SOFIE: DIDs & VCs

Dr. Dmitrij Lagutin, Aalto University

Dr. Nikos Fotiou, Athens University of Economics and Business

Dr. Yki Kortesniemi, Aalto University

22.3.2021

EU H2020 SOFIE Project 2018-2020

- Fragmentation is a major issue in IoT
  - Most of IoT systems are closed silos => difficult to exchange data, actions, etc. across IoT systems
  - Leads to high barriers of entry and reduces competition, worse privacy, etc.
- SOFIE provides secure open federation for existing (open and closed) IoT platforms through Distributed Ledger Technologies (DLTs)
  - Without requiring any changes to the existing IoT systems
  - Four pilots in three different areas: energy, supply chain, mixed reality gaming
- DIDs and VCs have been extensively used in SOFIE for identity management

Contents

- DIDs and VCs on (constrained) IoT devices
- Access control for WoT using VCs
- did:self method
- Enhancing privacy with ephemeral DIDs and ring signatures

DIDs and VCs on (constrained) IoT devices

Dmitrij Lagutin

Identifiers for Internet of Things

- IoT devices are becoming widespread in critical systems => secure identifiers for IoT are needed
  - Many IoT devices are also personal (e.g. heart beat monitors), therefore privacy is also important
- Identifiers and Credentials for IoT should support:
  - Self-sovereignty
  - No global root of trust needed
  - Strong cryptography for end-to-end protection (encryption, signatures)
  - Mutual authentication between the device and user
- DIDs and VCs are natural solutions for IoT devices to improve their security and privacy

Identifiers for constrained IoT devices

- Public key cryptography (such as ECC) used by DIDs and VCs is already feasible on a low cost modern IoT devices[1]
  - 8-bit microcontrollers can perform 1-2 ECC operations per second
  - Cheap (<0,50$) 32-bit Cortex-M0 can perform up to 13 ECC operations per second
- However, not all IoT devices can use public-key cryptography
  - Extremely constrained devices using older hardware
  - Lack of entropy or secure key storage
  - No software support and lack of upgrades

1 Yki Kortesniemi, Dmitrij Lagutin, Tommi Elo, and Nikos Fotiou. Improving the Privacy of Internet of Things with Decentralised Identifiers (DIDs). Journal of Computer Networks and Communications. 2019. https://doi.org/10.1155/2019/8706760

Identifiers for constrained IoT devices

- If IoT device is not able to process DIDs and VCs natively, a proxy based approach can be used
- A proxy acts as an end point for DID/VC-based communication and for communication with the actual IoT device the proxy can use other means, such as symmetric cryptography
- OAuth2 is a popular authorisation protocol
  - OAuth2 Authorisation Server (AS) enforces the authorisation policies, and can acts as proxy for DIDs/VCs

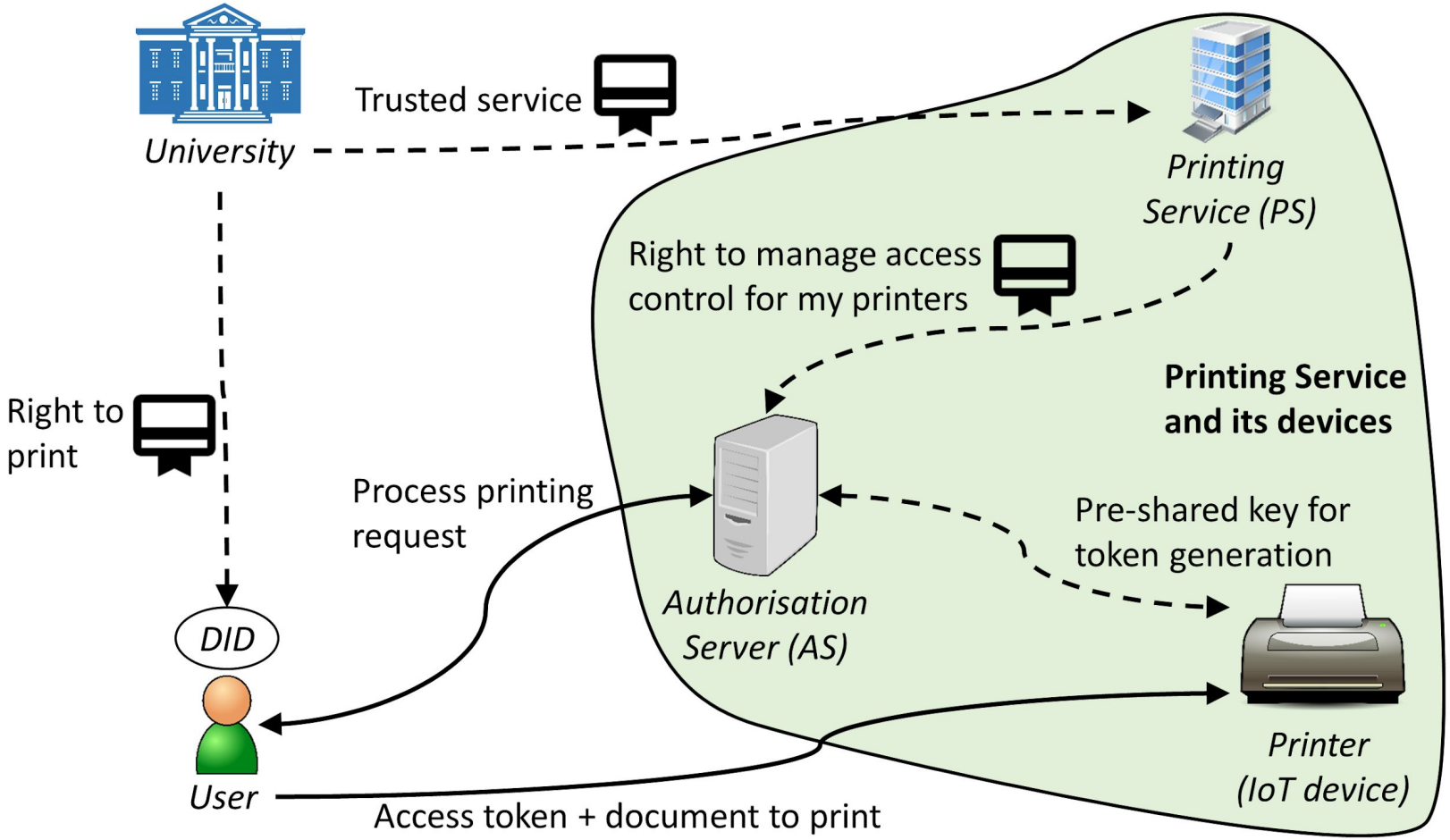
Identifiers for constrained IoT devices: Example[2]

- Visiting Lecturer wants to use University's printer (IoT device)
  - Lecturer does not have University's user account
- Printing Service is managed by third party which is compensated by University
- Goals:
  - Secure mutual authentication between user and the IoT device
  - Printing Service should not able to identify user or correlate its activities
  - Compatibility with legacy devices which do not support public key cryptography

2 Dmitrij Lagutin, Yki Kortesniemi, Nikos Fotiou, and Vasilios Siris. Enabling Decentralised Identifiers and Verifiable Credentials for Constrained IoT Devices using OAuth-based Delegation. Workshop on "Decentralized IoT Security and Standards" (DISS). San Diego, USA, 2019. https://dx.doi.org/10.14722/diss.2019.23005

Identifiers for constrained IoT devices: Example

- User (Lecturer) uses DID
- University, Printing Service, and its Authorisation Server (AS) use VCs
- User receives ACE-OAuth2 compatible access token from AS for communication with printer



Identifiers for constrained IoT devices: Conclusions

- DIDs and VCs are natural choices for offering good security and privacy for IoT devices
- Public key cryptography is feasible on constrained IoT devices
  - In some cases, a proxy-based approach is needed
- Potential use cases:
  - Secure device sharing in a broader sense
  - Providing access to third parties in privacy preserving way, e.g. technician working for another company
  - => Allows more flexible, open federation between different organisations

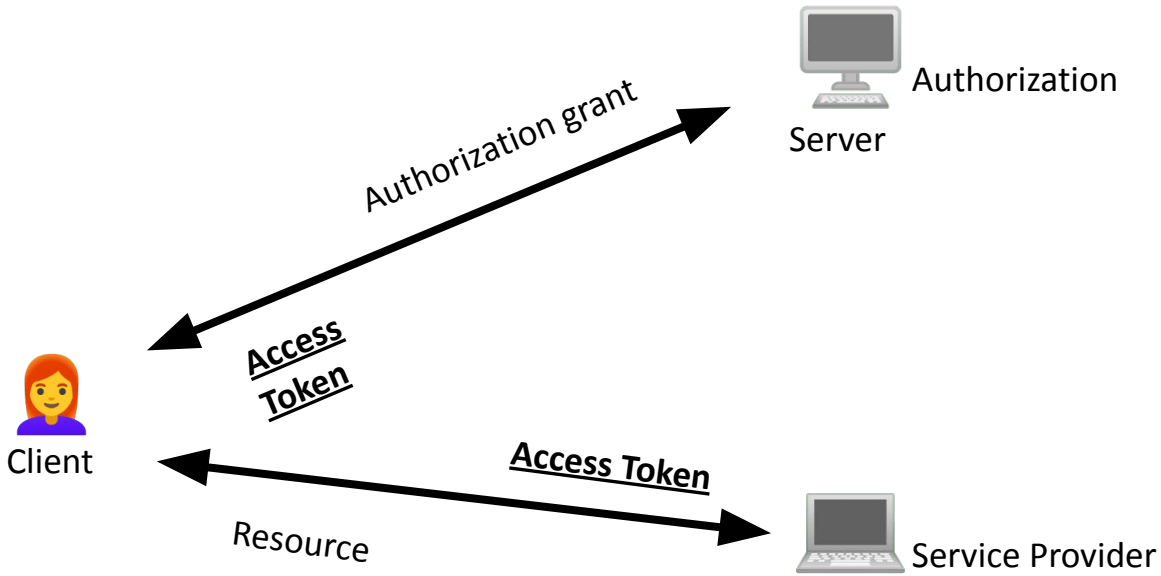
Access control for WoT using VCs

Nikos Fotiou

Our goal

- Efficient access control for systems that involve multiple users belonging to different organizations
- Desired properties:
  - Self-sovereignty
  - User privacy protection
  - Increased flexibility and scalability
  - Integration with existing standards
- Our approach:
  - Use *Verifiable credentials* as *access tokens*

Reference architecture



Access control: JWT Vs. VC

JWT

```
{
"sub": "aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
"aud": "xxxxxxxxxxxxexample",
"email_verified": true,
"token_use": "id",
"auth_time": 1500009400,
"iss": "https://cognito-idp.us-east-1.amazonaws.
"cognito:username": "janedoe",
"exp": 1500013000,
"given_name": "Jane",
"iat": 1500009400,
"email": "janedoe@example.com"
}
```

W3C VC

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://example.edu/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "https://example.edu/issuers/14",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "proof": { ... }
}
```

VC features

Machine readable description of the credential

It can be used as a “proof of possession”

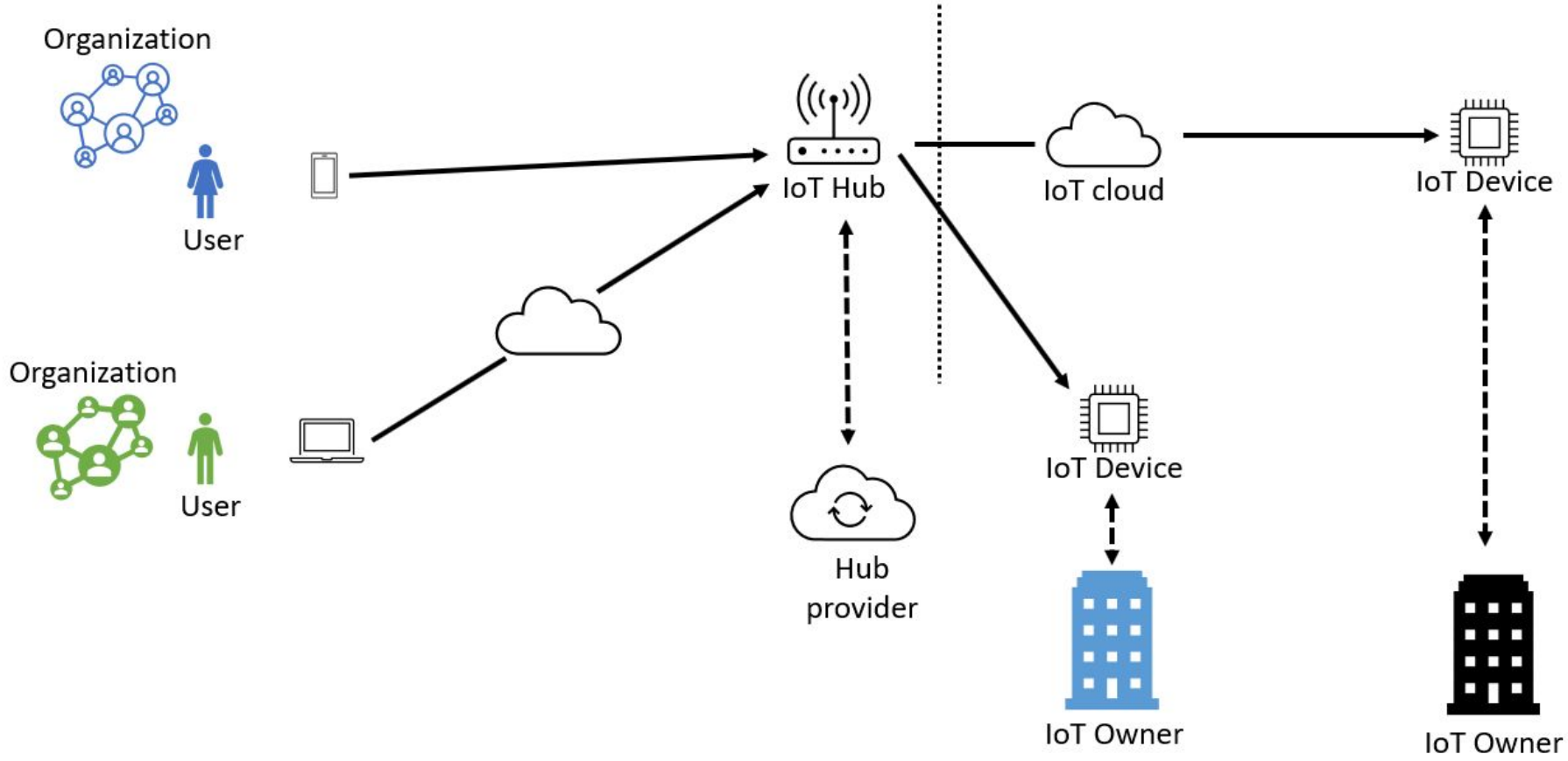
It can be generated using ZKP

Revocation, Multiple encodings, Business opportunities...

W3C VC

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://example.edu/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "https://example.edu/issuers/14",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "proof": { ... }
}
```

An “enterprise-IoT” use case



Hub WoT Thing Description

```
{
   "@context": ["https://www.w3.org/2019/wot/td/v1"],
   "id": "lamp1",
   "title'': "Main entrance light''
   "properties": {
      "status": {
         "forms": ["href": "https://sofie-iot.eu/hubA/lamp1/status"]
      }
   },
   "actions": {
      "toggle": {
         "forms": ["href": "https://sofie-iot.eu/hubA/lamp1/toggle"]
      }
   },
   "events": {...}
}
```

The “SOFIE credential”

```
{
 "@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://mm.aueb.gr/contexts/access_control/v1"
 ],
 "id": "https://www.sofie-iot.eu/credentials/examples/1",
 "type": [ "VerifiableCredential", "AllowedURLs"],
 "issuer": "did:nacl:qhfcPPDch__JN3m5fuMoSkZi_QHMi3N99HRj_Wtv_hE",
 "issuanceDate": "2010-01-01T19:23:24Z",
 "credentialSubject": {
          "id": "did:nacl:XvCUDs8CFCo5VPjLUsNA0BJHW_QlOrCyYuuALN9oHiA",
          "acl": [
               {
                "url": "https://sofie-iot.eu/hubA/lamp1/toggle",
                "methods": [ "POST"]
               },
               {
                "url": "https://sofie-iot.eu/hubA/lamp1/status",
                "methods": ["GET" ]
               }
      ]
  },
 "proof": {}
}
```

The issuer

Only this user can use this credential

Hub WoT Thing Description with VC-based AC

```
{
  "@context": ["https://www.w3.org/2019/wot/td/v1","https://mm.aueb.gr/contexts/access_control/v1"],
  "securityDefinitions": {
        "auth_toggle": {
          "@type":["VerifiableCredential","AllowedURLs"],
          "context": "https://mm.aueb.gr/contexts/access_control/v1",
          "issuer": "did:nacl:qhfcPPDch__JN3m5fuMoSkZi_QHMi3N99HRj_Wtv_hE",
          "filter":["$.credentialSubject.acl[?(@.url='https://sofie-iot.eu/hubA/lamp1/toggle')]"]
        }
  }
  "id": "lamp1",
  "title'': "Main entrance light''
  "properties": {
    "status": {
      "forms": [{
        "href": "https://sofie-iot.eu/hubA/lamp1/toggle",
        "security":"auth_toggle"
      }]
    }
  }
  ...
```

JSON-Path

VC-based AC enforcement

- A transparent HTTP proxy, located before the hub, parses the WoT TD file and applies AC rules(*)
- Benefits:
  - Each organization can freely decide which uses can access each IoT device.
  - (Dis)Allowing a user to access an IoT device does not involve any communication with the hub.
  - The hub does not have access to the user management system of the organizations
  - The hub does not have to “understand” the business logic of each organization.

* https://github.com/SOFIE-project/identity-authentication-authorization

did:self method

Nikos Fotiou

Self-sovereignty Vs. Flexibility

(1) https://w3c-ccg.github.io/did-method-key/

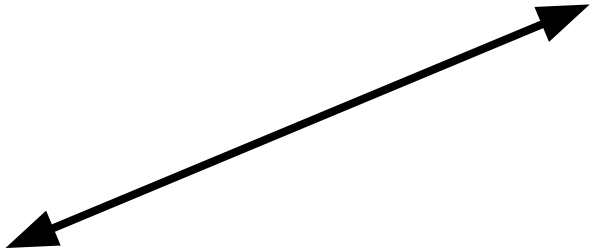
(2) https://sovrin-foundation.github.io/sovrin/spec/did-method-spec-template.html

Self-sovereignty Vs. Flexibility

did:key — did:sov

```
did:key:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH
```

DID registry



```
{
  "id": "did:sov:mnjkl98uipsndg2hdjdjuf7",
  "publicKey": [{
      "id": "key1"
      "type": "ED25519SignatureVerification",
      "publicKeyBase58": "...",
      "authorizations": ["all"]
    }],
  "authentication": [{
      "type": "ED25519SigningAuthentication",
      "publicKey": "key1"
    }],
  "service": [{
      "type": "agentService",
      "serviceEndpoint":"https://www.sovrin.org/agents"
    }]
}
```

Self-sovereignty Vs. Flexibility

(*) https://github.com/mmlab-aueb/did-self

did:self

- DIDs are public keys
- The corresponding private key is used for signing a DID document

```
{
 "id"="did:self:PubkeyA"
  "authentication"=[
        "publicKeyJWK"= {
             PubKeyC
        }
   ]
}
```

id	did:self:PubkeyA
SHA-256	<hash1>
Signed by	did:self:PubkeyA

Benefits

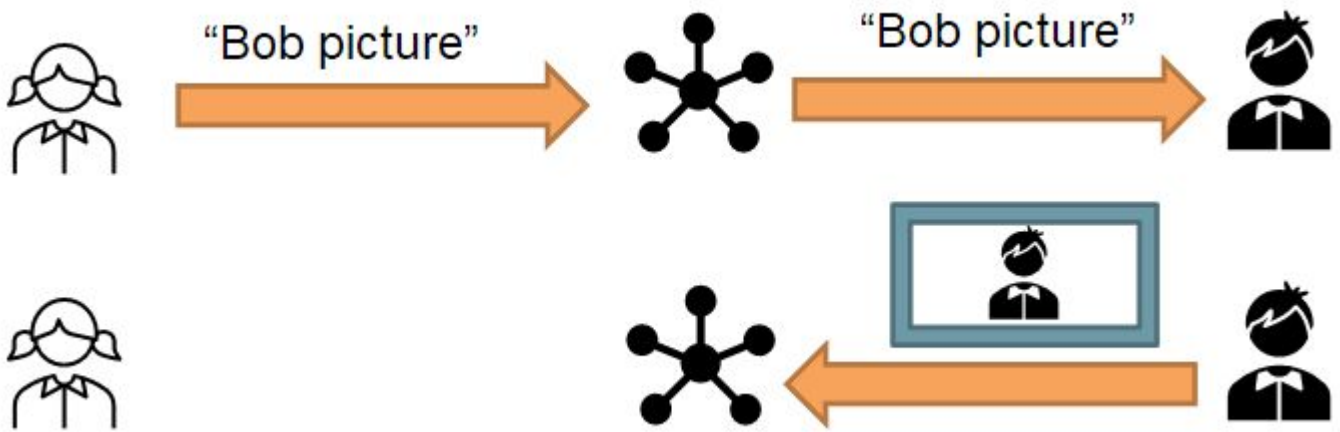
- No need for a registry that manages DID document →DID owners disseminate the document by themselves.
- DID owners can rotate their keys.
- DID owners can (temporarily) delegate their DID or access rights related to their DID (e.g., authorize another user to generate digital signatures on their behalf).
- Mechanisms for recovering from identity theft.

Use cases

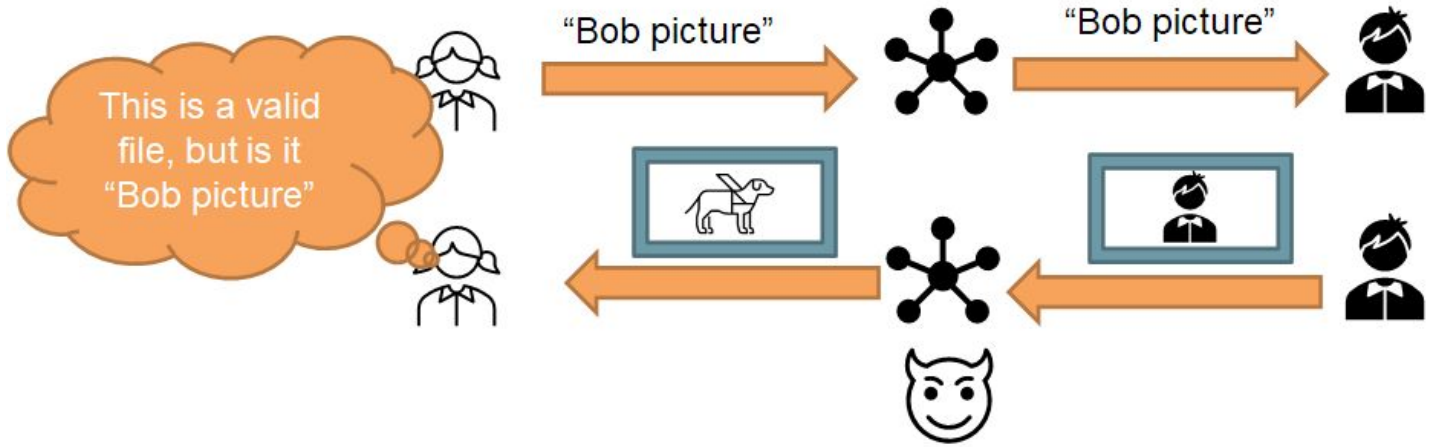
- OAuth 2.0 PoP access tokens without user tracking
  - Legacy PoP token even if they are updated regularly they contain the user key ➡️user tracking
- Secure and private delegation of verifiable credentials
  - Create a temporary key-pair for you travel laptop and use this key-pair to prove possession of a VC
- Self-certified content identifiers

  ➡️https://mm.aueb.gr/scn4ndn/

Content Authenticity: A Big Challenge



Content Authenticity: A Big Challenge



Enhancing Privacy with Ephemeral DIDs and Ring Signatures

Yki Kortesniemi

Antonio Antonino, Shamim Biswas, Yki Kortesniemi, Dmitrij Lagutin. *Improving Privacy with Ring Signatures and Ephemeral Decentralized Identifiers*. Submitted manuscript

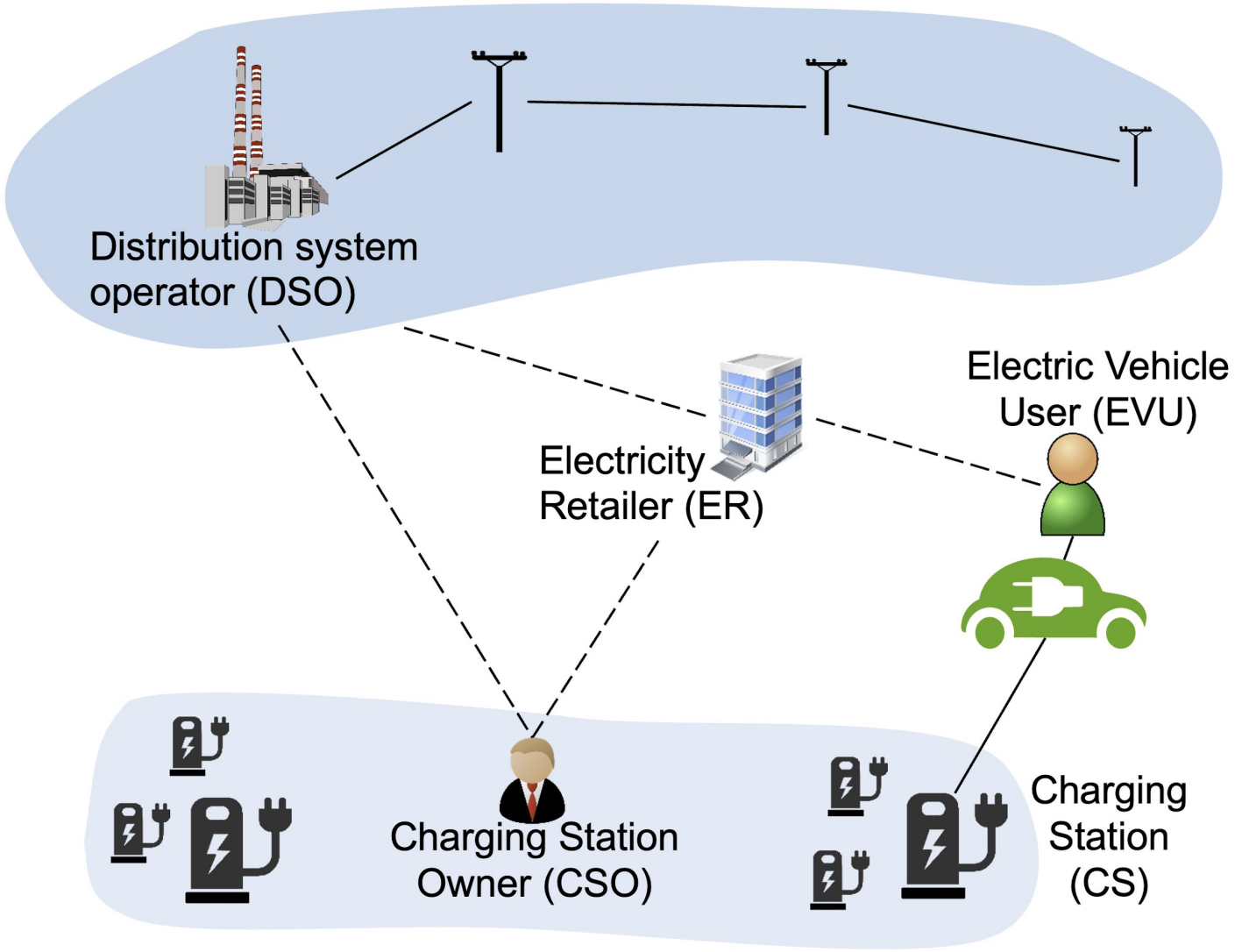
The problem of long-lived identifiers

- Long-lived identifiers enable tracking
  - if they are globally unique (as DIDs are...), it's even easier
- We can mitigate by using a different DID for each service
  - and change DIDs from time to time
- Still, using the same DID multiple times allows correlating those uses
  - data analysis can reveal further information and enable predictions

⇒ How can this be avoided?

Use Case: Electric Vehicle Charging

- Electric Vehicle Users (EVUs) buy the electricity for their cars from an Electricity Retailer (ER)
  - the charging can take place at any of the compatible Charging Stations (CSs)
- The price of electricity varies depending on the time and location of charging
  - timing and locating the charging suitably helps balance the electrical grid so the grid operator (DSO) pays the ER for this balancing
- ER incentivises the EVUs to participate


Distribution system operator (DSO)
Electricity Retailer (ER)
Electric Vehicle User (EVU)
Charging Station Owner (CSO)
Charging Station (CS)

Assumptions & Requirements

- All parties use DIDs
  - ER knows EVU's identity and CSO knows CS's identity in all cases
- Separate VC for each DID
  - EVU uses a VC from ER to prove the right to charge at the CS
  - CS uses a VC from CSO to prove it's district
- For the charging transaction to qualify for the incentive, it has to contain information about time and location (on a district level)
- However, transaction must NOT reveal
  - the exact location (i.e. the CSs identity)
  - EVUs identity to the CS
- If EVU or CS use just long-lived DIDs, we cannot meet the requirement

2 Approaches: Ephemeral DIDs and ring signatures

- ephemeral (single-use) DIDs
  - each DID is used for just one charging transaction
- ring signatures
  - ring is a group of DIDs; each signature done by one of the ring members looks like it could have been done by any of them
  - By making a ring of all CSs in a district, CSs can use long-lived DIDs with ring signatures

Test scenarios

- Comparing 3 scenarios
  - all parties use long-lived DIDs (baseline)
  - EVUs and CSs use ephemeral DIDs
  - EVUs use ephemeral DIDs and CSs use ring signatures
- Use Norway as bases for assumptions:
  - 356 districts
  - 50 CSs per district
  - 5 transactions per CS per day
- Evaluate
  - how much is privacy improved?
  - how is resource consumption affected?

Results: Ring signatures

- computational complexity and size of a ring signature grows as a function of the ring size
  - though suitable for this use case, this limits the suitability for case requiring large rings

Ring size	1	10	100	1 000	10 000
Signing[1] (ms)	0,4	6,4	67	670	7 100
Signature size (bytes)	64	352	3,2K	32K	320K

[1] Prototype was running on a modern mobile phone

Results: charging transaction

- The time to authorise the charging transaction is nearly the same for all 3 solutions: 2,2-2,6 s (ring signature is the slowest)[1]
- Monthly transaction logs for the whole country:

	Storage	Processing time (CPU hours)
baseline scenario	0,74 GB	4 hours 42 minutes
ephemeral scenario	4,0 GB	4 hours 42 minutes
ring signature scenario	8,7 GB	87 hours 18 minutes

[1] Prototype was running on 2 modern mobile phone and used BLE for communications

Results: Privacy

- Both ephemeral and ring signature solutions achieve the privacy goals:
  - EVU's identity is not revealed to CS/CSO/DSO
  - EVU's location (=CS's real identity) is not revealed to ER/DSO
- In ephemeral scenarios a misbehaving CSO could also prove CS's identity and thus location, but in ring signature scenario it cannot

Results: Summary

- Both solutions achieve the privacy goals
  - ring signature provides slightly better privacy
- Both privacy-preserving solutions require an order of magnitude more storage than baseline
  - still perfectly feasible for a real system
- Ring signature requires an order of magnitude more processing than the other solutions
  - still perfectly feasible for a real system

  ⇒ Ephemeral approach is more efficient with only slightly reduced privacy, which can be particularly relevant for constrained devices