Decentralised IDentifiers and Friends

Vurucu ve Akillica Alt Başlık

Abdulhamit Kumru

Blokzincir Laboratuvarı

2020

Nelerden bahsedecegiz

- SSI and DID
- DID Fundamentals
- DID Auth
- DID Communication

SSI giris slayti

Non est potestas Super Terram quæ Comparetur ei Iob. 41. 24.
LEVIATHAN

SSI dan bahset

ssi nedir, felsefesi kisaca *A survey on essential components of a self-sovereign identity* alinti yap

SSI ilkeleri

ssi ilkelerinden bahset kisaca

- self soverinty surveyini oku
- ssi anlatan figurleri ekle

SSI DID

SSI did iliskisinden bahset did ile baglantisini oradan ekle

DID giris slayti

bilgilendirici resim - ! DID tasaraminda by design olan ozellikler neler

DID Motivasyon

neden boyle birsey lazim, suanki sistemlerin neleri eksik

- binding identifier and keys
- ssi ile ilgisi olmayan avantajlar
    - semantic web

kullandigim sunumlari kaynak olarak goster - DID architectual deep down - kullandigim sunumlar . . .

DID Core Feautres

!!! bu slaytin yerini yeniden degerlendir did gerekliliklerinden bahset, specin sagladigi esneklikten bahset

intro

subtitle boyle kullaniliyor

- !!! primati koy
- !!! asil sunumdan bahset ve referans ver

- What DIDs are
- What DIDs mean
- Why DIDs work
- What DIDs mean

What DIDs are

How DIDs work

Why DIDs work

What DIDs mean

Sovrin

did:sov

Hyperledger Indy

imp of did sov

did auth giris

- web auth ietf rfc lerine degin

DID Auth rwot6

rwot6 DID Auth dan bahset

guncel durum

- did auth grubu calismalari durmus did siop daki degisiklikler sebebiyle
- did authN ???

hali hazirdaki auth protokolleri

!!! bu protokolleri ogren

- The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Scheme
- Self-Issued OpenID Connect Provider DID Profile v0.1 https://identity.foundation/did-siop/
- OAuth
- FIDO
- OpenID Connect
- Kerberos
- LDAP (Active Directory)
- SSO implementations
  - Kerberos Based
  - OAuth Based
  - Security Assertion Markup Language (SAML)
  - Smart-card Based

Auth protokolleri taksonomisi

- !!! taksonomi yap
  - SSO tax doi: 10.1016/j.protcy.2012.05.019
- !!! central decentral, federated, peer ???
- !!! internetten survey bul
- !!! CAS nerede duruyor

Auth protokollerinin kisaca ozetleri, degerlendirme

OpenID Connect

. . .

DID ve DID auth burada nerede duruyor

Halihazirdaki Auth protokolleri ve DID Auth

kisalt . . .

Self-Issued OpenID Connect Provider DID Profile v0.1

This specification defines the “SIOP DID Profile” (SIOP DID) that is a DID AuthN flavor to use OpenID Connect (OIDC) together with the strong decentralization, privacy and security guarantees of Decentralized Identifiers (DID) for everyone who wants to have a generic way to integrate Identity Wallets into their web applications.

- Staying backward compatible with existing OIDC clients and OPs that implement the SIOP specification which is part of the OIDC core specification as per [OIDC.Core] to reach a broader community.
- Adding validation rules for OIDC clients that have DID AuthN support to make full use of DIDs.
- Not relying on any intermediary such as a traditional centralized public or private OP while still being OIDC-compliant.

DID ve DID auth potansiyeli

TLS ten kisaca bahset

tls is de facto standard of todays internet.

Previous Works

DID SSL

Telegram Sam did ssl den bahset

biz ne yaptik

Biz ne yapmaya calistik DID-TLS Indy Auth

indy auth projesinden bahset - motivasyonumuz neydi - hangi toollari frameworkleri kullandik

ne yaptik ne yapamadik

- ne ogrendik
- neyi beceremedik

olursa ne olur olmasi icin ne lazim olmasi ne kadar mantikli

- olmasi icin ne gerekli
- ortada devrim varken kimin gidecegi kimin kalacagi cok belli olmuyor
- ne yapmak istedigimiz iyi anlamak lazim

DIDComm giris slayti

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

- !!! hyperledger aries didcomm peerdid tarihsel surec, kim kimi ortaya cikarmis
- !!! alt basliklari tarihsel akisa gore sirala
- aries rfcleri ietf rfclerine degin ?

DIDComm Design Attemps

- Secure
- Private
- Interoperable
- Transport-agnostic
- Extensible

DIDcomm Building Blocks

- Peer DIDs
- Agents

Peer DIDs

peer did rasyoneli

peer DID method

peer did methodu peer did nedir

- tum didler resolvable olmali dedik fakat globally resolvable demedik :)

peer did ve did comm

peer did methodu peer did nedir - peer did olmadan

Agents

historic agents, indy-aries

. . . .

Hyperledger Aries

- didcommm aries iliskisi, hyperlerdger arieste ortaya cikmis bir fikir
- DID Agents

  tabi bu isleri bizim yerimize birisi yapmasi lazim

DID comm V2

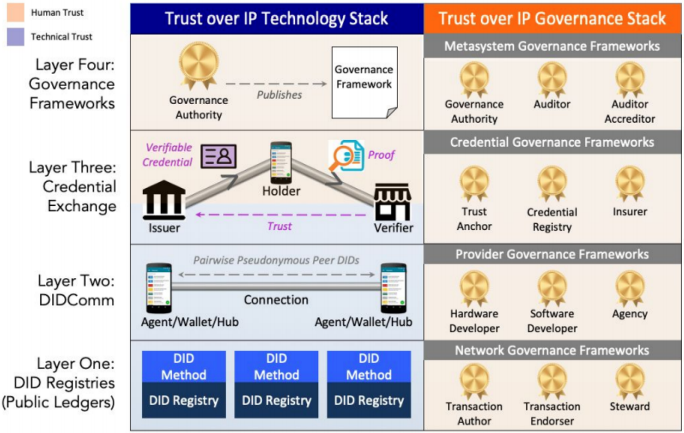
bundan bahsetmeye ne kadar gerek var emin degilim

Changes summary

- Formalization of methods used in V1
  - JWM based envelope
  - ECDH-1PU standardized form of AuthCrypt
- Both DID and key in each message
- Special Handling of Peer DIDs eliminated
- Message structure split between ‘headers’ and body.
- No AnonCrypt encryption method

trust over ip stack

trust over ip stack semasindan didcomm un nerede oldugundan bashet



Hangi Auth Protokolleri yerine kullanilabilir

sikintili ifade . . .

Hangi protokollerle beraber kullanilabilir

- webRTC
  HearRO *A Blockchain Powered Phone System Using Secure Digital Identities To Deliver Better Customer Service*
- SSH (DID Auth ?)
  PAM kullanılarak (kolayca ?) implement edilebilir
- websocket
  websocket over DID comm . . . didcomm over websocket aries rfc lerinde onerilmis
- DID Digital Rights Management (DRM)?
  . . .

DIDComm Messaging

https://identity.foundation/didcomm-messaging/spec/

DIDcomm nerelerde kullanilabilir 2

- webpush ?
  push notifications over DID comm . . .
- webhooks ?
  . . .
- ngok ? (sacma olabilir)
  secure tunnels to localhost with DID comm
- webtorrent, bittorrent ???
  . . .

Sources

- Decentralized Identifiers (DIDs) fundamentals