TRUST Over IP

5 Year
Symposium

Is DID SCID the Ultimate DID Method?

Drummond Reed & Markus Sabadello
Co-Chairs, ToIP DID SCID Task Force
November 19, 2025

TRUST Over IP

THE LINUX FOUNDATION

DID SCID Task Force

DID SCID Method Spec

The most secure, flexible, portable, and decentralized DID method

Why is this important?

Because cryptographically verifiable identifiers are the fundamental building blocks of all decentralized trust!

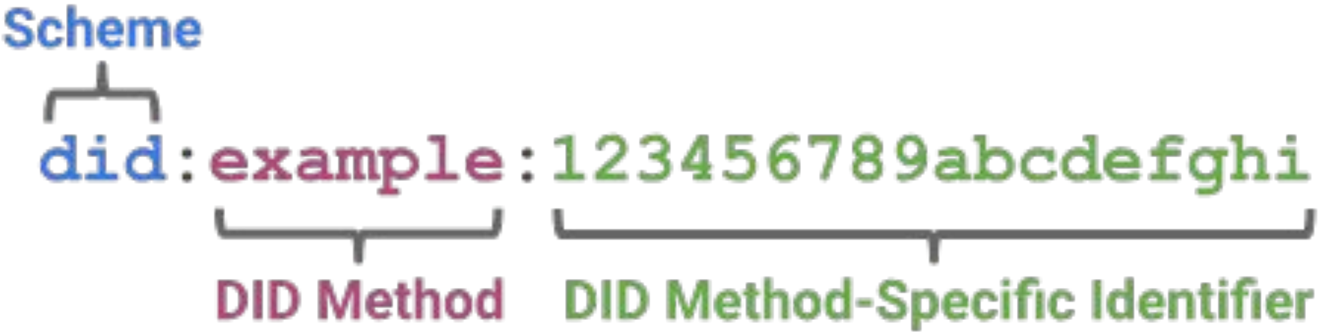
Part One

What is a DID method and why should you care?

The W3C approved W3C Decentralized Identifiers (DIDs) 1.0 on 19 July 2022.

At that time there were over 150 DID methods in the W3C DID registry.

Each DID method defines a way to bind a DID (a globally unique identifier string) to a DID document that contains the bound cryptographic key material and service endpoints.

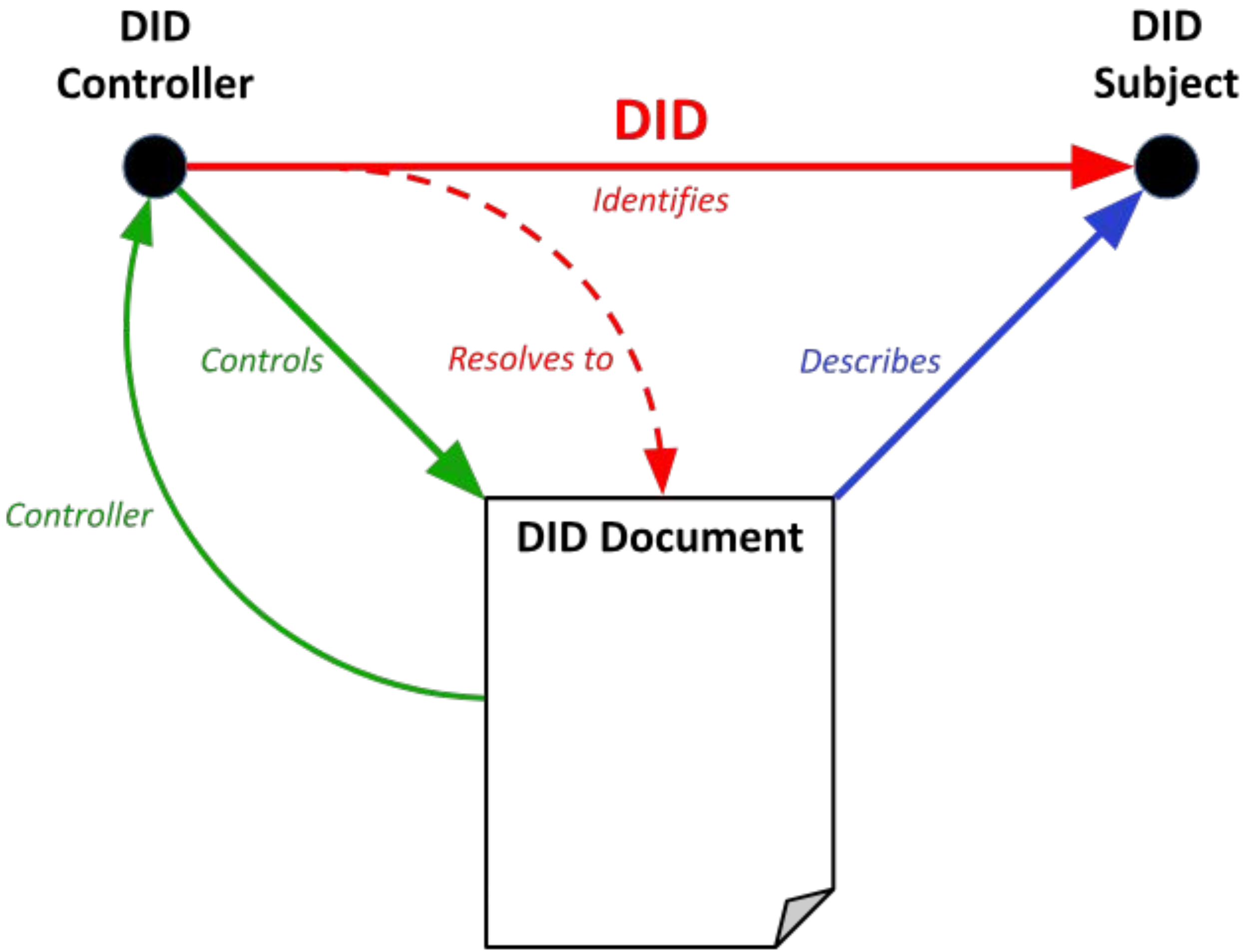


Scheme

did:example:123456789abcdefghi

DID Method

DID Method-Specific Identifier


DID Controller
DID Subject
DID
Identifies
Controls
Resolves to
Describes
Controller
DID Document

Many potential implementers asked:
“Do we really need 150+ ways to do this? Isn’t this a barrier to interoperability?”

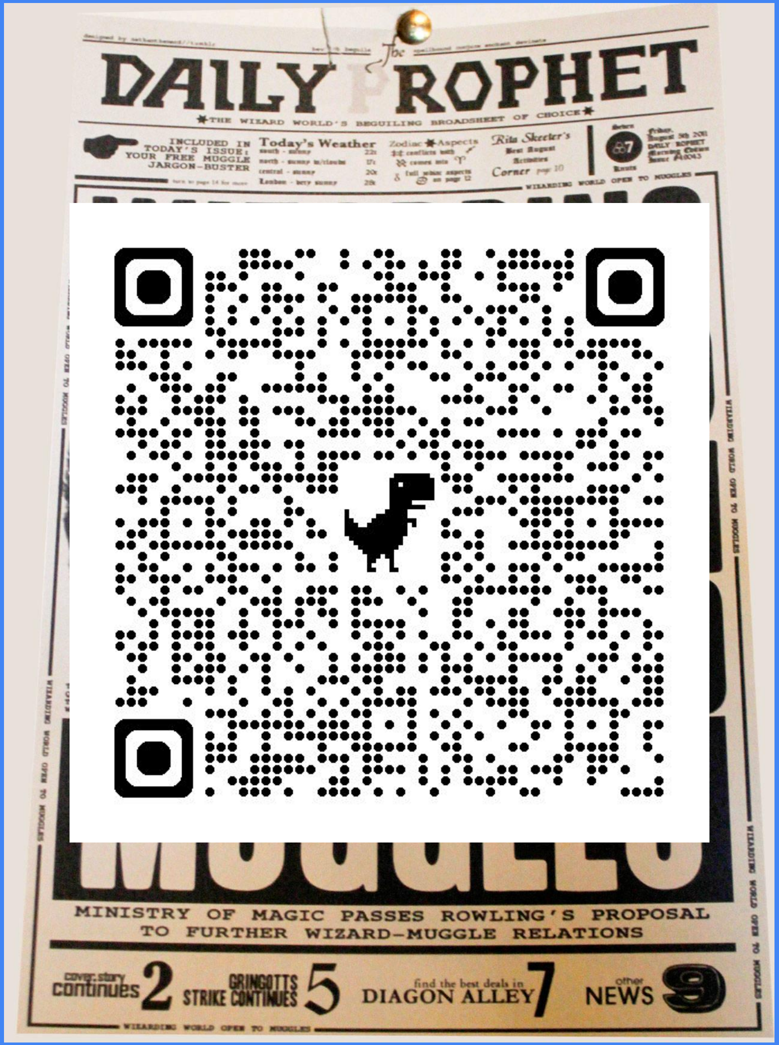
Part Two

What is a self-certifying identifier (SCID) and why should you care?

KERI for Muggles

IIW #33
Day 2 - Session #12
13 October 2021

https://keri.one

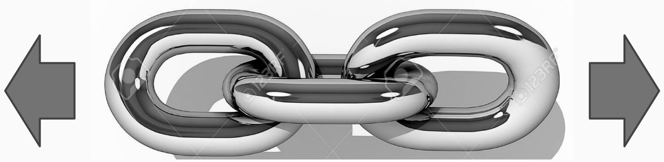

The DAILY PROPHET
THE WIZARD WORLD'S BEGUILING BROADSHEET OF CHOICE
INCLUDED IN TODAY'S ISSUE: YOUR FREE MUGGLE JARGON-BUSTER
Today's Weather
Zodiac Aspects
Rita Skeeter's Best August Activities Corner
WIZARDING WORLD OPEN TO MUGGLES
MUGGLES
MINISTRY OF MAGIC PASSES ROWLING'S PROPOSAL TO FURTHER WIZARD-MUGGLE RELATIONS
cover story continues 2
GRINGOTTS STRIKE CONTINUES 5
find the best deals in DIAGON ALLEY 7
other NEWS 9

#1: Self-Certifying Identifiers

A self-certifying identifier (SCID) is a identifier that can be proven to be the one and only identifier tied to a public key using cryptography alone*

* No blockchain needed

Public key— MUST be shared



Cryptographic binding

Private key— MUST NOT be shared

keri:21tD
AKCERh95u
GgKbJNHYp

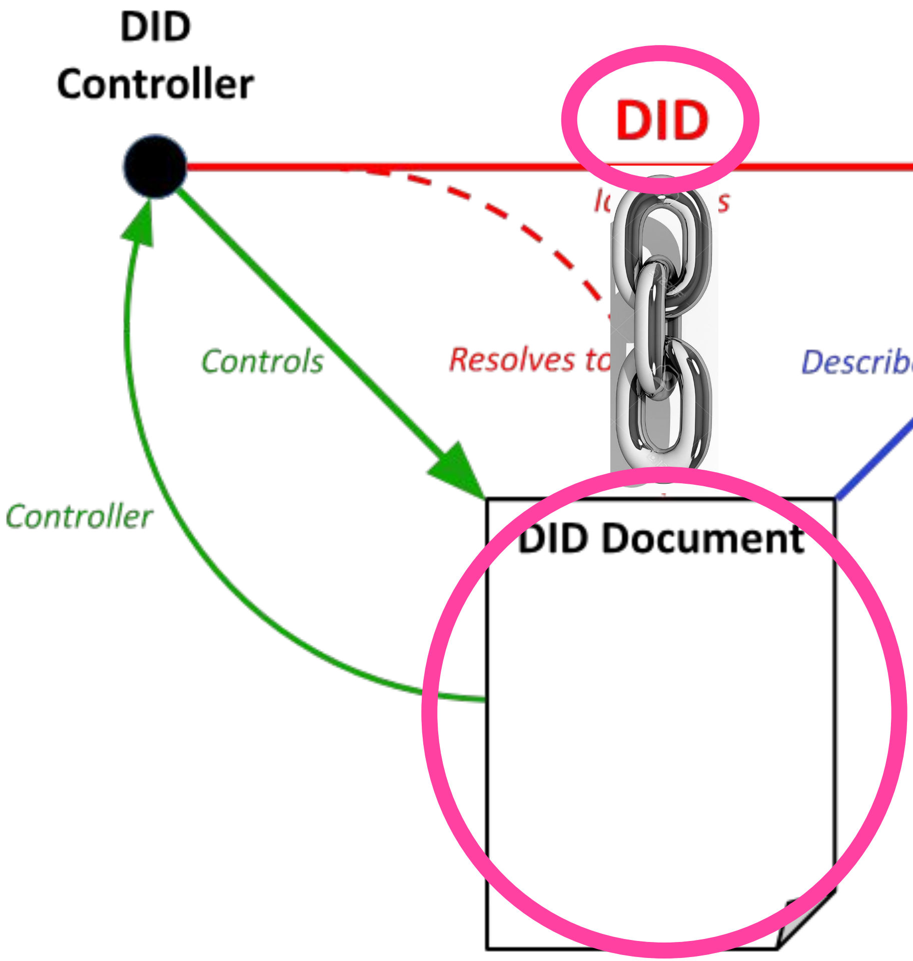
Public key

Cryptographic binding

Self-certifying identifier

Benefit #1

You can prove you control a SCID without needing to rely on ANYONE outside your control (even a blockchain)



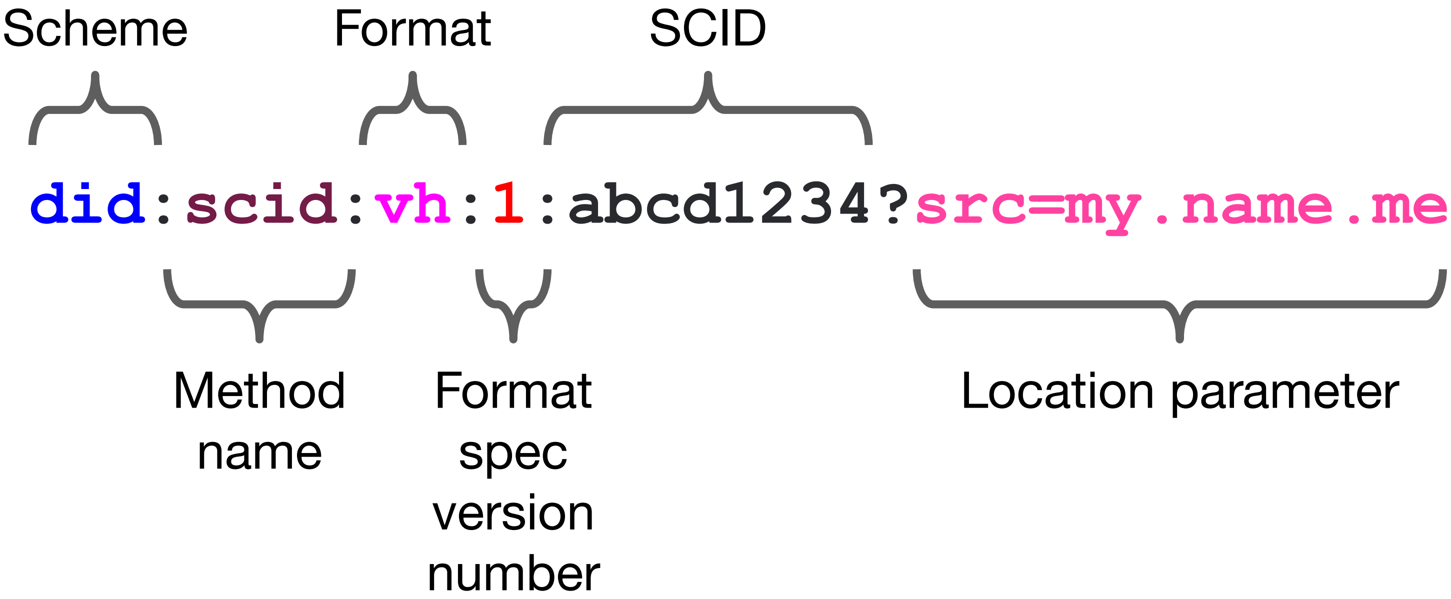
With a SCID, this binding is done **strictly using cryptography**— no external system is needed for verification

After KERI AIDs (autonomic identifiers) showed the way, several more SCID-based DID methods have been developed, including did:webs, id:webvh, did:jlinc, and did:plc.

Part Three

What is the did:scid method and why should you care?

did:scid is essentially a “metamethod” because its goal is to standardize how any SCID-based DID method can become location-independent.



Scheme

Format

SCID

`did:scid:vh:1:abcd1234?src=my.name.me`

Method name

Format spec version number

Location parameter

By separating the location of the verifiable history of DID document(s), did:scid enables the history file to be located anywhere.

These location options include:

1. Peer-to-peer exchange
2. Web servers
3. Blockchains
4. Distributed file systems (e.g., IPFS)

CONCLUSION:

By separating location from the SCID—and by supporting multiple SCID formats—the did:scid method is the most secure, flexible, portable, and decentralized DID method on the market.

TRUST Over IP

THE LINUX FOUNDATION

DID SCID Task Force

TRUST
Over IP