EPFL

EPFL Center for Digital Trust

Privacy in Electronic Identities

Linus Gasser, C4DT/EPFL

About These Slides

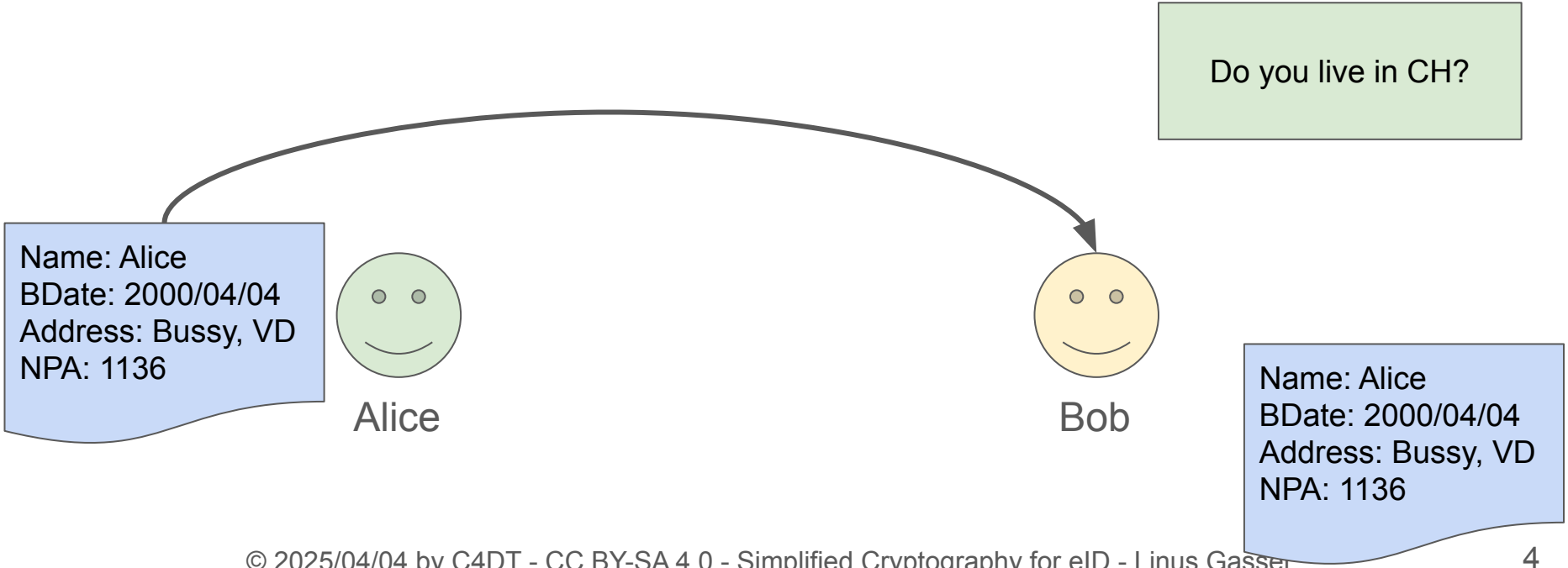
These slides were taken from the E-ID Cryptography Hands-on Workshop on the 29th of October 2024, organized by the Factory of c4dt.epfl.ch. You can find the workshop here:

https://github.com/c4dt/eid-workshop

The material in here is ***simplified***, but serves as an explanation on the challenges of making a secure and private E-ID system. Don't hesitate to reach out to factory@c4dt.org .

Part 1 - Cryptographic Elements of Swiyu

Attribute Sharing



Attribute Sharing - 1st Problem

Is the data correct?

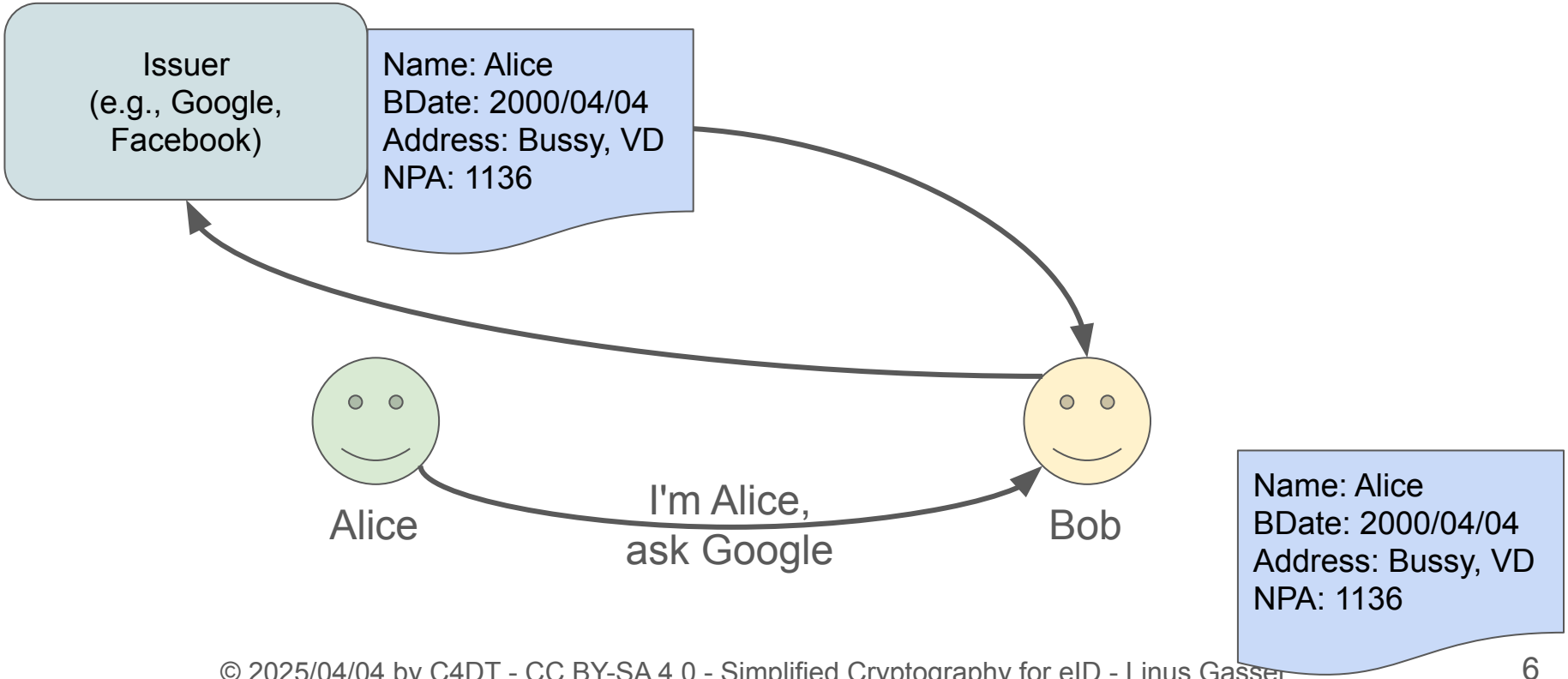
Name: Alice
BDate: 2000/04/04
Address: Bussy, VD
NPA: 1136

Alice

Bob

Name: Alice
BDate: 2000/04/04
Address: Bussy, VD
NPA: 1136

Using Trusted Third Party



Using Trusted Third Party - 2nd Problem

Issuer
(e.g., Google,
Facebook)

Name: Alice
BDate: 2
Address
NPA: 11

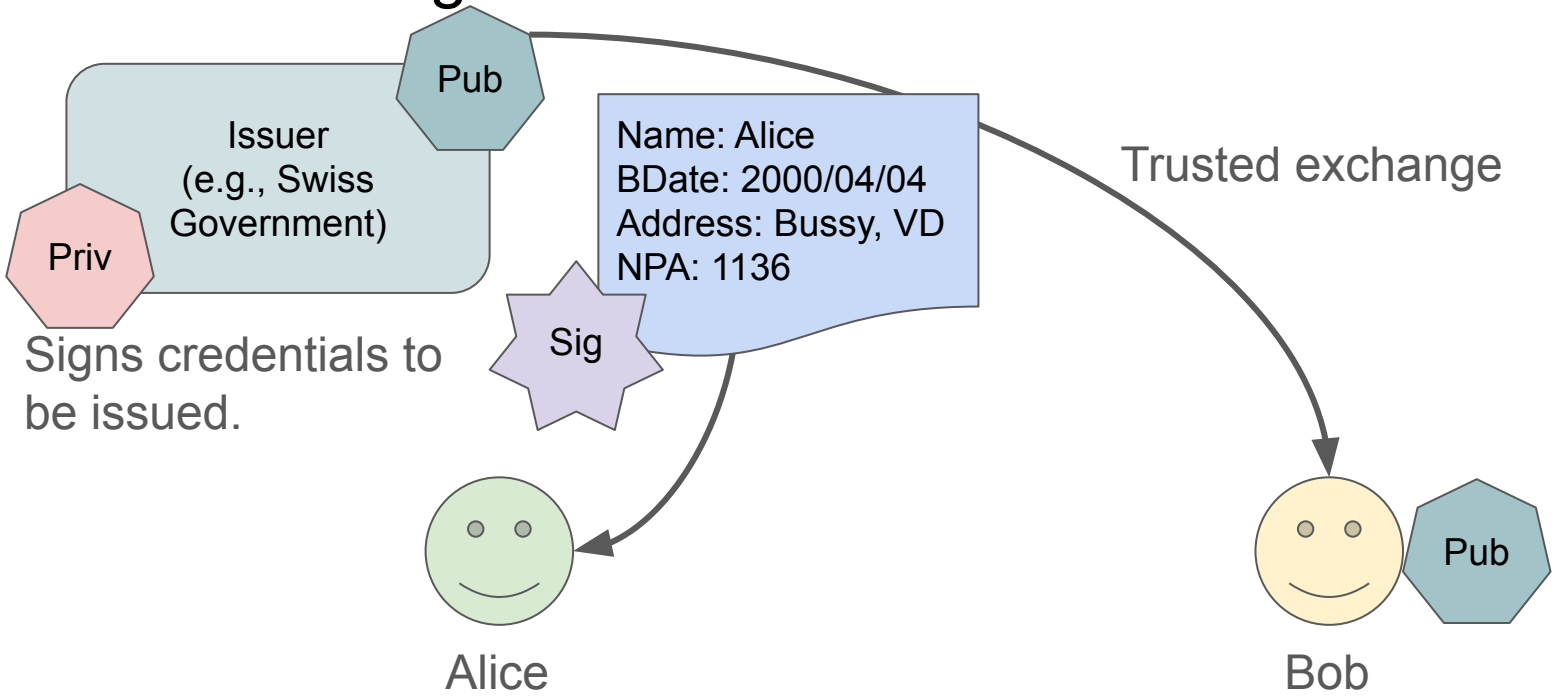
Issuer learns what
Alice is doing

Alice

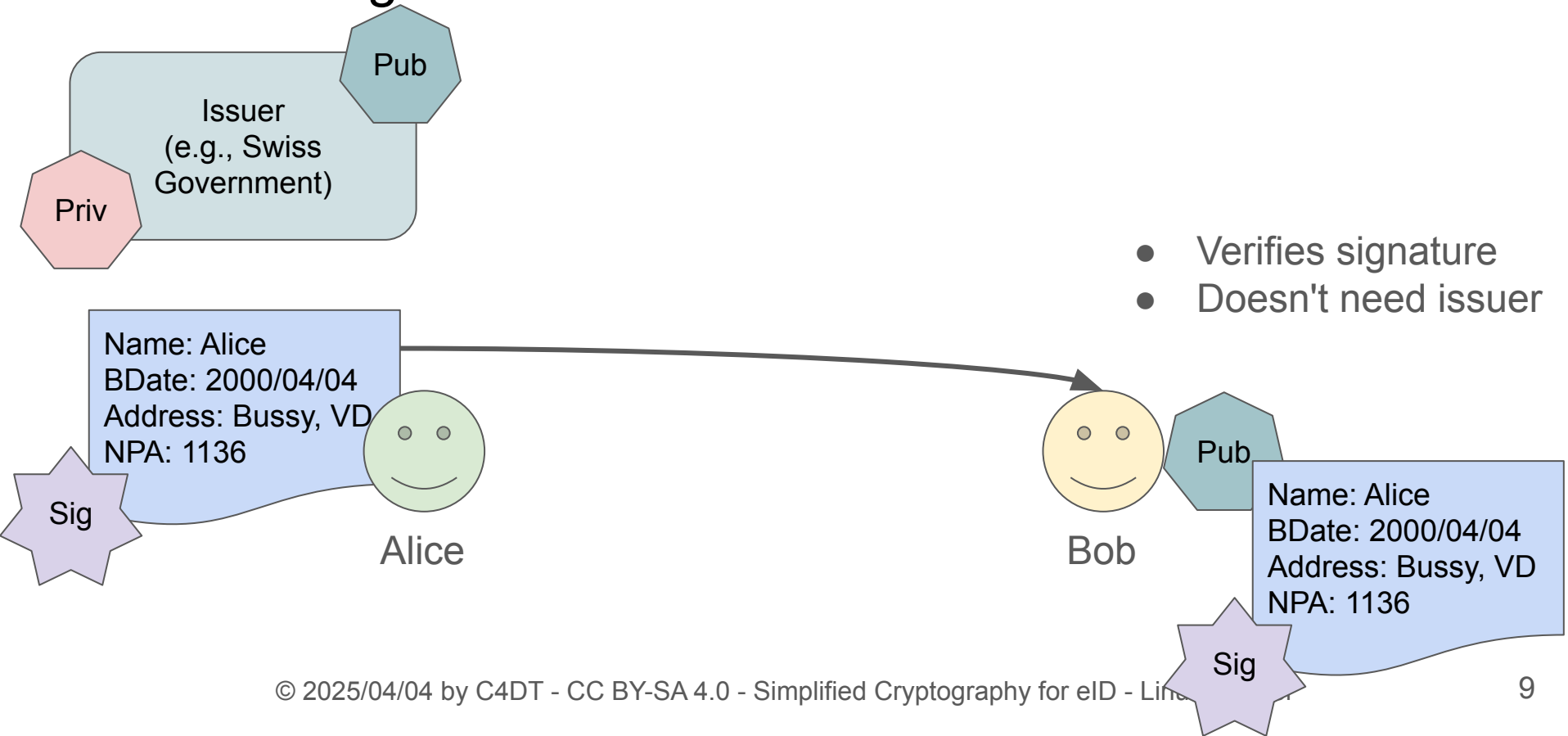
Bob

Name: Alice
BDate: 2000/04/04
Address: Bussy, VD
NPA: 1136

Self-Sovereign Identities

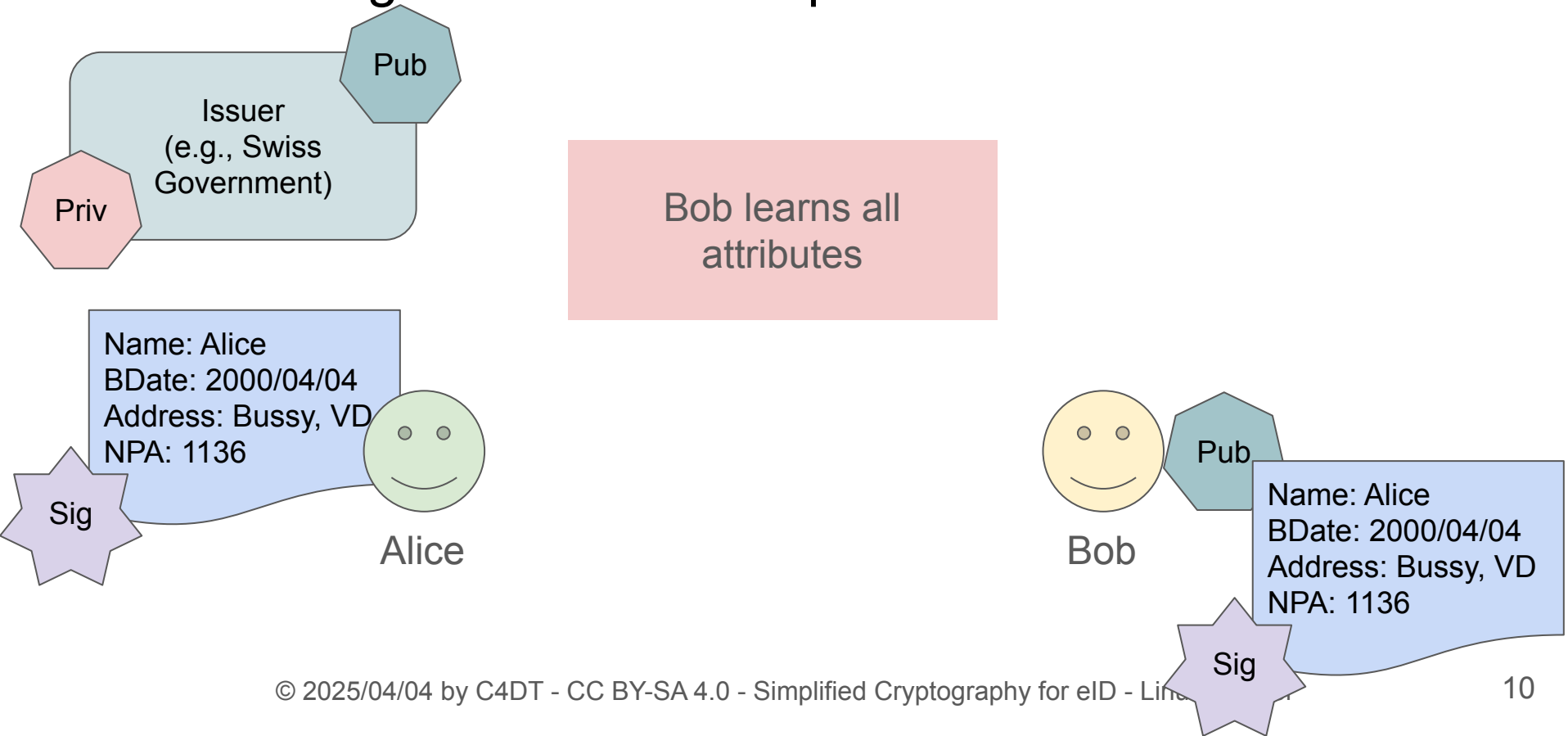


Self-Sovereign Identities

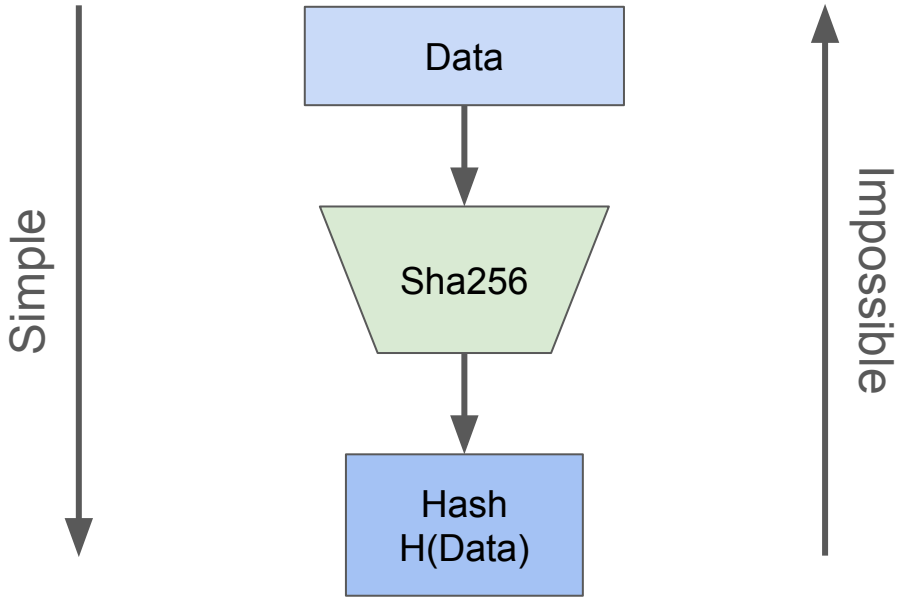


- Verifies signature
- Doesn't need issuer

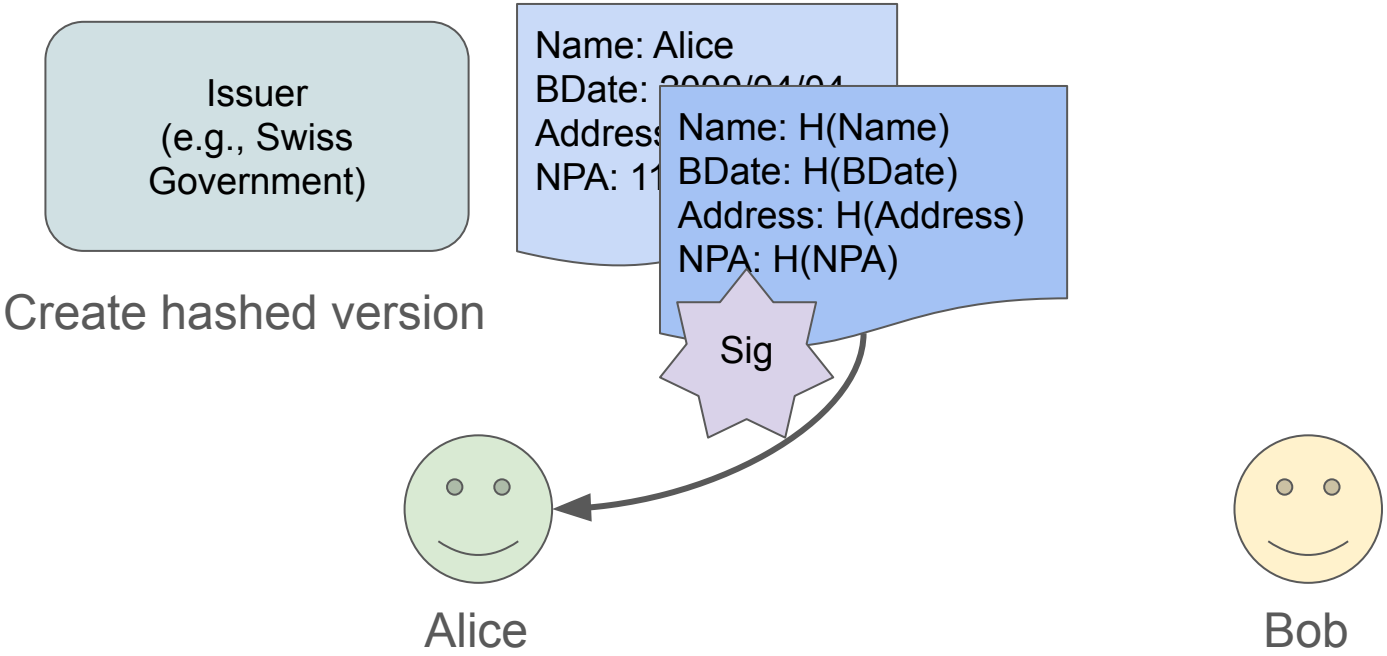
Self-Sovereign Identities - 3rd problem



What is a Hash?



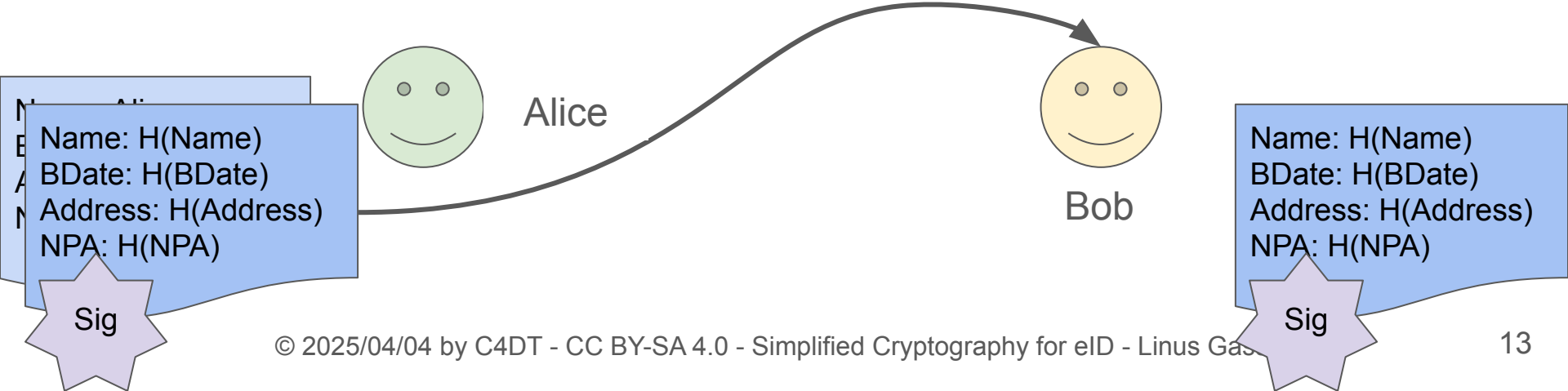
Selective Disclosure



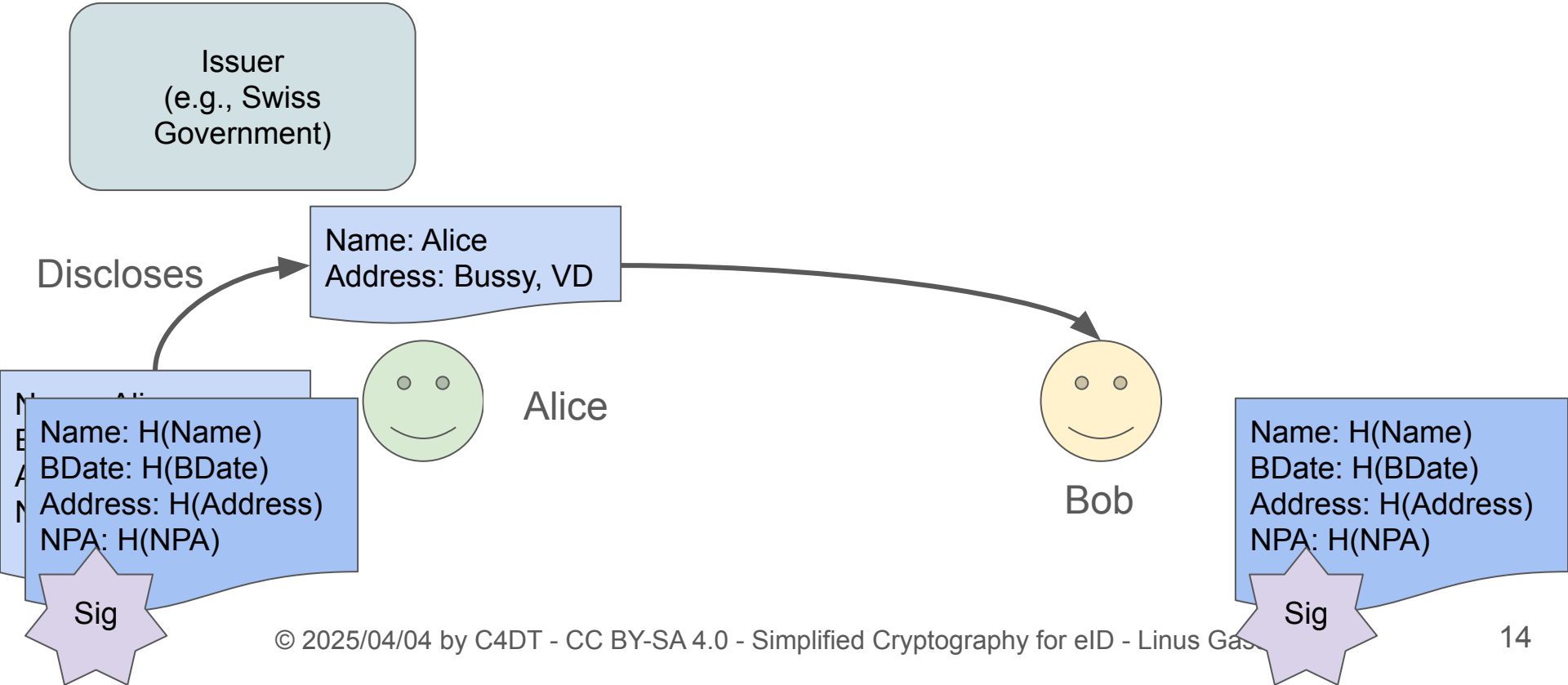
Selective Disclosure

Issuer
(e.g., Swiss
Government)

- Verifies signature
- Hashes give no information about Alice

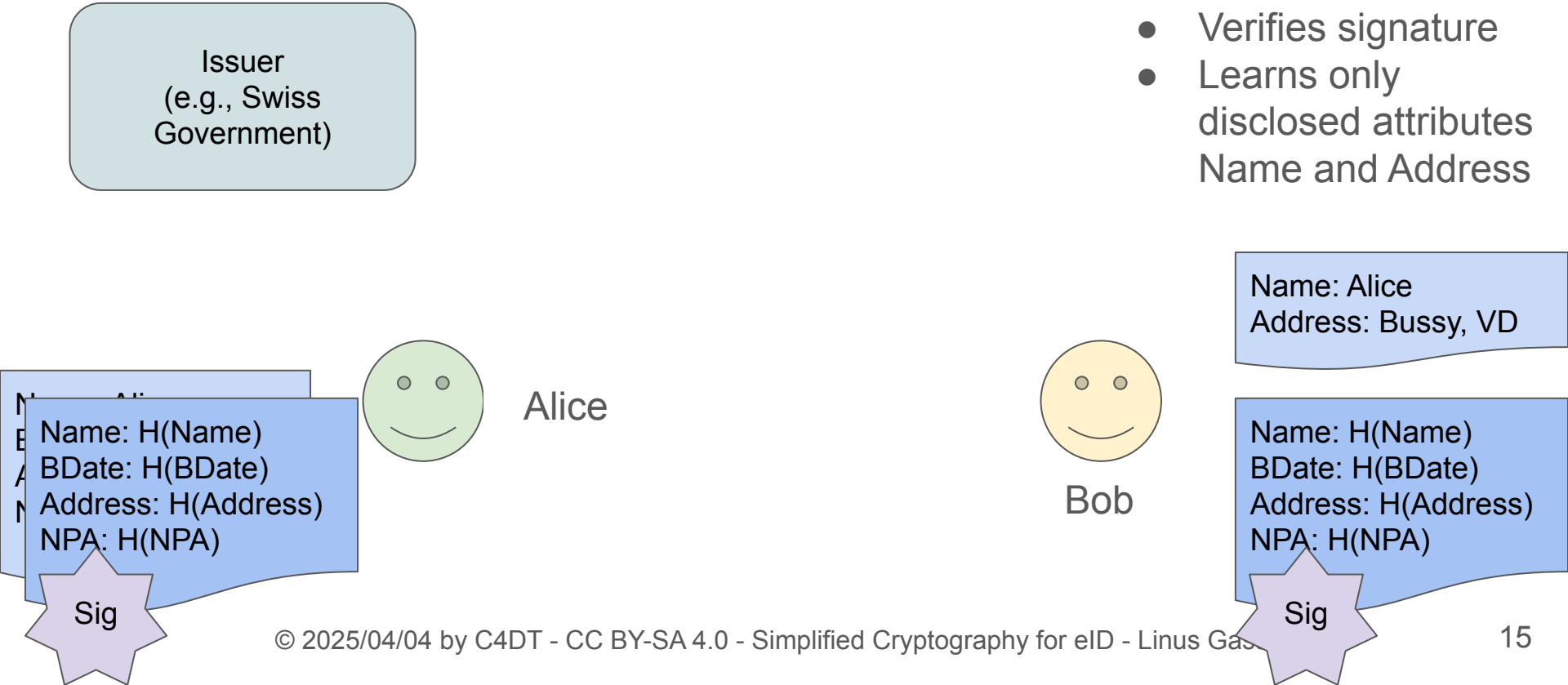


Selective Disclosure



Selective Disclosure

- Verifies hashes
- Verifies signature
- Learns only disclosed attributes Name and Address



End of Part 1

The EUDI-Wallet, and the CH eID solution, will include at least these parts.

- Self-sovereign identity
  - Keeps the usage of the identity hidden to the issuer
- Selective disclosure
  - Allows the holder of the credentials to hide some of the attributes

Another part which is not shown here is the "device binding", so you cannot copy your E-ID to another phone.

Part 2 - Additional Privacy Measures

Selective Disclosure - 4th Problem

Issuer
(e.g., Swiss
Government)

Linkability: Bob and Charlie can track Alice, and learn more about her

ame: Alice
Address: Bussy, VD

BDate: 2000/04/04
NPA: 1136

Name: H(Name)
BDate: H(BDate)
Address: H(Address)
NPA: H(NPA)

Sig

Alice

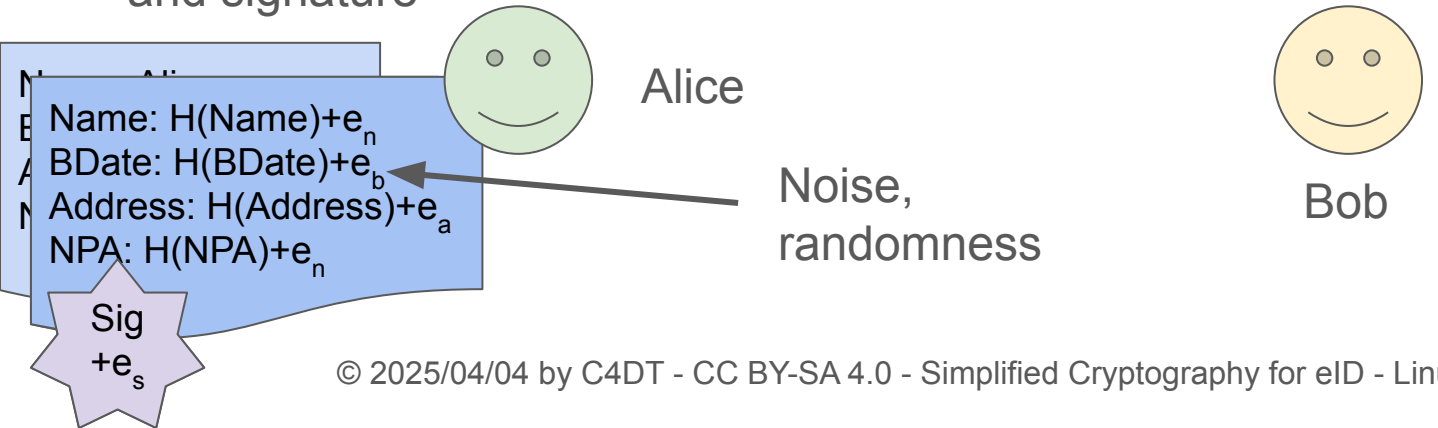
Bob

Carole

Blinding Data with BBS+

Issuer
(e.g., Swiss
Government)

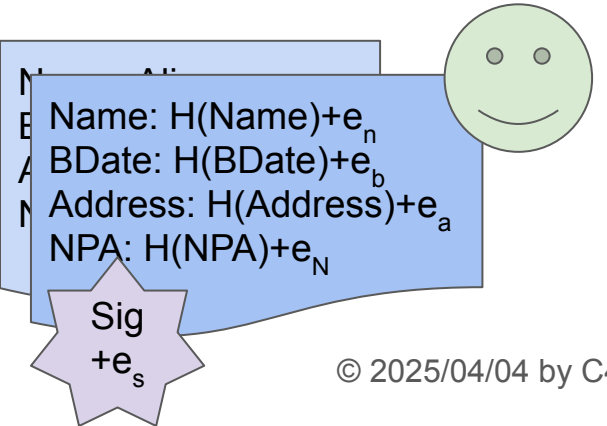
- Blinds her hashes and signature



Blinding Data with BBS+

Issuer
(e.g., Swiss
Government)

GA Travelcard for 25
year old?

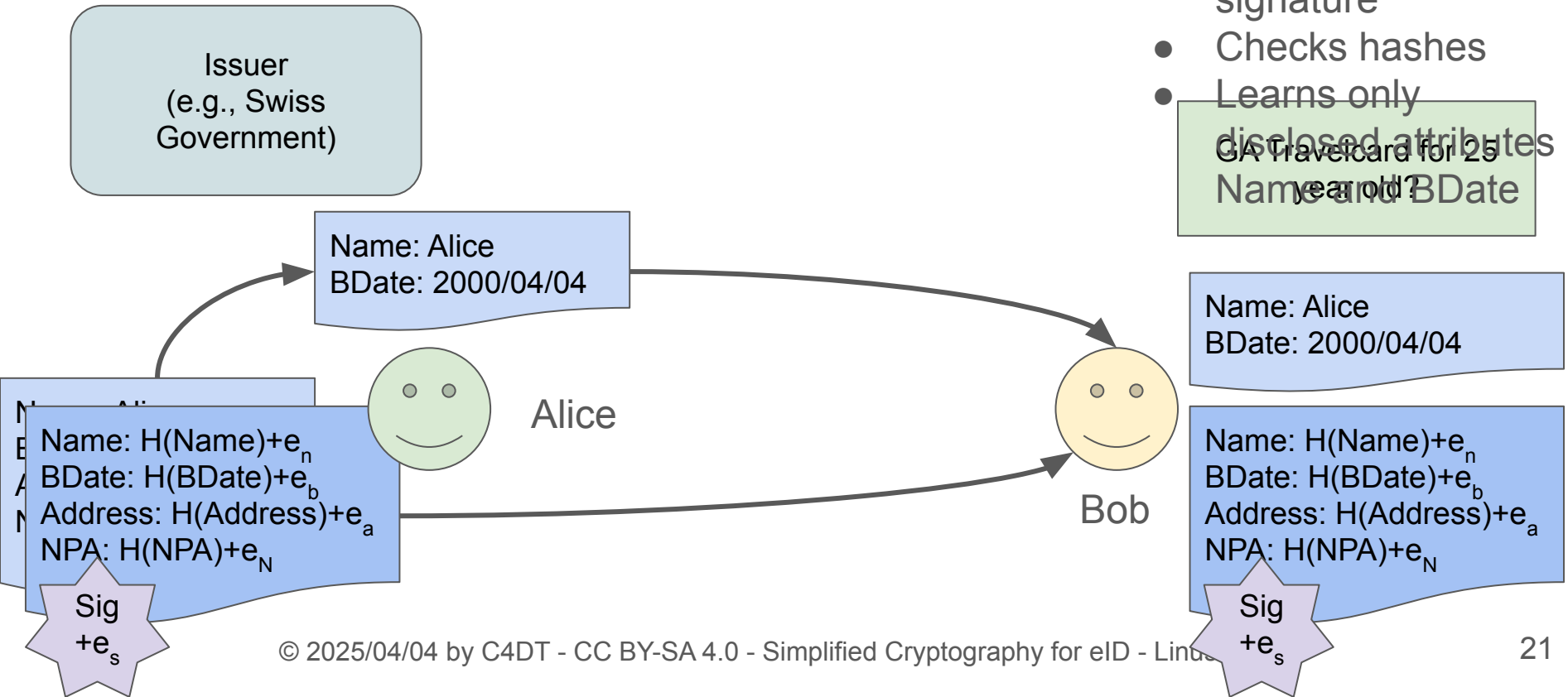


Alice

Bob

Blinding Data with BBS+

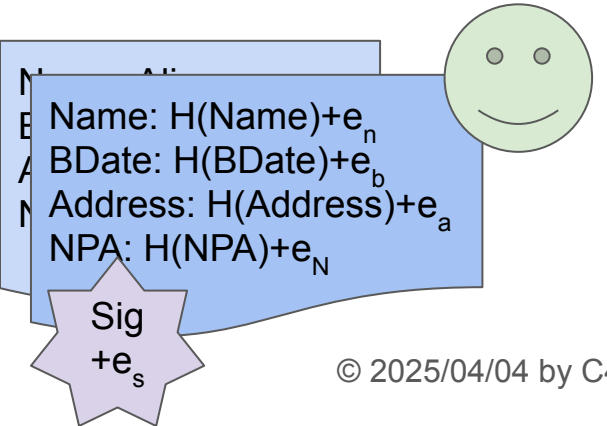
- Verifies blinded signature
- Checks hashes
- Learns only disclosed attributes



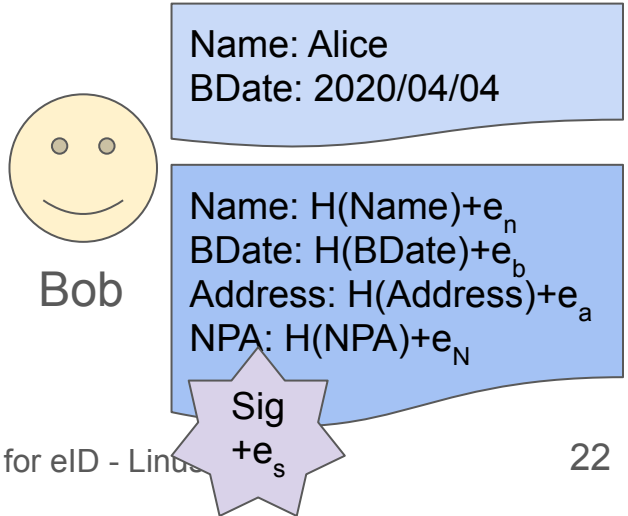
Blinding Data with BBS+ - 5th Problem

Issuer
(e.g., Swiss Government)

Too Much Information: Bob learns more than necessary.

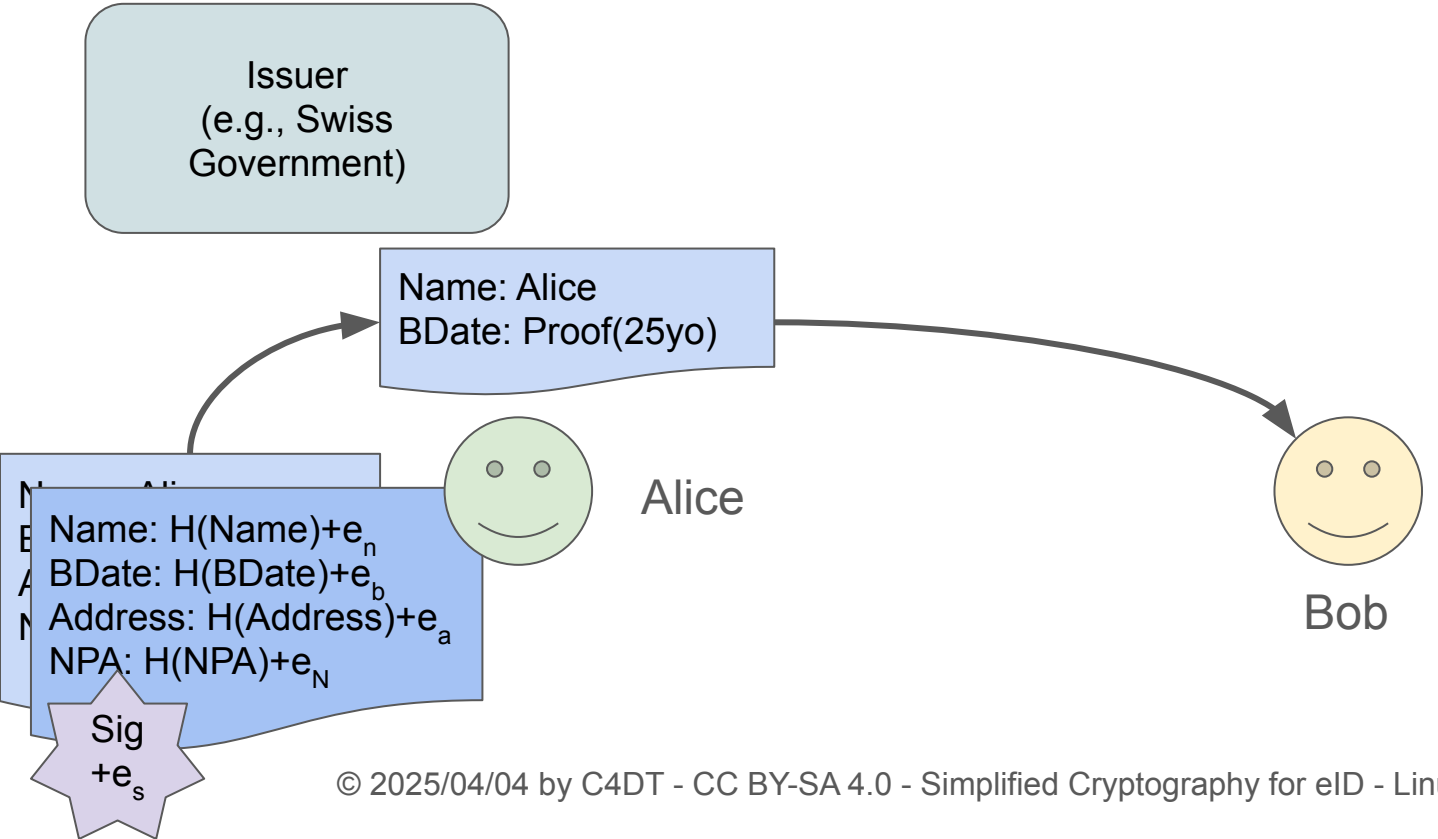


Alice



Bob

Predicate Proofs - Zero Knowledge Proofs



Predicate Proofs - Zero Knowledge Proofs

- Verifies blinded signature
- Verifies hashes
- Verifies proof
- Learns only predicates

Issuer
(e.g., Swiss Government)

Name: Alice
BDate: Proof(25yo)

Name: H(Name)+e_n
BDate: H(BDate)+e_b
Address: H(Address)+e_a
NPA: H(NPA)+e_N

Sig +e_s

Alice

Bob

Name: H(Name)+e_n
BDate: H(BDate)+e_b
Address: H(Address)+e_a
NPA: H(NPA)+e_N

Sig +e_s

Predicate Proofs - Zero Knowledge Proofs - 6th Problem

Issuer
(e.g., Swiss Government)

Too much cryptography - will people use eID? What other conditions need to be met?

Name: Alice
BDate: Proof(25yo)

Alice

Name: H(Name)+e_n
BDate: H(BDate)+e_b
Address: H(Address)+e_a
NPA: H(NPA)+e_N

Sig +e_s

Bob

Name: H(Name)+e_n
BDate: H(BDate)+e_b
Address: H(Address)+e_a
NPA: H(NPA)+e_N

Sig +e_s

Summary

The EUDI-Wallet, and the CH eID solution, will include at least these parts.

- Self-sovereign identity
  - Keeps the usage of the identity hidden to the issuer
- Selective disclosure
  - Allows the holder of the credentials to hide some of the attributes

Another part which is not shown here is the "device binding", so you cannot copy your E-ID to another phone.

C4DT, together with two of its partners, starts research on existing and new algorithms and libraries for the other parts:

- Blinding Data with BBS+
  - Remove the "Linkability" from eID
- Predicate Proofs
  - Minimize the transferred information
- Private Revocation
  - Private eID invalidation

All these parts exist, but they are slow, sometimes not tested, or not private enough.

Links

- A short summary of our hands-on workshop: https://c4dt.epfl.ch/article/e-id-hands-on-workshop/
- Link for Swiyu: https://www.eid.admin.ch/en
- GitHub for Swiyu: https://github.com/swiyu-admin-ch

Unrelated side project: Decentralized Resource Sharing in Your Browser