ARCADIAN-IoT

ARCADIAN-IOT TRAINING

DECENTRALIZED IDENTIFIERS

Ross Little (EVIDEN - ATOS)

15/09/2023

AGENDA

1. Introduction to Decentralized Identifiers (DIDs) and their use
2. DIDs employed in ARCADIAN-IoT
   a. DID:WEB
   b. DID:PEER
   c. DID:PRIV
3. Summary of DIDs used in ARCADIAN-IoT & their Suitability

1. INTRODUCTION TO DECENTRALIZED IDENTIFIERS (DIDS) AND THEIR USE

WHAT ARE DECENTRALIZED IDENTIFIERS (DIDS)

ARCADIAN-IoT

A new type of globally unique identifier that enables a verifiable decentralized digital identity.

- A DID refers to any subject (e.g., a person, organization, thing)
- DIDs make use of cryptographic key pairs for authentication and verification.
- Public keys are associated with DIDs, allowing for secure and verifiable interactions without relying on a central certificate authority.
- No central registry stores all DIDs and associated data. Public DIDs are often, but not always, stored on a decentralized network or blockchain.
- A DID enables the subject to prove control over their identifier by proving that they are the holder of the private key used for verification.
- A DID supports a variety of use cases, such as self-sovereign identity, verifiable credentials, secure communication, and even data sovereignty.

DID AND DID DOCUMENT (DOC) SPECIFICATION

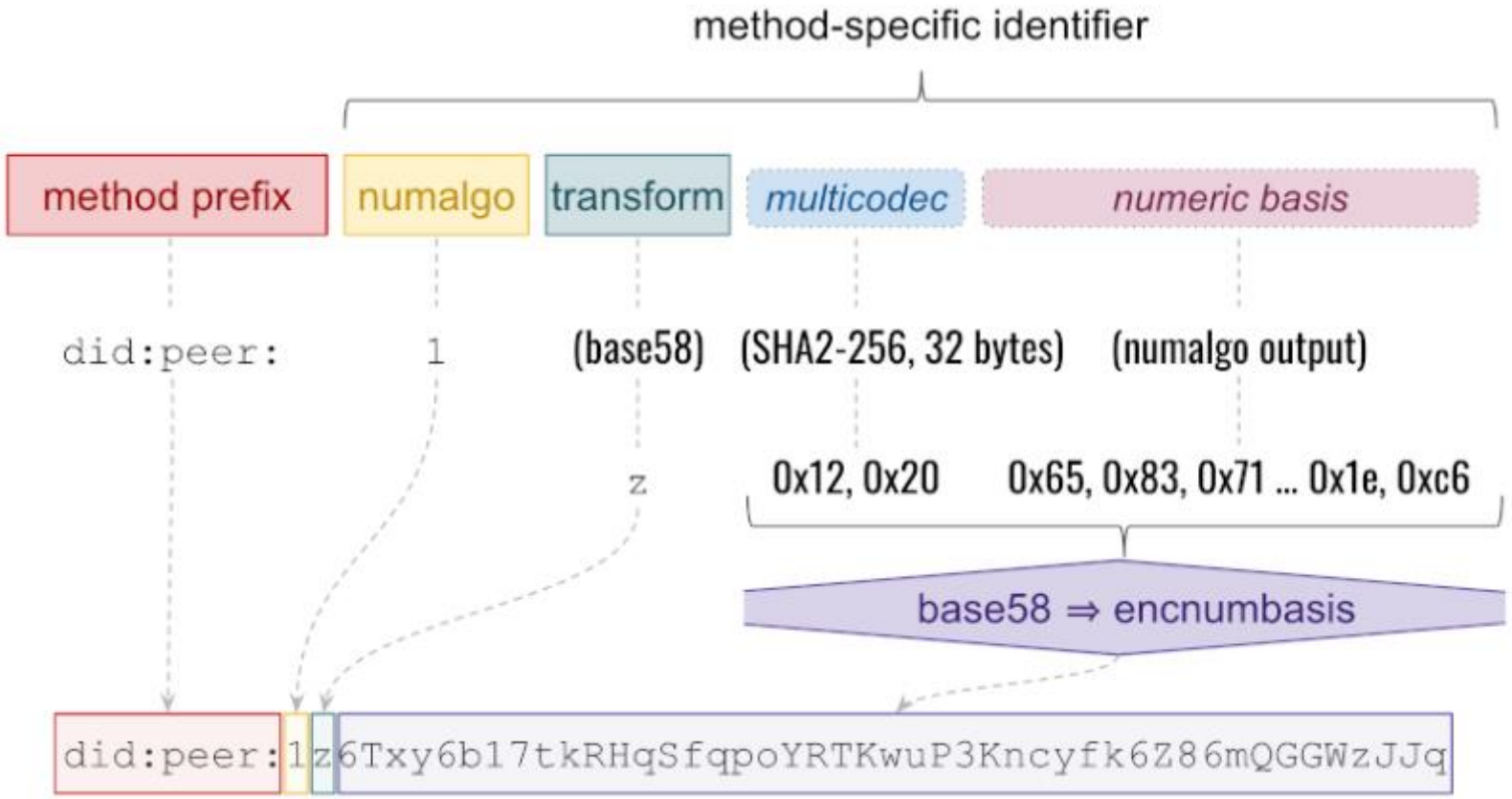
EXAMPLE 1: A simple DID document

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

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

2. DIDS EMPLOYED IN ARCADIAN-IOT

DID:PEER METHOD



Ref: Peer DID Method Specification (identity.foundation)

DID:PEER (NUMALGO 0) – NO DID DOC

ARCADIAN-IoT

- A did:peer:0 method is the same as did:key in that the numeric basis is the base58 encoded public signing key and its multibase-encoded multicodec value to identify the signature algorithm used for verifying digital signatures. Example:

did:key:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH
did:peer:0z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH

Decode Base58

ed0194966b7c08e405775f8de6cc1c4508f6eb227403e1025b2c8ad2d7477398c5b2

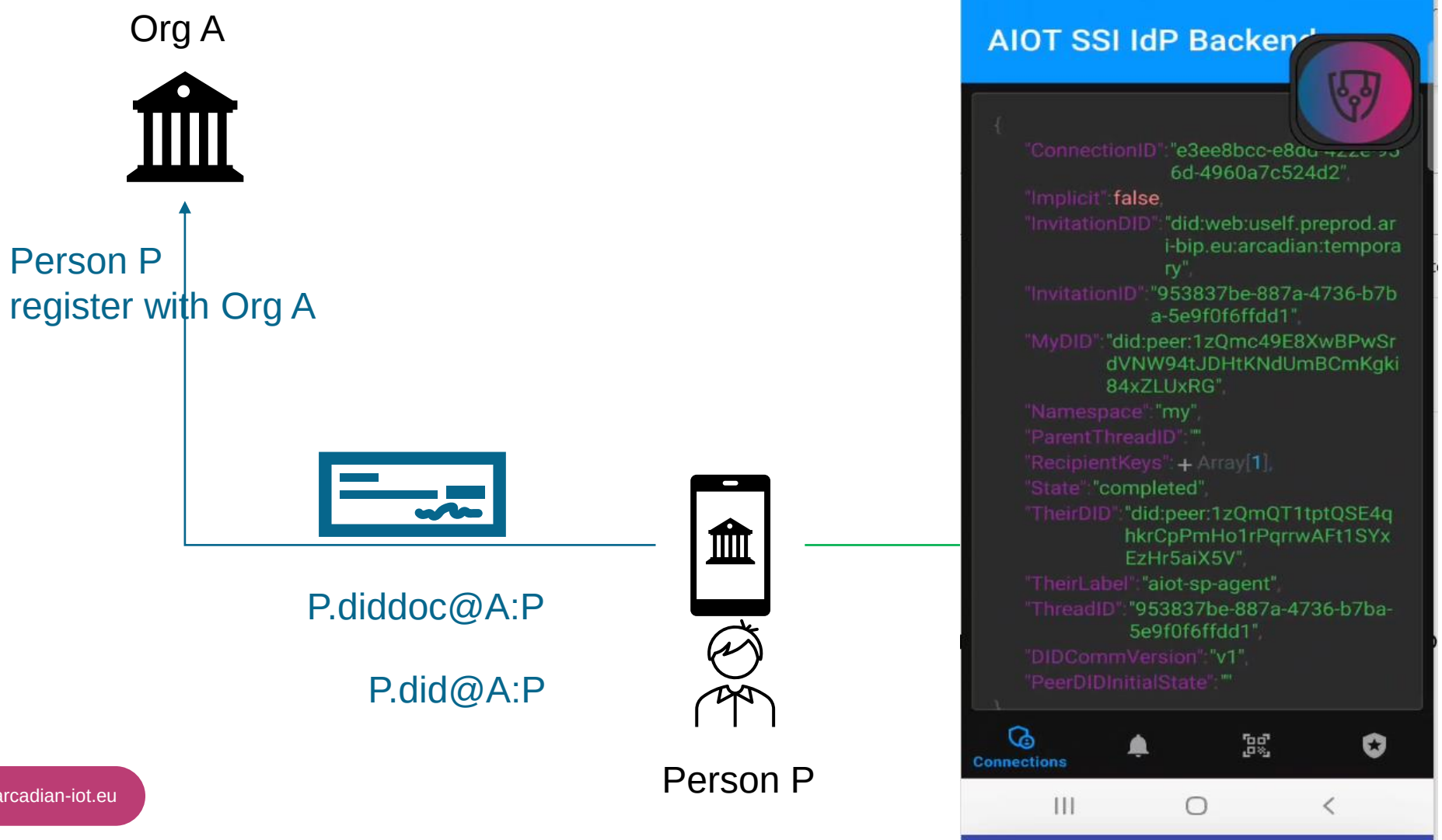
Multicodec hexadecimal value	public key byte length	Description
0xe7	33 bytes	secp256k1-pub - Secp256k1 public key (compressed)
0xec	32 bytes	x25519-pub - Curve25519 public key
0xed	32 bytes	ed25519-pub - Ed25519 public key
0x1200	33 bytes	p256-pub - P-256 public key (compressed)
0x1201	49 bytes	p384-pub - P-384 public key (compressed)
0x1202	?? bytes	p521-pub - P-521 public key (compressed)
0x1205	?? bytes	rsa-pub - RSA public key. DER-encoded ASN.1 type RSAPublicKey according to IETF RFC 8017 (PKCS #1)

DID:PEER (NUMALGO 1) – DID DOC SHARED (WITHOUT DID INSIDE)

ARCADIAN-IoT

- A did:peer:1 method creates a locally stored DID doc that contains the public key, used for verification of the DID Doc or any credentials sent by the entity.
- The shared DID Doc does not contain the actual DID value instead just an “id” variable.
- The numeric basis of the DID is the SHA256 hash of the bytes of the DID doc, so that the receiver can verify the DID Doc integrity.
- New key pairs are generated with corresponding DID Docs created for sharing with different parties, so to avoid tracking of persons' across different services.

DID:PEER (NUMALGO 1) – DID DOC SHARED WITHOUT DID



DID:WEB METHOD

ARCADIAN-IoT

- DIDs that target a distributed ledger face significant challenges in establishing trust around identities to incentivize mass adoption.
- The DID web method uses a web domain's existing reputation so does not have this challenge.
- Globally unique public identifiers for use by organizations and things.
- Resolves to a well known endpoint hosted by the organization´s domain.
- Makes use of existing web standards.
- However, availability of the DID depends on the resilience and security of the domain.

DID:WEB METHOD

ARCADIAN-IoT

did:web:eviden.com

Resolves to

https://eviden.com/.well-known/did.json

did:web:iotgw.eviden.com:dev:scbvancy28okf9s

Resolves to

https://iotgw.eviden/dev/scbvancy28okf9s/did.json

Note: DID Doc, may reside on the IoT GW for constrained devices or act as a proxy to the actual IoT Device.

Ref: https://w3c-ccg.github.io/did-method-web/

DID:WEB ARCADIAN-IOT DEMO

1. Create DID

2. Resolve: did:web:aiot-ssi-backend.preprod.ari-bip.eu:jp3Ysz1zrZFYUmZ69zaW3v4QcwzbURgSymfeuSGAgtWCLFdAY

https://aiot-ssi-backend.preprod.ari-bip.eu/jp3Ysz1zrZFYUmZ69zaW3v4QcwzbURgSymfeuSGAgtWCLFdAY/did.json

DID:PRIV METHOD

ARCADIAN-IoT

- This is a private did method that is only resolvable inside the ecosystem of the organizations that are making use of it, as it resides in a permissioned blockchain.
- We provide a decentralized blockchain network for creating DIDs storing DID Docs for all participating organizations that have access to the network.
- Any participating organization given access to the network can create a did:priv.
- To update/delete a DID Doc, the organization that created the DID is in the blockchain´s public state and only that organization will be allowed to do this.
- DID Docs are stored off-chain in Private Data Collections with only the hash stored on-chain to make it more privacy preserving.

DID:PRIV DEMO

1. Create DID

```
WW930+A182805@LAPTOP-4OPFAIDD MINGW64 ~
$ curl -X POST -H "Content-Type: application/json" -d '{"didDoc": {"@context": "https://www.w3.org/ns/did/v1", "id": "did:priv:jtw5KQhnWaoiDqMtJuXvtjnxdng1LAH5c8eUcifmX6eUnfJxg"
, "publicKey": [{"id": "did:priv:jtw5KQhnWaoiDqMtJuXvtjnxdng1LAH5c8eUcifmX6eUnfJxg#keys-1", "type": "Ed25519VerificationKey2018", "controller": "did:priv:jtw5KQhnWaoiDqMtJuXvtjn
xdng1LAH5c8eUcifmX6eUnfJxg", "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"}]}}' https://vdrfabric.dev4.ari-bip.eu/store
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   493  100    96  100   397    328   1360 --:--:-- --:--:-- --:--:--  1694{"result":"","transactionID":"6906c61bdda8ad3e2118685954b7d7cdc39c26706128005377acaa6f9bfea8c8"}
```

2. Resolve did:web

```
WW930+A182805@LAPTOP-4OPFAIDD MINGW64 ~
$ curl -X GET "https://vdrfabric.dev4.ari-bip.eu/qu
  % Total    % Received % Xferd  Average Speed   Ti
                                 Dload  Upload   To
100   384  100   384    0     0   1473      0 --:--
ifmX6eUnfJxg","id":"did:priv:jtw5KQhnWaoiDqMtJuXvtj
```


```
{
   "@context":"https://www.w3.org/ns/did/v1",
   "id":"did:priv:jtw5KQhnWaoiDqMtJuXvtjnxdng1LAH5c8eUcifmX6eUnfJxg",
   "publicKey":[
      {
         "controller":"did:priv:jtw5KQhnWaoiDqMtJuXvtjnxdng1LAH5c8eUcifmX6eUnfJxg",
         "id":"did:priv:jtw5KQhnWaoiDqMtJuXvtjnxdng1LAH5c8eUcifmX6eUnfJxg#keys-1",
         "publicKeyBase58":"H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV",
         "type":"Ed25519VerificationKey2018"
      }
   ]
}
```


```
5KQhnWaoiDqMtJuXvtjnxdng1LAH5c8eUc
```

3. SUMMARY OF DIDS USED IN ARCADIAN-IOT & THEIR SUITABILITY

SUMMARY OF DIDS USED IN ARCADIAN-IOT & THEIR SUITABILITY

ARCADIAN-IoT

- did:peer is suitable for persons in SSI wallets:
  - Pairwise did:peer is privacy preserving with DIDs created per party that it is being shared with and have no meaning/use outside that relationship.
  - did:peer has no endpoint and its did doc is communicated directly between the different parties with no ledger or verifiable data registry needed.
  - Only integrated with DIDCOMM protocol specified by Decentralized Identity Foundation
- did:web is suitable for organisations that use the reputation of their own domain to fully host and manage their own DIDs for its organization and things.
- did:priv is suitable for organisations and their things where a permissioned ledger is setup to provide for the creation and hosting of did docs. This provides the DLT technology benefits of availability and security.

ARCADIAN-IoT

THANK YOU FOR YOUR ATTENTION

arcadian-iot.eu

ARCADIAN-IoT project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101020259

THIS PROJECT IS PART OF THE NEXT GENERATION IoT

www.ngiot.eu