

DRAFT Text revised 28.10

A DIF & ToIP joint Statement of Support for the [Decentralized Identifiers \(DIDs\) v1.0](#) specification becoming a W3C Standard.

This statement was co-written by DIF and ToIP, it can also be read at [ToIP's blog here](#).

On 3rd August 2021, the World Wide Web Consortium [proposed](#) advancing the Decentralized Identifiers (DIDs) v1.0 specification to their W3C Recommendation stage, the ultimate level of the [W3C standards process](#), which indicates that the specification as currently defined is technically sound, mature and ready for adoption. This includes the expectation that this will allow for widespread implementation, as well as further development and ongoing evaluation, paving the way for future versions.

Collectively, the memberships of the [Decentralized Identity Foundation](#) (DIF) and the [Trust Over IP \(ToIP\) Foundation](#) represent over 350 companies globally who are committed to the development and implementation of decentralized identity and trust infrastructure. Many of these organizations have contributed directly or indirectly to the W3C DID 1.0 specification for one simple reason: the DID layer of cryptographically verifiable identifiers is foundational to the common infrastructure we are building together and on top of; therefore, this spec is an integral part of DIF's and ToIP's shared vision for an empowered, secure and interoperable future, and in line with [W3C TAG Ethical Web Principles](#).

As such, DIF and ToIP support the Decentralized Identifiers (DIDs) 1.0 specification **becoming an official W3C Recommendation**. DID 1.0 represents the efforts of over thirty active W3C Working Group contributors over the past two years—on top of contributions from dozens of others in the W3C Credentials Community Group and its predecessors for several years before that. This is a significant milestone in the digital identity sector. Having common ground for development, particularly in terms of interoperability, allows work to continue with renewed energy and focus. It also mitigates the risk of shifting goalposts, which seriously hinders long-term development, investment, and widespread adoption.

DIDs are a critical part of a technical foundation for the products and activities of many of our members. Many of the implementations in the [DID Working Group's implementation](#) report were developed by engineers and companies who collaborate openly at DIF on points of technical interoperability, and at ToIP on points of policy and governance. DIF also hosts the [Universal Resolver](#), a community project which puts practical intra-DID method interoperability into practice by co-developing a “translation engine” for diverse DIDs with contributions from DIF members and non-members alike. Similarly, other DIF efforts like the [DID Communications](#) protocol and the [Presentation Exchange](#) protocol and ToIP efforts like the [ToIP Trust Registry Protocol](#) serve to align a broad range of implementations and ecosystems already building on these standards, laying the groundwork for robust interoperability across ecosystems and diverse families of technologies.

This specification is the result of half a decade of sustained, broad-based, dedicated work on the part of W3C, DIF, and ToIP members. We acknowledge also the work done by numerous, forward-thinking organizations who have already built working implementations using the provisional specification, thereby laying the foundations of new infrastructures for “identity data”. We believe DIDs will change the course of digital identity by building in better user controls, portability and interoperability at the lowest possible level, while also offering increased security and simplicity for implementers and service providers. This advancement unlocks new opportunities for our digital lives, and we look forward to leveraging DIDs and other technologies developed in the community to champion a new class of user-first, self-owned digital identity systems.

Signed,
DIF & ToIP

October, 2021

END OF POST

TO BE DELETED - REFERENCE ONLY

Suggested existing use-cases, to be included pending confirmation that they are using this DIDCore spec:

[Aruba Health App](#)

[OrgBook BC](#), developed by the Government of British Columbia, Canada

[IATA Travel Pass](#) (all issuing health labs use DIDs)

[MemberPass](#) (all issuing credit unions use DIDs)

Appendix A

Recommendations from the October 2020 W3C TAG Finding, [W3C TAG Ethical Web Principles](#):

Security and privacy are essential

We will write specs and build platforms in line with our responsibility to our users, knowing that we are making decisions that change their ability to protect their personal data. This data includes their conversations, their financial transactions and how they live their lives. We will start by creating web technologies that create as few risks as possible, and will make sure our users understand what they are risking in using our services.

The web must make it possible for people to verify the information they see

We have a responsibility to build web technologies to counter misinformation, allowing information sources to be traceable and facts to be checkable. The concept of origin and source is core to the web's security model. We will make sure the new web technologies we create do not work against this architectural principle.

The web must enhance individuals' control and power

We recognize that web technologies can be used by developers to manipulate people, complicate isolation and encourage addictive behaviors. We recognize these risks and seek to mitigate against them when creating these technologies and platforms. We will therefore favor a decentralized web architecture that minimizes single points of failure and single points of control. We will also build Web technologies for individual developers as well for developers at large companies and organizations. The web should enable do-it-yourself developers.