Decentralised IDentifiers and Friends

Vurucu ve Akillica Alt Başlık

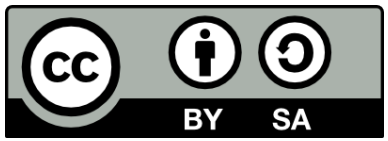
Abdulhamit Kumru

Blokzincir Laboratuvarı

2020

Nelerden bahsedecegiz

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



SSI giris slayti

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

DID Auth rwot6

rwot6 DID Auth dan bahset

Auth protokolleri taksonomisi

!!! taksonomi yap

Auth protokollerinin kisaca ozetleri, degerlendirme

DID ve DID auth burada nerede duruyor

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

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

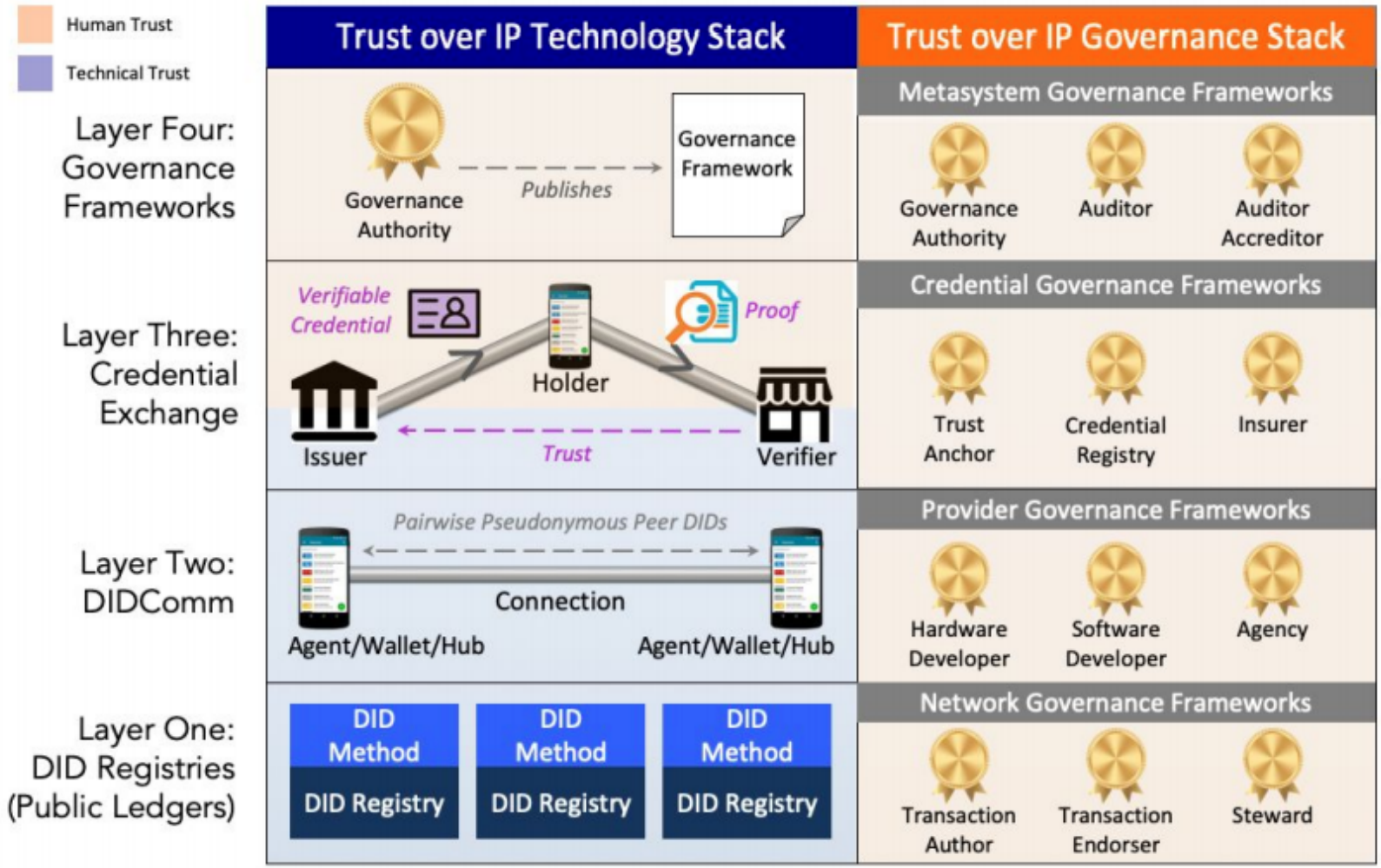
bundan bahsetmeye ne kadar gerek var emin degilim

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