Decentralized Identity Foundation (DIF)

Overview and update for W3C CCG

clare@identity.foundation

July 18, 2023

DIF

Contents

- **DIF Overview**
  - Scope: DIDs, VCs; Issuer, Holder, Verifier Model
  - DIF Mission
  - DIF is a Linux Foundation Project
- **DIF Update**
  - DIF Working Groups
  - Examples of DIF Contributions
  - DIF Ecosystem
  - DIF Identifiers and Discovery WG
  - DIF Applied Cryptography (BBS)
  - DIF Hackathon Summary
  - Use Case Example
  - DIF Korea SIG

DIF

DIF Overview

Decentralized Identity: Primary Scope

DIDs, VCs; Issuer, Holder, Verifier

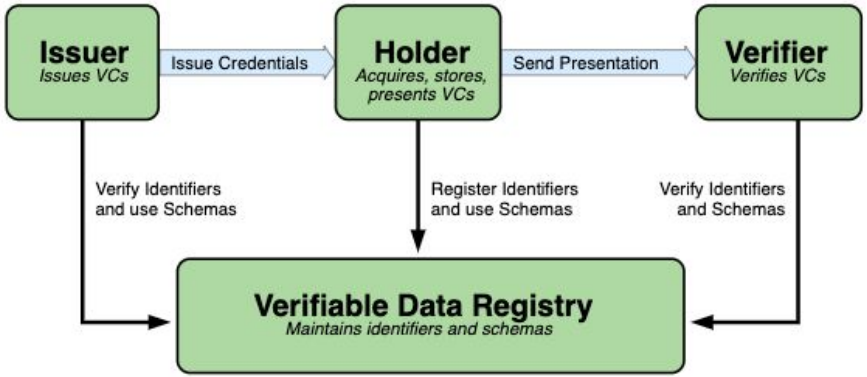
Decentralized Identifiers (DIDs) v1.0

Core architecture, data model, and representations

W3C Recommendation 19 July 2022

Verifiable Credentials Data Model v1.1

W3C Recommendation 03 March 2022



Source: https://www.w3.org/TR/did-core/
Source: https://www.w3.org/TR/vc-data-model/

Decentralized Digital Identity

Decentralized Identifiers (DIDs) v1.0

Core architecture, data model, and representations

W3C Recommendation 19 July 2022

Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity.

A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID.

Source: https://www.w3.org/TR/did-core/

DIF Mission

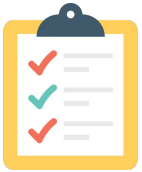
DIF exists to advance the interests of the decentralized identity community, including performing research and development to advance “pre-competitive” technical foundations towards established interoperable, global standards.

DIF Focus

DIF is an **engineering-driven organization** focused on developing the foundational elements necessary to establish an open ecosystem for decentralized identity and ensure interop between all participants.

Structured Collaboration

DIF enables members to engage in pre-competitive industry collaboration by providing processes, tools and Intellectual Property Rights (IPR) protection

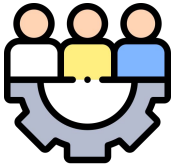


Technical Specifications

Groups in DIF develop specifications for emerging standards, DIF also develops protocols, components and data formats against which implementers can execute

Reference Implementations

Beyond specifications, DIF members develop open source reference implementations of the technical components and protocols they create



Industry Coordination

As a leading industry organization in the decentralized identity space, DIF seeks to align participants to advance their common interests

Images: www.flaticon.com

DIF

Source: https://identity.foundation/governance/about

DIF is a Linux Foundation Project

Part of Linux Foundation

DIF is a Linux Foundation Project, a non-profit 501(c)(6)

IPR Protection

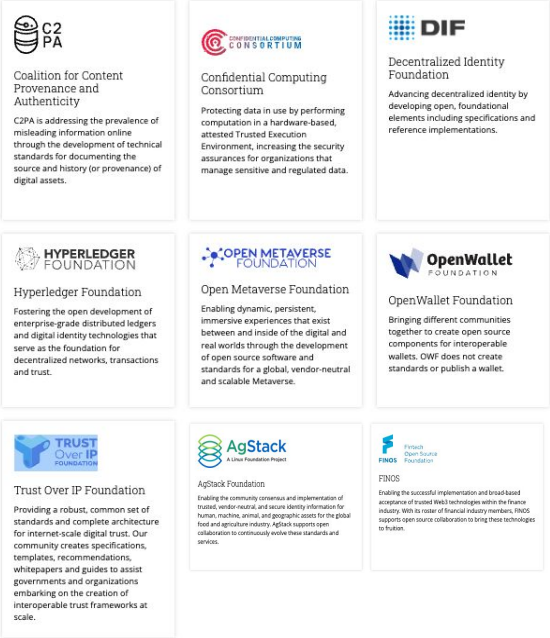
- Specifications created in DIF Working Groups are protected under W3C Patent Policy
- Software is protected under Apache License 2.0

Linux Foundation Digital Trust Initiative

DIF is part of the Linux Foundation “Digital Trust” initiative (May 2023).

Goal:

To improve project discovery and encourage greater collaboration on open source projects with common goals.



Source: https://www.w3.org/Consortium/Patent-Policy/
Source: https://www.apache.org/licenses/LICENSE-2.0
Source: https://www.linuxfoundation.org/blog/aligning-open-source-projects-with-common-objectives-meet-lf-digital-trust
Source: https://www.linuxfoundation.org/projects/digital-trust

DIF

DIF Update

WG creation policy, https://github.com/decentralized-identity/org

DIF Working Groups

Claims and Credentials

Presentation Exchange v2 released Feb 2023
Working towards v2 of Wallet Rendering
Data agreement developing consent receipts

Identifiers and Discovery

Discussion of rotating and revoking keys in DID documents and how that relates to VC issuance and verification

Secure Data Storage

DWN group recently completed the encrypted data vault and they are busy implementing. Work being done on a companion guide

Wallet Security

Work on Universal Wallet Backup Containers
Looking to engage wallet vendors in a forum on common problems in backup and recovery

DIDComm

DIDComm is at v2
Discussion of creating a training, course or DIDcomm orientated playground

Sidetree

See the latest spec for the full Sidetree specification (currently v1.0.1)

Applied Cryptography

BBS updated the IRTF draft which is based on the DIF draft for the IETF meeting in March

DID Authentication

OIDC4VP and OIDC4VC
(This work is being undertaken in OpenID)

Terms
IRTF = Internet Research Task Force (long term focus)
IETF = Internet Engineering Task Force (shorter term, engineering and standards)
BBS, BBS Signature Scheme, comes from the authors: Boneh, Boyen and Shacham

Terms
OIDC4VP = OpenID Connect for VP, Verifiable Presentation
OIDC4VC = OpenID Connect for Verifiable Credentials

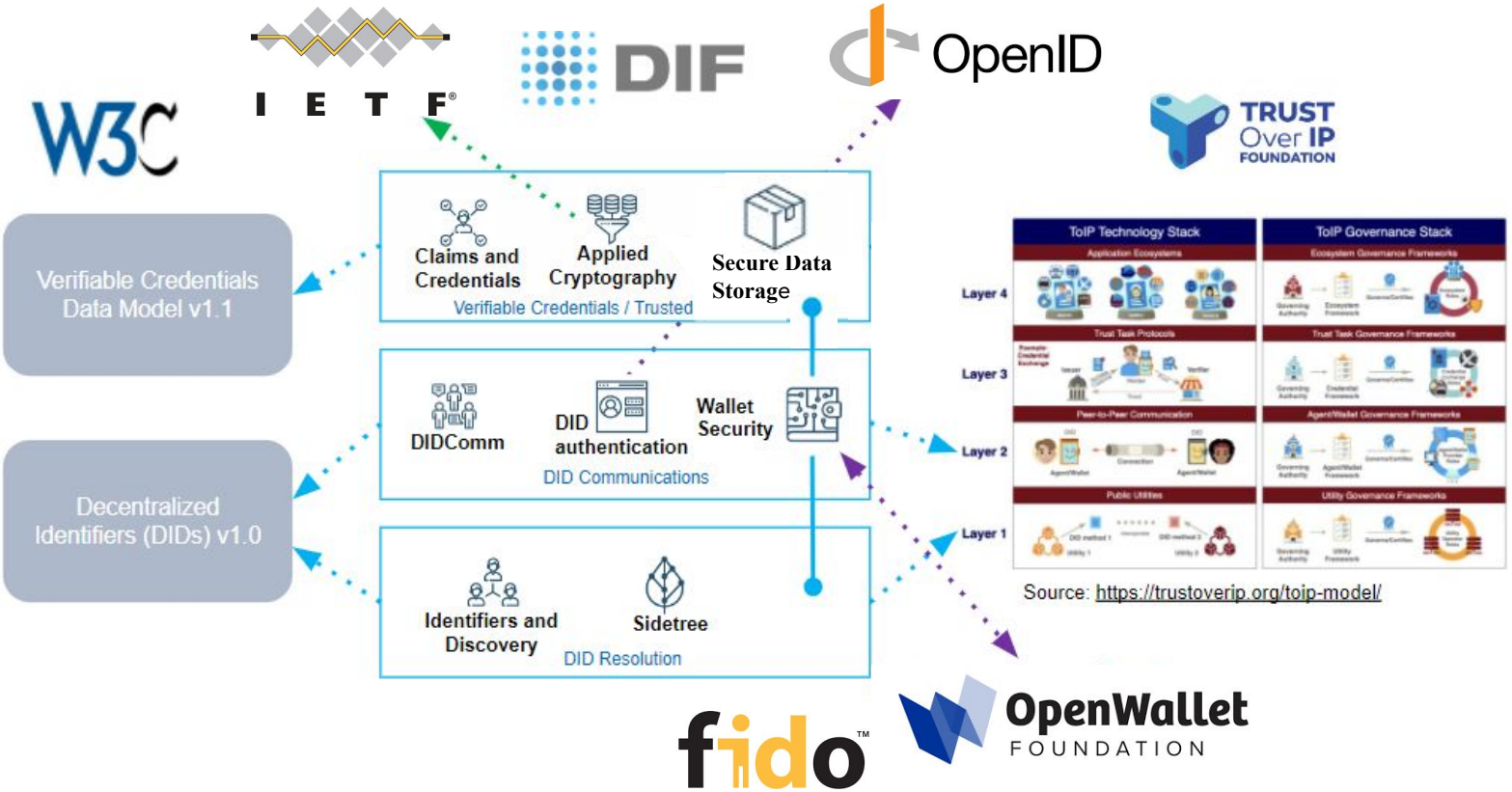
DIF

DWN = Decentralized Web Nodes, check out the AMA (March 2, 2023) by Daniel Buchner here: https://www.youtube.com/watch?v=MNXowKcB73E

Examples of DIF Contributions, WG Focus

Name	Description	Where Used, Links
Universal Resolver	Resolves DIDs across many different DID methods, based on W3C DID Core 1.0 and DID Resolution specifications	Universal Resolver, https://dev.uniresolver.io/, DID linter program, https://didlint.ownyourdata.eu/
Sidetree	A blockchain-agnostic protocol enabling public, permissionless, decentralized DID overlay networks	Used in Identity Overlay Network (ION), a DID Method implementation using the Sidetree protocol atop Bitcoin
DIDComm	Secure, private, transport-agnostic communication built atop the decentralized design of DIDs. Came from Aries, DIDComm v2.1	Contender for ToIP Trust Spanning Protocol, used by Indicio for Aruba travel, Hyperledger Aries.
Presentation Exchange	A set of data formats Verifiers can use to articulate proof requirements and Holders can use to describe proofs, PE 2.0	Used in OIDC4VC flow, specification is here, https://identity.foundation/presentation-exchange/
Wallet Security	A set of APIs to enable Identity Wallet and Verifier interoperability, Wallet container backup	Coordinating with Open Wallet Foundation (OWF) which does software, DIF does specifications
DID Authentication	Went to OpenID Foundation, became OpenID Connect for VCs (OIDC4VC), also Self-Issued OpenID Provider (SIOP)	OpenID OIDC4VC libraries are here, https://openid.net/sg/openid4vc/libraries/
Decentralized Web Nodes (DWNs)	Data storage and message relay mechanism entities can use to locate public or private permissioned data related to a DID	DWN SDK here, https://github.com/TBD54566975/dwn-sdk-js
Applied Cryptography	BBS signatures was presented to IETF 116 in Yokohama in March, IETF published Draft 03 on July 10, 2023	Used by Trinsic, MATTR, and others
JSON Web Proof (JWP)	Addition to JOSE family, supports ZKP, includes analog for COSE, a CBOR Web Proof that mirrors the same features	Initial JWP proposal and planned space for the development of this work
Trust Establishment	Specification by which a Party makes trust statements about a given Party for a given Topic using Trust Establishment Documents	Collaborating with Trust over IP (ToIP), implemented by companies such as Cheqd and Indicio

DIF Ecosystem



DIF

DIF Identifiers and Discovery WG

Charter: "Specifications, implementations, test suites, etc. related to creation, derivation, resolution, management, use of all forms of decentralized identifiers (i.e. including, but not limited to W3C DIDs)"

Meetings: Approximately biweekly, since 2019

Some recent topics:

- DID Lint: https://didlint.ownyourdata.eu/
- JSON schema for DID documents
- did:btco (Bitcoin Ordinals)
- did:polygonid (Polygon ID)
- DIDs for legal entities and natural persons (GDPR)
- New Universal Resolver/Registrar drivers for did:cheqd, did:ethr, etc.
- DIDs and Nostr

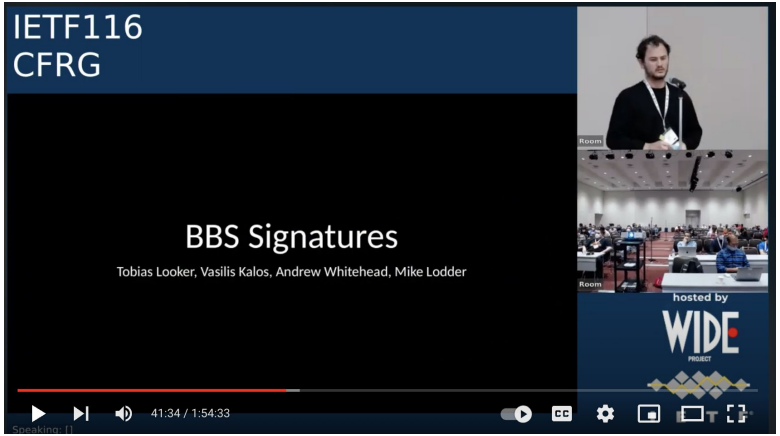
Selected Work Items (Code and Specs)
Universal Resolver
Universal Registrar
did:peer
.well-known DID Configuration
JavaScript: did-resolver, ethr-did-resolver, web-did-resolver
TypeScript: did-jwt, did-jwt-vc
Rust did:key library
DID Registration specification
Secret recovery methods
(former) KERI
(former) Sidetree

Source: GitHub, https://github.com/decentralized-identity/identifiers-discovery

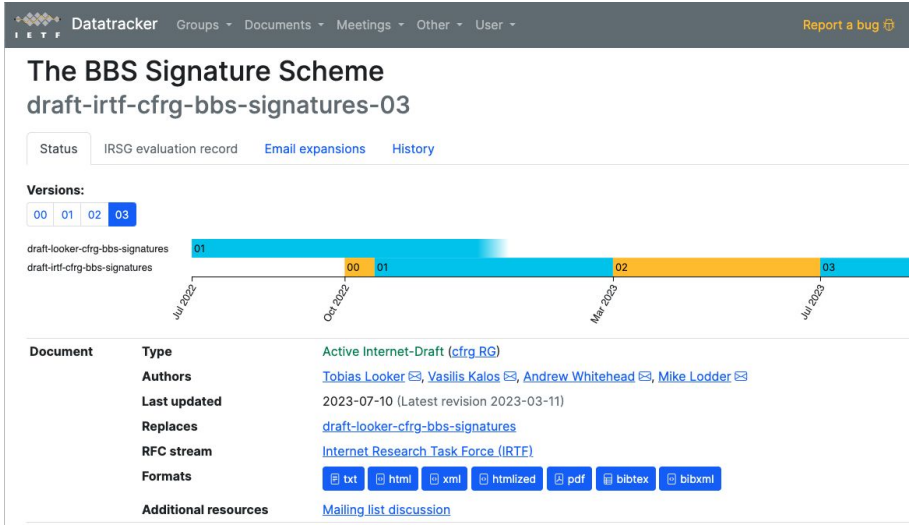
DIF Applied Cryptography WG, BBS Signatures

MARCH: Tobias Looker and Vasilis Kalos presented the updated Draft of the BBS specification at the Cryptography Forum Research Group (CFRG) at IETF 116 in Yokohama (March 2023)

- The specification, developed by the DIF Applied Cryptography WG, describes a pairing-based, multi-message signature that supports selective disclosure and zero-knowledge proofs
- You can watch their presentation here
- The slide deck can be found here, click on *The BBS Signature Scheme*



JULY: Draft 03 integrates the optimizations of Stefano Tessaro and Chenzhi Zhu, reducing the signature and proof size (and proving the security of the scheme)



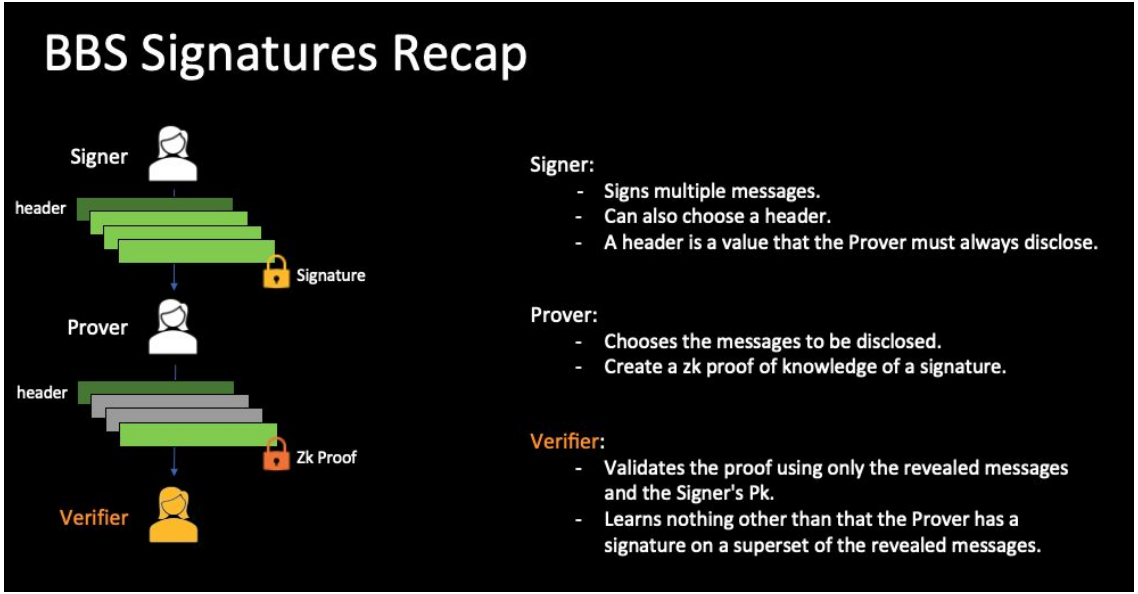
Source: https://datatracker.ietf.org/meeting/116/proceedings/
Source: YouTube video, https://www.youtube.com/watch?v=GZRb-w-xxtY start at 41:20
Source: BBS deck, https://datatracker.ietf.org/meeting/116/proceedings/, click on *The BBS Signature Scheme*
Source: DIF GitHub repo: https://github.com/decentralized-identity/bbs-signature
Source: IETF website, https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/03/
Source: https://christianpaquin.github.io/2023-07-13-of-u-prove-and-bbs.html

BBS Signature Scheme

The BBS Signature Scheme
draft-irtf-cfrg-bbs-signatures-03

Abstract

BBS is a digital signature scheme categorized as a form of short group signature that supports several unique properties. Notably, the scheme supports signing multiple messages whilst producing a single output digital signature. Through this capability, the possessor of a signature is able to generate proofs that selectively disclose subsets of the originally signed set of messages, whilst preserving the verifiable authenticity and integrity of the messages. Furthermore, these proofs are said to be zero-knowledge in nature as they do not reveal the underlying signature; instead, what they reveal is a proof of knowledge of the undisclosed signature.



Source: https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/03/
Source: BBS deck, https://datatracker.ietf.org/meeting/116/proceedings/, click on *The BBS Signature Scheme*

DIDComm

§Purpose and Scope

The purpose of DIDComm Messaging is to provide a secure, private communication methodology built atop the decentralized design of DIDs.

…

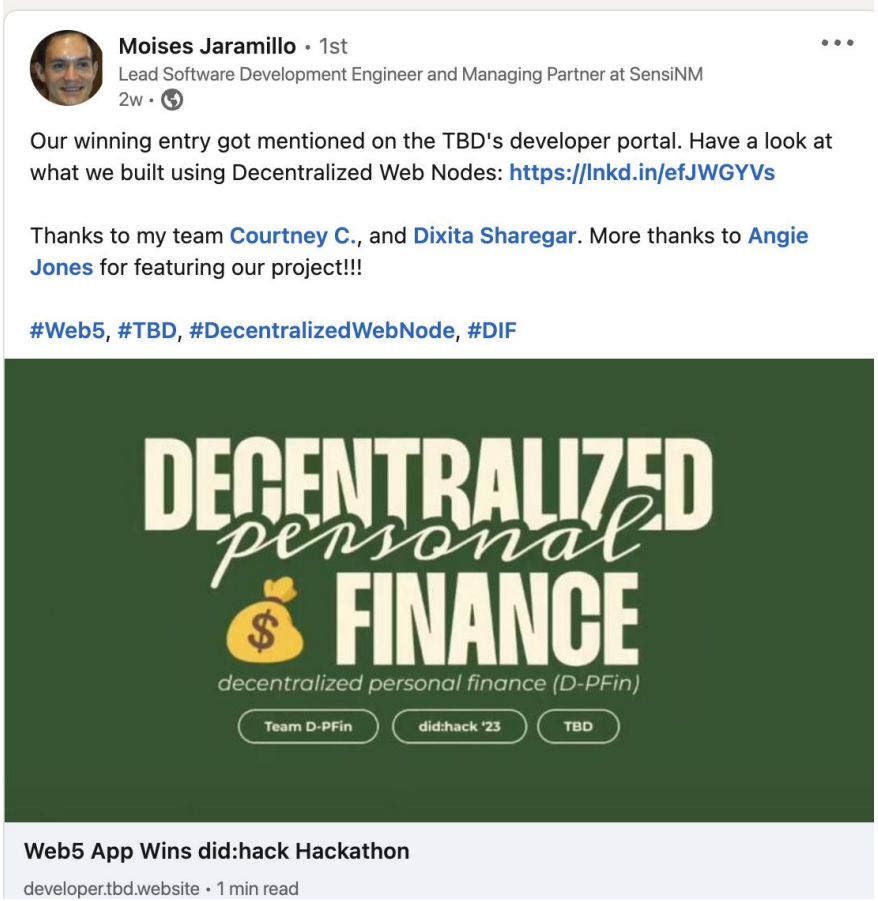
DIDComm Messaging enables higher-order protocols that inherit its security, privacy, decentralization, and transport independence.

Examples include exchanging verifiable credentials, creating and maintaining relationships, buying and selling, scheduling events, negotiating contracts, voting, presenting tickets for travel, applying to employers or schools or banks, arranging healthcare, and playing games.

Source: https://identity.foundation/didcomm-messaging/spec/v2.1/

DIF Hackathon

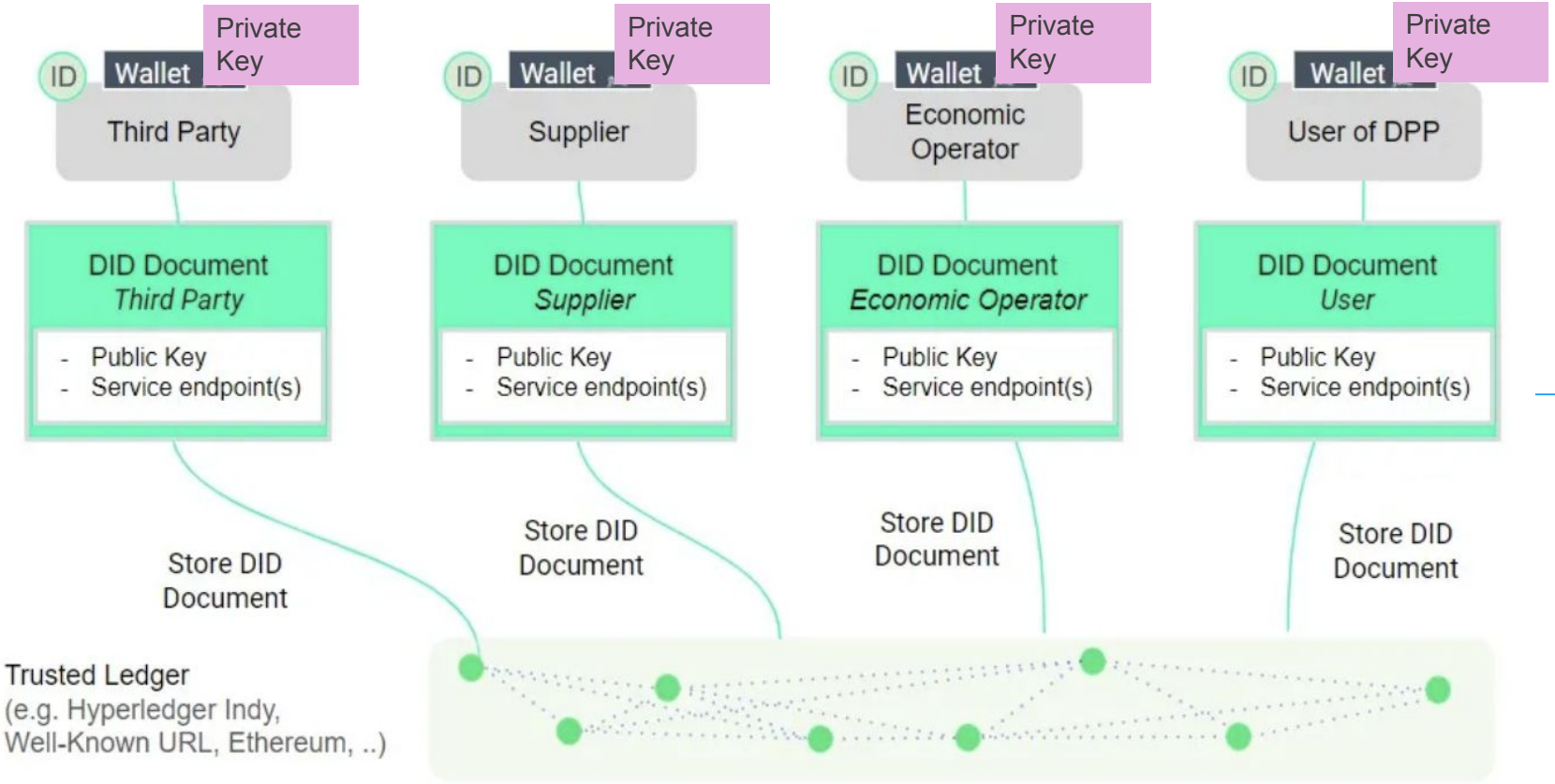
- did:hack (June 5-8, 2023)
- Presenters from Trinsic, Dock, Aviary Tech, TBD, Danube, Spruce ID
- Eventbrite 151/ Discord 143
- 50 participants
- 9 people joined groups or submitted solo
- Winner was *Decentralized Personal Finance (D-PFin)*



Source: https://www.linkedin.com/posts/moisesjaramillo_web5-app-wins-didhack-hackathon-activity-7078076016891453440-_cZn?utm_source=share&utm_medium=member_desktop
Source: https://developer.tbd.website/blog/did-hack/

DIF

Example Use Case: EU Digital Product Passport (DPP)



Source: https://medium.com/@susi.guth/implementing-digital-product-passports-using-decentralized-identity-standards-f1102c452020

DIF Korea SIG Kickoff Meeting

DIF Korea SIG Kickoff Meeting

- **Chair for DIF Korea SIG:** Kyoungchul Park, CEO K4Security (collaborating with Ministry of Science and Information Communication Technology to research Decentralized Identity)
- **Location:** Ramada Encore by Wyndham Busan Haeundae
- **Date and Time:** July 19, 2023, 15:00-19:00

Attendees:

- Vice President of Korea Information Security Society
- Chairman of the Next Generation Authentication Forum and Member of the Personal Information Protection Committee
- Telecommunications Technology Association (TTA)
- Korea Internet & Security Agency
- Bank of Korea
- Relevant Professors and Researchers
- BlockChain Special Zone Officials
- Many corporate officials (inviting Samsung)

Draft Agenda:

- Korea SIG Registration, Purpose, Role
- Discuss hot issues (major issues in the future)
- Upcoming schedule (online meeting, monthly)

Source: https://identity.foundation/SIG-Korea/
Source: https://blog.identity.foundation/korea-sig/

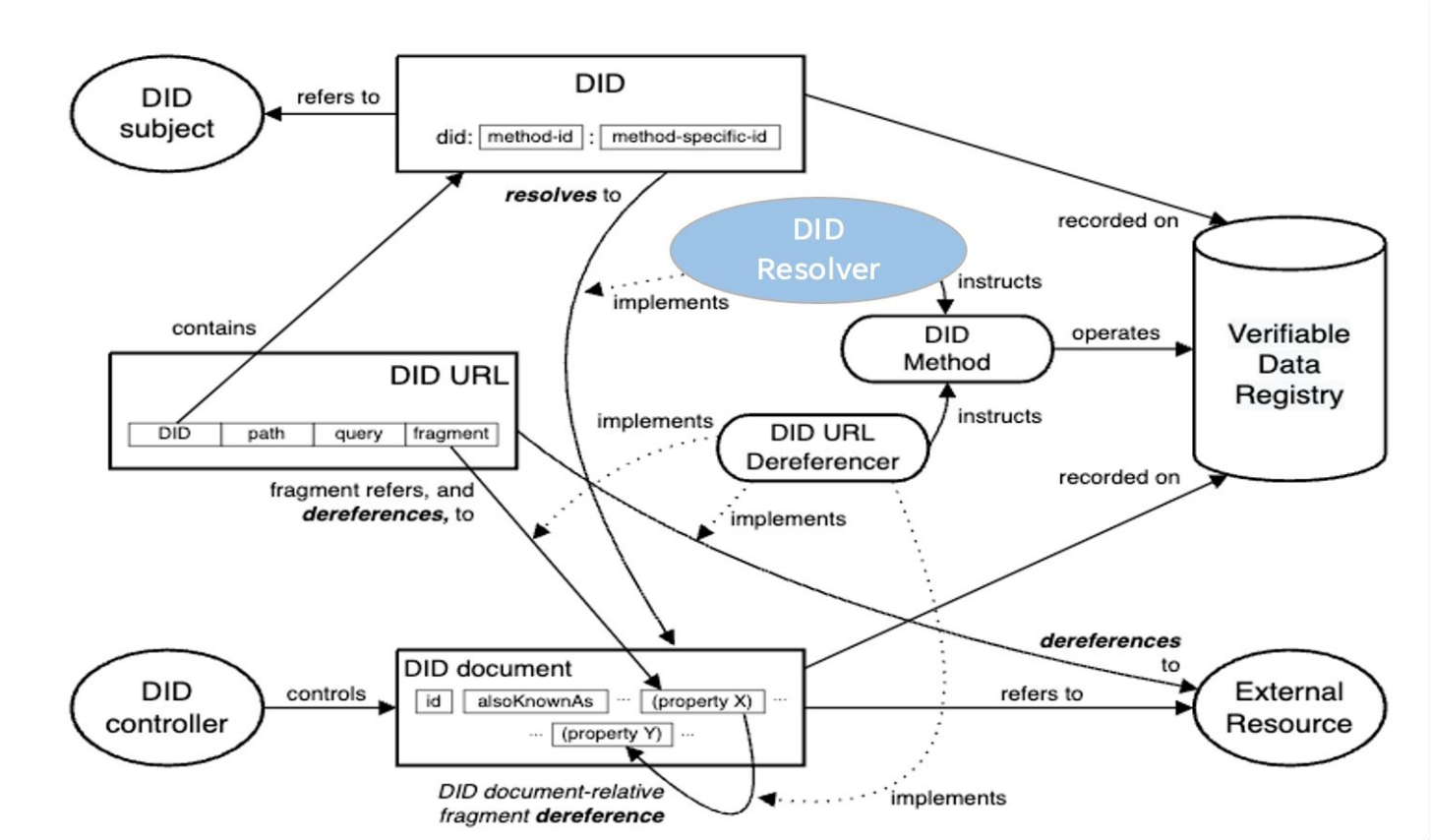
Thank You

DIF website: https://identity.foundation

clare@identity.foundation

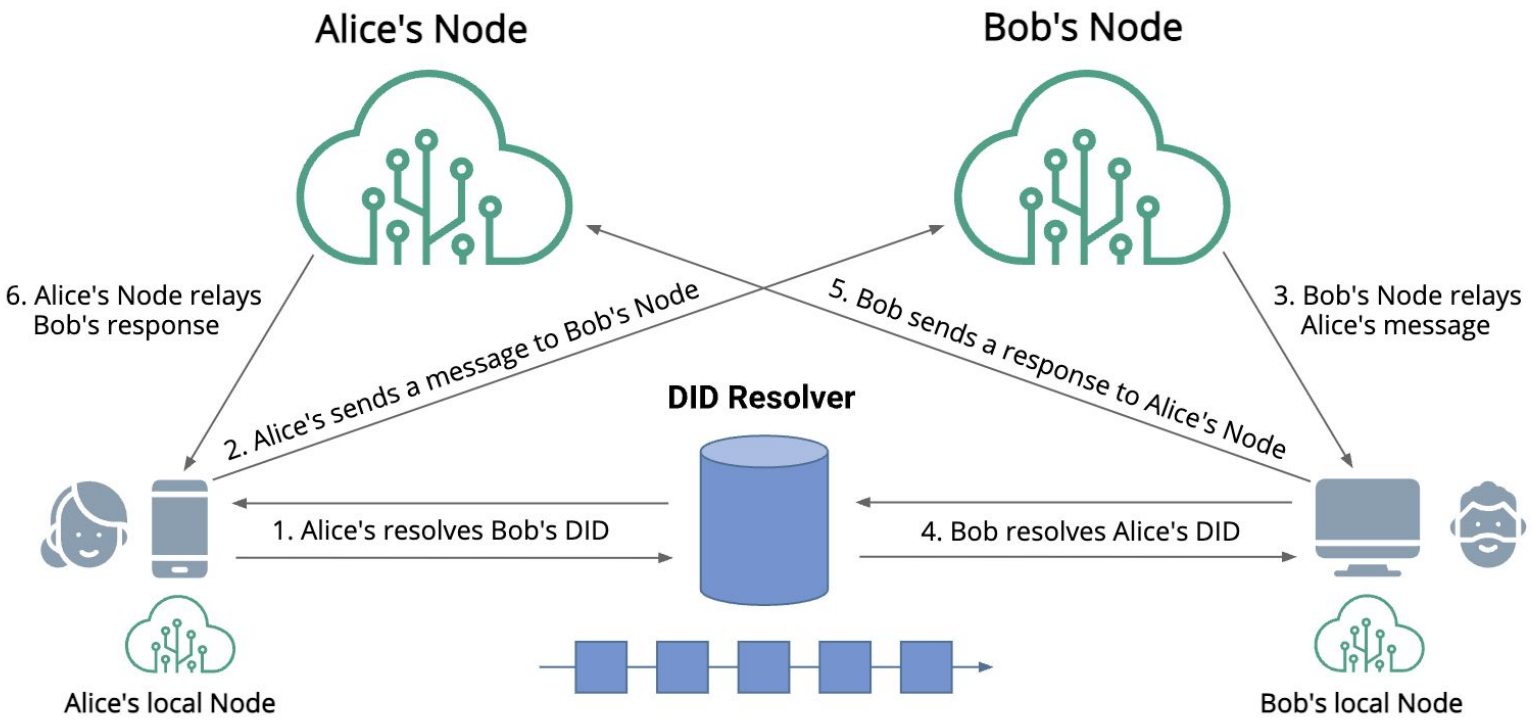
DIF

DID Resolver



Source: https://www.w3.org/TR/did-core/

Decentralized Web Node Topology



Source: https://identity.foundation/decentralized-web-node/spec/#topology

DIF collaborates with our Liaison Partners to build the ecosystem

W3C®

DIN

TNO

Trust Alliance New Zealand

OpenID

Technische Universität Berlin

3 Innovation

TRUST Over IP FOUNDATION

fido ALLIANCE

Digital Identity LABORATORY

DIF

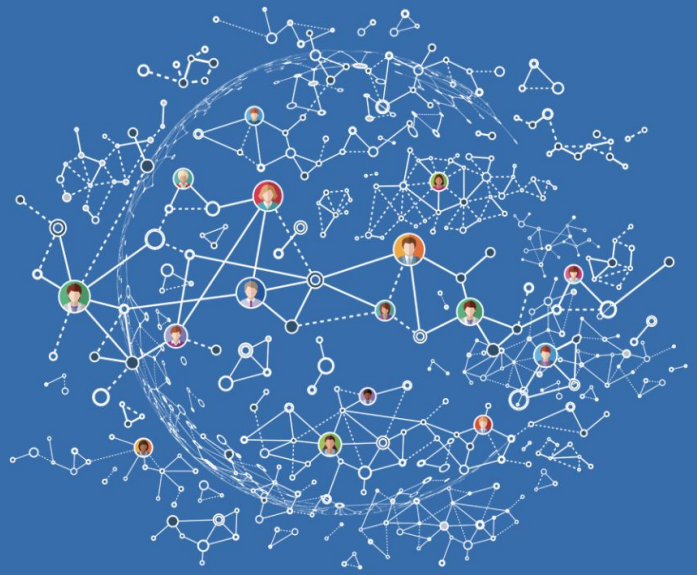
DIF

Work Interoperability Services Events Join DIF Blog About

Together we're building a new identity ecosystem

Join us in developing the foundational components of an open, standards-based, decentralized identity ecosystem for people, organizations, apps, and devices.

BECOME A MEMBER



Nominations are open for the 2023 Steering Committee Election

click here for more information

Source: https://identity.foundation/

Decentralized Identity Myths

Myths

- W3C Recommendations define DIDs and VCs
- Our work is done

Reality

- We are just beginning

Events at ETHDenver (March 2023)

- WalletCon
- ETHDenver Climate Summit, panel, *How Decentralized Identity Will Change the Climate Accountability Conversation*
- did:day – Half-day event focused on DIDs

DID = Decentralized Identifier
VC = Verifiable Credential
W3C = World Wide Web Consortium

Source: https://blog.spruceid.com/announcing-did-day-an-exploration-of-decentralized-identity-at-ethdenver-buidlweek/

DIF

Why decentralized identity?

Decentralized identity enables control over data and brings trust to digital interactions.

It enables numerous commercial use cases beyond identity verification and authentication.

Self-Sovereign Identity has been adopted as a policy goal by legislatures including Canada, Bhutan and EU

Internet-scale trust

Gartner

"The additional layer of security that decentralized identity will offer without compromising consumer privacy is invaluable."

Business value

wipro

"Decentralized identity offers numerous advantages separate of the greater identity autonomy it delivers to customers."

Regulatory alignment

European Parliament

"All EU citizens have the inalienable right to a digital identity that is under their sole control."

https://www.gartner.com/reviews/market/decentralized-identity-solutions
https://www.wipro.com/innovation/improve-detection-of-online-frauds-using-decentralized-identity-management/#
https://www.europarl.europa.eu/doceo/document/ITRE-PR-732707_EN.pdf

DIF

References

- Allen, Christopher; Brock, Arthur; Buter, Vitalik; Callas, Jon; Dorje, Duke; Lundkvist, Christian; Kravchenko, Pavel; Nelson, Jude; Reed, Drummond; Sabadello, Markus; Slepak, Greg; Thorp, Noahy; Wood, Harlan T. *Decentralized Public Key Infrastructure* (December 2015), https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/dpki.pdf
- Askin, Jonathan; Foucek, Chynna; Abualy, Sydney; Furs, Alexei. *Trust in a Trustless System: Decentralized, Digital Identity, Customer Protection, and Global Financial Security* (January 2022), https://law.mit.edu/pub/trustinatrustlesssystem/release/1
- Baya, Vinod. *Digital Identity, Moving to a Decentralized Future*, (October 2019), https://www.citi.com/ventures/perspectives/opinion/digital-identity.html
- Bicacki, Kemal; Crispo, Bruno; Tanenbaum, Andrew. *How to Incorporate Revocation Status Information into the Trust Metrics for Public-Key Certification* (March 2005), https://dl.acm.org/doi/pdf/10.1145/1066677.1067037 (Requires ACM Membership)
- Boneh, Fan. *DeFi Lecture 11: Decentralized Identity* (November 2021), https://www.youtube.com/watch?v=3FL-1HMKvYA
- Chang, Wayne. *Upgradeable Decentralized Identity – DID Method Traits* (July 2022), https://blog.spruceid.com/upgradeable-decentralized-identity/
- Chang, Wayne. *Sign-in with Ethereum* (January 2023), https://www.youtube.com/watch?v=VHwzE6mVm_s
- Collins, Benjamin. *Beyond Blockchain: How Decentralized Identifiers Work* (February 2023), https://medium.com/transmute-techtalk/beyond-blockchain-how-decentralized-identifiers-dids-work-20bb199d038
- Cooper, David A., Computer Security Division, NIST, *A Closer Look at Revocation and Key Compromise in Public Key Infrastructures, https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/paperg2.pdf*
- DIDComm V2 Guidebook (2022), https://didcomm.org/book/v2/didrotation
- DID the Decentralized Identifier, https://decentralized-id.com/web-standards/w3c/wg/did/decentralized-identifier/
- Fdhila, Walid; Stifter, Nicholas; Kostal, Kristian; Saglam, Cihan; Sabadello, Markus. *Methods for Decentralized Identities: Evaluation and Insights*, http://eprints.cs.univie.ac.at/7094/1/2021-1087.pdf

References

- Fernandes, Bruno Miguel Gomes. Self-Sovereign Identity Decentralized Identifiers, Claims and Credentials using non Decentralized Ledger Technology (November 2021), https://repositorium.sdum.uminho.pt/bitstream/1822/82791/1/Bruno%20Miguel%20Gomes%20Fernandes.pdf?utm_source=substack&utm_medium=email
- Genise, Nick; Balenson T., David. *Cryptography Review of W3C Verifiable Credentials Data Model (VCDM) and Decentralized Identifiers (DIDs) Standards and Cryptography Implementation Recommendations* (October 2021), http://www.csl.sri.com/papers/vcdm-did-crypto-recs/crypto-review-and-recs-for-VCDM-and-DIDs-implems-FINAL-20211015.pdf
- Guth-Orlowski, Susanne; Ebert, Johannes; Thiermann, Ricky. *Implementing Digital Product Passports using decentralized identity standards* (April 2023), https://medium.com/@susi.guth/implementing-digital-product-passports-using-decentralized-identity-standards-f1102c452020
- Jacques, Samuel; Lodder, Michael; Montgomery, Hart. *ALLOSAUR: Accumulator with Low-Latency Oblivious Sublinear Anonymous credential Updates with Revocations* (October 2022), https://eprint.iacr.org/2022/1362.pdf
- Brunner, Clemens; Gallersdörfer, Ulrich; Knirsch, Fabian; Engel, Dominik; Matthes, Florian. *DID and VC: Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust* (December 2020), https://dl.acm.org/doi/fullHtml/10.1145/3446983.3446992
- MATTR, *Create a Static Key DID*, https://learn.mattr.global/tutorials/dids/did-key
- Park Chang-Seop; Nam, Hye-Min. *A New Approach to Constructing Decentralized Identifier for Secure and Flexible Key Rotation* (October 2021), https://ieeexplore.ieee.org/abstract/document/9583584
- Pope, Nick; Tabor, Michał; Barreira, Iñigo; Nicholas Dunha; Granc, Franziska; Thiell, Christoph; Fiedler, Arno (ENISA). *Digital Identity: Leveraging the SSI Concept to Build Trust* (January 2022), https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust
- Thorstensson, Joel. *Key Revocation in Self-Certifying Protocols* (April 2022), https://blog.ceramic.network/key-revocation-in-self-certifying-protocols/#:~:text=Key%20revocation%20%2D%20a%20function%20in,the%20new%20key%20becomes%20active

References

- Rocco, Gregory. *Decentralized Identity and Web3* (August 2022), https://blog.spruceid.com/decentralized-identity-and-web3/
- Sabadello, Markus. *The Power of DIDs #2: Creating DIDs* (April 2023), https://www.linkedin.com/posts/danube-tech_the-power-of-dids-2-creating-dids-activity-7051844692723789824-2UjD?utm_source=share&utm_medium=member_desktop
- Smith, Samuel. *Key Event Receipt Infrastructure (KERI): A secure identifier overlay for the inter*net (May 2020), https://www.youtube.com/watch?v=izNZ20XSXR0
- Sporny, Manu. *Verifiable Credentials and DIDs* (September 2022), https://www.youtube.com/watch?v=Nk8Ey0MC528
- W3C Recommendation, *Decentralized Identifiers (DIDs) v1.0, Core architecture, data model, and representations* (July 2022), https://www.w3.org/TR/did-core/
- Weston, Georgia. *Self Sovereign Identity & Decentralized Identity – An Unlimited Guide* (July 2022), https://101blockchains.com/self-sovereign-identity-and-decentralized-identity/
- Windley, Philip. *Digital Identity Design, Deploy, and Manage Identity Architectures* (February 2023), O'Reilly Media