, providers, patients, and data.

[slides: Healthcare](https://www.w3.org/Security/201812-Auth-ID/08.5_-_Day_1_-_Market_Verticals_-_Health_Care.pdf)

### ​3.7.3.​ Market Verticals: Supply Chain

Jim Masloski shared the challenge of a supply chain ledger that requires transparency for some aspects, and confidentiality for others. Used DIDs to identify the brokers, suppliers, and customers, and Verifiable Credentials to describe products and provenance. A challenge was pulling information from legally mandated forms.

[slides: Government, Supply Chain, Legal](https://www.w3.org/Security/201812-Auth-ID/08_-_Day_1_-_Market_Verticals_-_Understanding_Current_and_Future_Problems.pdf)

### ​3.7.4​ Market Verticals: Legal

Scott David shared “mild” and “wild” perspectives on legal practice relating to DIDs.

[slides: Government, Supply Chain, Legal](https://www.w3.org/Security/201812-Auth-ID/08_-_Day_1_-_Market_Verticals_-_Understanding_Current_and_Future_Problems.pdf)

### ​3.7.5​ Enterprise: Once Upon a Time

John Fontana gave a history of 25 years in tech journalism, covering security, directories, messaging, identity, and the “wild ride from an LDAP directory to where we are now, and how much has been accomplished.” He remarked on the tremendous amount of work standards require, and commended the group, saying that collaboration through standards seemed closer now than ever.

[conclusion of Day 1]

## 3.8 Exploring Cultural and Economic Perspectives

### 3.8.1 Current Situation of Japanese fragmented ID Platforms

Takashi Minamii described the fragmentation and siloed identity systems used in Japan, where conglomerates build their own identity platforms and drivers’ licenses are the most common know-your-customer method. He identified a strong need for a loose identity federation.

### 3.8.2 Automatic Identification Standards

Shigeya Suzuki described structured identifiers, looking at GS1 standards including UPC bar codes. He suggested an opportunity for intersection between the work in GS1 and DIDs.

[slides: Cultural and Economic Perspectives](https://www.w3.org/Security/201812-Auth-ID/10_-_Day_2_-_Exploring_Cultural_and_Economic_Perspectives.pdf)

### 3.8.3 Law and Borders

From an Asia Pacific perspective, Pindar Wong invited the group to think about the next billion+, making self-administered identifiers serve netizen expatriates and displaced people whose right to work online is uncertain or unlawful as they have questionable legal standing or non-lawful status.

[slides: Law and Borders: Self-Administered IDentifiers and NExTPats: NETizen eXpatriates](https://www.w3.org/Security/201812-Auth-ID/10.3_Day_2_-_PindarWong.pdf)

## ​3.9.​ Trusted Identity

Tom Jones and Mary Hodder spoke of the challenges of providing and using a “trusted identity,” one backed with verified claims upon which a recipient can rely.

[slides: Use Case](https://www.w3.org/Security/201812-Auth-ID/12_-_Day_2_-_Trusted_Identity.pdf)

## ​3.10. Avoiding Mistakes and Minefields

Jeff Hodges shared common challenges on the path from idea through specification and implementation. He noted the errors of inconsistent terminology assumptions and models, and that trust doesn’t scale. A principle of “flexitility was proposed -- build something that is nominally useful yet malleable such that it can evolve to satisfy further use cases.”

[slides: Avoiding Mistakes and Minefields](https://www.w3.org/Security/201812-Auth-ID/11_-_Day_2_-_Avoiding_Mistakes_and_Minefields.pdf)

## ​3.11.​ Roadmap: Attestations

Mathias Brossard described attestation as a building-block for IoT security, starting from EAT and RAT.

[slides: Attestation roadmap](https://www.w3.org/Security/201812-Auth-ID/13.5_-_Day_2_-_Attestation-Arm.pdf)

## ​3.13.​ Roadmap: Decentralized Identifiers and Verifiable Credentials

Christopher Allen built a picture of the decentralized identity stack, from Verifiable Credentials (VCs), Decentralized Identifiers (DIDs), DID-Auth, and further potential technologies for future work. He shared the [Credentials Community Group’s roadmap](https://w3c-ccg.github.io/roadmap/) [diagram](https://w3c-ccg.github.io/roadmap/diagram.html).

[slides: DID & VC Architecture roadmap](https://www.w3.org/Security/201812-Auth-ID/13_-_Day_2_-_5_Year_Roadmap__DIDs,_VCs,_and_Attestations.pdf)

## ​3.14.​ Roadmap: Biometrics

John Callahan focused on enterprise use of biometrics with proof-of-liveness enabling “roaming KYC.” (Know Your Customer)

[slides: Biometric Authenticators](https://www.w3.org/Security/201812-Auth-ID/14_-_Day_2_-_5_Year_Roadmap__Authenticators.pdf)

## ​3.15.​ Roadmap: Payment Authentication

Marie Lathière described European regulations requiring strong customer authentication, proposing that delegating authentication to merchants, with WebAuthn, can enable good security and user experience.

[slides: the impacts of European regulation](https://www.w3.org/Security/201812-Auth-ID/14.5_Day_2_-_5_Year_Roadmap__Authenticators,_Gemalto.pdf)

# 4.​ Data Produced by Workshop

Participants broke-out into discussion groups several times. Some of their outputs were reported in [minutes](https://www.w3.org/Security/strong-authentication-and-identity-workshop/10Dec2018.html#item10). Other data were captured on index cards and “dot-voting” sheets. [These materials are linked](https://drive.google.com/drive/folders/190gzWNE-ynAk3DWsU2nN3B4Q2VL3W6IF?ths=true).

# ​5.​ Identified Trends

## ​5.1.​ Integration of WebAuthn with Legacy Systems

There exist large legacy authentication systems that provide high assurance deployed and used by major governments and corporations. Two examples include the Common Access Card (CAC) and the Personal Identity Verification (PIV) card systems. There is work being performed to use this existing infrastructure to create "derived credentials" for use by newer authentication technologies such as that provided by the WebAuthentication specification, and potentially mechanisms provided via DID-Auth.

## ​5.2.​ Decentralized Identifiers and Verifiable Credentials

A number of technology companies that participated in the workshop are involved with building solutions based on Decentralized Identifiers and Verifiable Credentials and integrating them with more traditional identity and credential issuing systems at large corporations and large governments. In many of these projects, W3C's focus on global interoperability and combating vendor lock-in were identified as key reasons that government and industry funding is being directed toward building an interoperable ecosystem. Many of the proof of concepts focus on interoperability at the Decentralized Identifier, Credential Issuer, Credential Holder (digital wallet), and Credential Verifier roles. While much of the work to date has focused on data models, there is increasing interest in interoperable protocols that move the interoperable data formats from DID Ledger to Issuer to Holder to Verifier.

## ​5.3. Privacy-Enhancing Technologies

There is a strong trend towards privacy-enhancing technologies that place primary control of identifiers, credentials, and authenticators into the hands of individuals. There was also an identified desire to move away from centralized control and storage for information related to identifiers, credentials, and authenticators. While this bodes well for addressing a variety of recent data breaches and questions around data sovereignty, the community seemed to agree that there was still a great deal of work that needed to be done to ensure privacy-enhancing technologies were used by default in the future. Many in attendance at the workshop noted that constant vigilance would be required by the W3C community, as well as the greater technical community, to ensure the current trend continues.

# ​6.​ Community Next Steps

The following next steps have been identified by members of the community:

* The next Rebooting the Web of Trust (RWoT) is March 1-3 in Barcelona. All of these are expected to be active topics there, especially DIDs and the general direction of turning “DID Auth” into other existing protocols.
* The next Internet Identity Workshop is April 30 through May 2 in Mountain View, CA. This too is expected to continue to advance the community dialog. <https://www.internetidentityworkshop.com/>
* W3C Credentials Community Group Roadmap: <https://w3c-ccg.github.io/roadmap/diagram.html>
* IETF non-WG EAT list (Entity Attestation Token) <https://mailarchive.ietf.org/arch/browse/eat/>
* IETF non-WG RATS list (Remote ATtestation ProcedureS) <https://mailarchive.ietf.org/arch/browse/rats/>and draft charter <https://datatracker.ietf.org/doc/charter-ietf-rats/>

# ​7.​ W3C Next Steps

The following next steps are currently under way at W3C:

* DID charter out for advance-notice review: <https://lists.w3.org/Archives/Public/public-new-work/2019Feb/0004.html>
* Verifiable Claims Data Model v1.0 nearing Candidate Recommendation: <https://w3c.github.io/vc-data-model/>
* WebAuthn API is a W3C Recommendation: <https://www.w3.org/TR/webauthn/>. The WG is preparing v2 work.

Upcoming F2Fs and Meetings

* The Verifiable Claims Working Group has a face-to-face meeting in Barcelona March 4-5, immediately following RWoT.