W3C: Decentralized Identifiers (DIDs) 1.0

return to the W3C Standards

Table 1: Data sheet for Decentralized Identifiers (DIDs) V1.0

Title	Decentralized Identifiers (DIDs) v1.0; Core architecture, data model, and representations
Acronym	DID
Version	1.0
Series	TR
Document Number	
Release Date	21 April 2020 – **Working Draft**
Download	https://www.w3.org/TR/2020/WD-did-core-20200421/

Note: The following is an excerpt from the W3C site. It is provided here as a convenience and is not authoritative. Refer to the original document as the authoritative reference. Given the direct call-out to dlt and blkchn, have included the first two paragraphs of the Introduction as well.
Note: This specification is under active development; implementers are advised against implementing the specification unless they are directly involved with the W3C DID Working Group.

Abstract

Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity. A DID identifies any subject (e.g., a person, organization, thing, dm, abstract entity, etc.) that the controller of the DID decides that it identifies. These new identifiers are designed to enable the controller of a DID to prove control over it and to be implemented independently of any centralized registry, identity provider, or certificate authority. DIDs are URLs that associate a DID subject with a DID document allowing trustable interactions associated with that subject. Each DID document can express cryptographic material, verification methods, or service endpoints, which provide a set of mechanisms enabling a DID controller to prove control of the DID. Service endpoints enable trusted interactions associated with the DID subject. A DID document might contain semantics about the subject that it identifies. A DID document might contain the DID subject itself (e.g. a data model).

This document specifies a common data model, a URL format, and a set of operations for DIDs, DID documents, and DID methods.

Introduction (excerpt)

Conventional identity management systems are based on centralized authorities such as corporate directory services, certificate authorities, or domain name registries. From the standpoint of

cryptographic trust verification, each of these centralized authorities serves as its own root of trust. To make identity management work across these systems requires implementing federated identity management.

The emergence of distributed ledger technology (DLT) and blockchain technology provides the opportunity for fully decentralized identity management. In a decentralized identity system, entities (that is, discrete identifiable units such as, but not limited to, people, organizations, and things) are free to use any shared root of trust. Globally distributed ledgers, decentralized P2P networks, or other systems with similar capabilities, provide the means for managing a root of trust without introducing a centralized authority or a single point of failure. In combination, DLTs and decentralized identity management systems enable any entity to create and manage their own identifiers on any number of distributed, independent roots of trust.