EPFL

EPFL Center for Digital Trust

Privacy in Electronic Identities

Linus Gasser and Carine Dengler, C4DT/EPFL

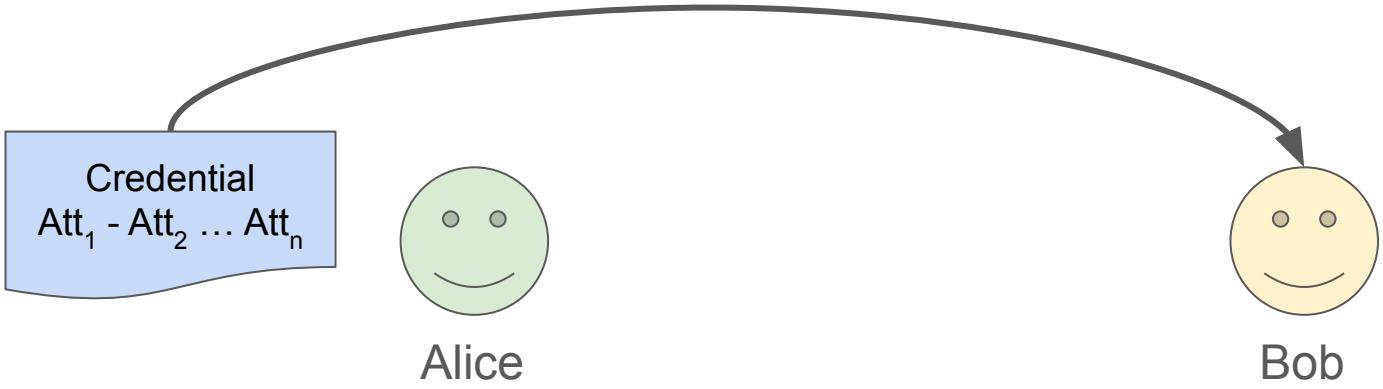
About These Slides

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 .

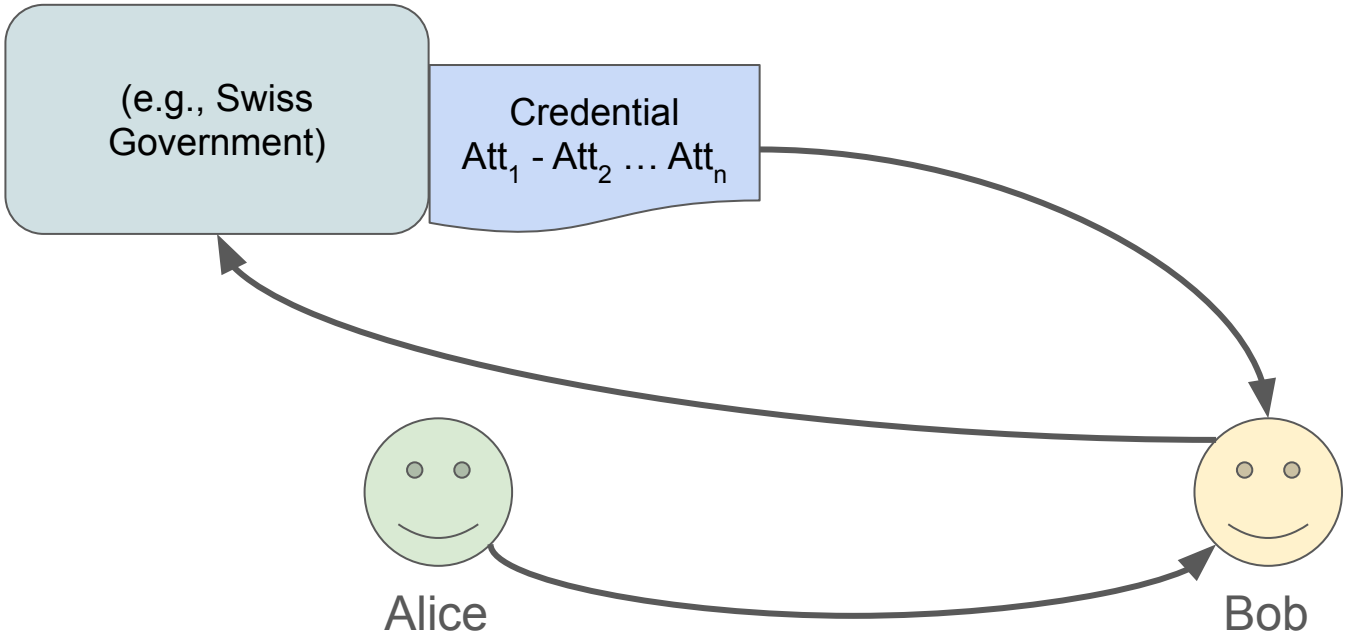
Attribute Sharing



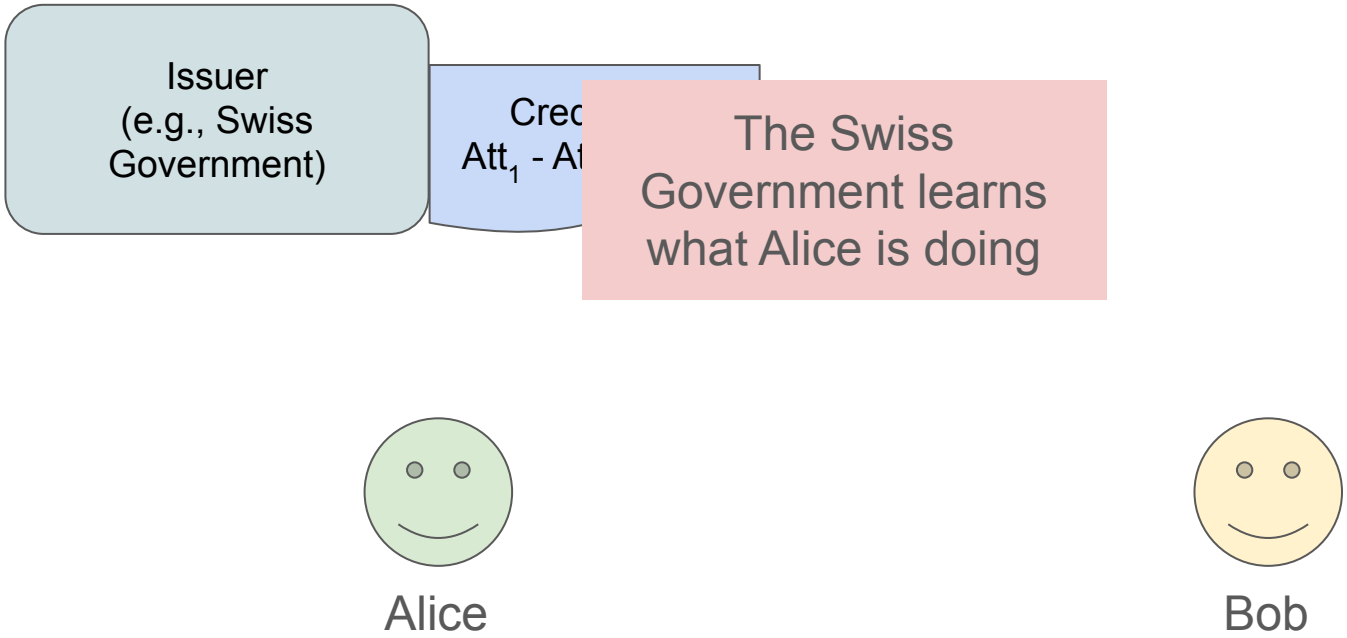
Attribute Sharing - 1st Problem

Are the attributes correct?

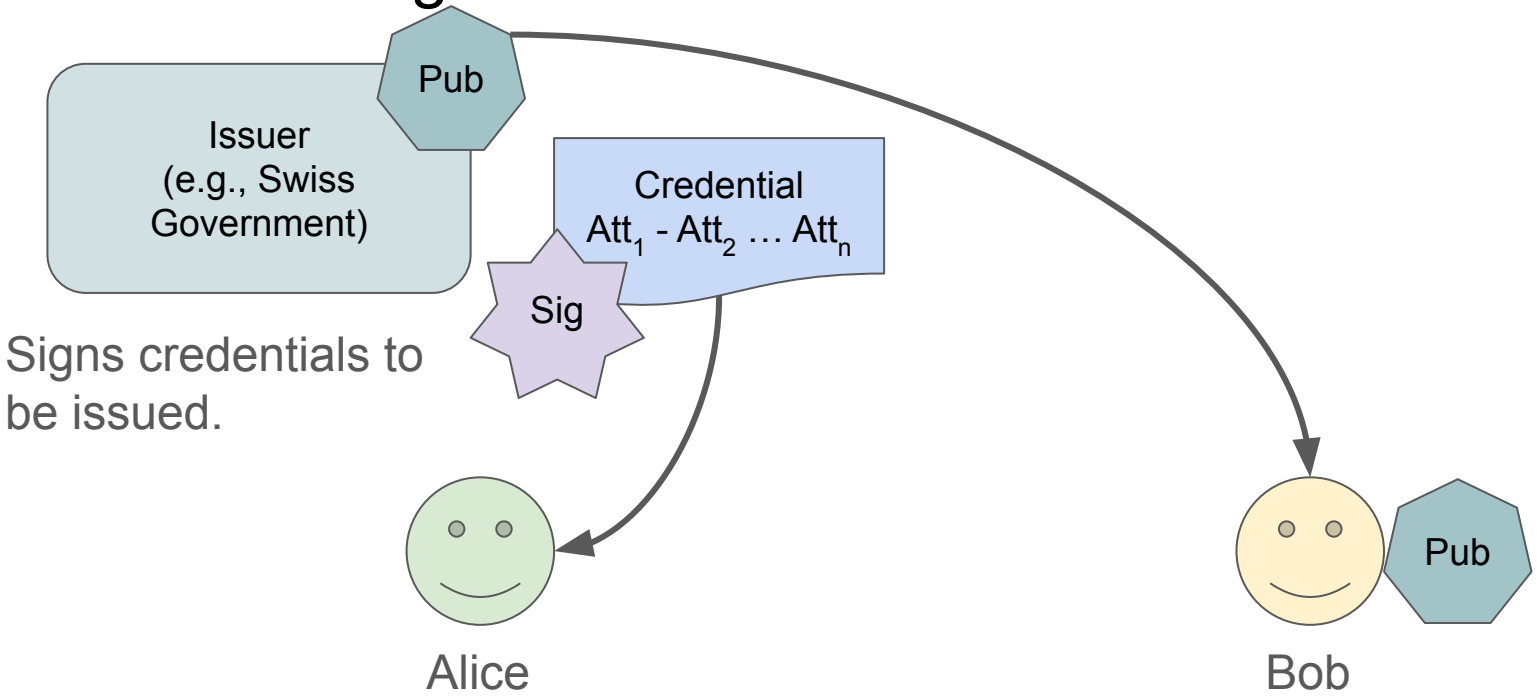
Using Trusted Third Party



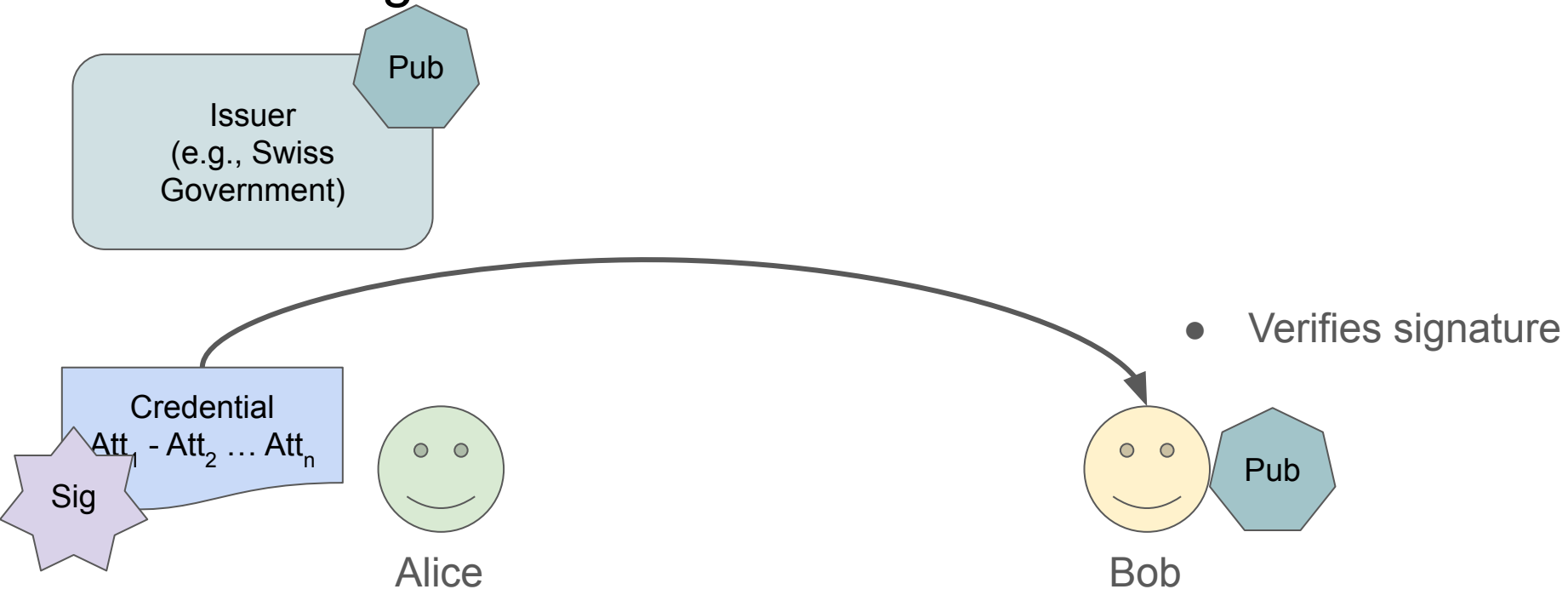
Using Trusted Third Party - 2nd Problem



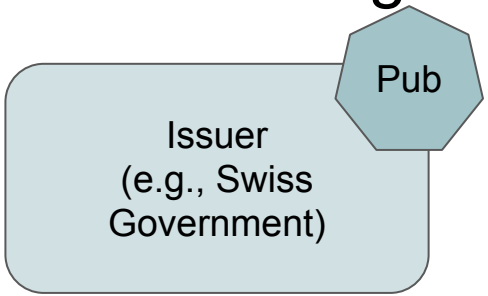
Self-Sovereign Identities



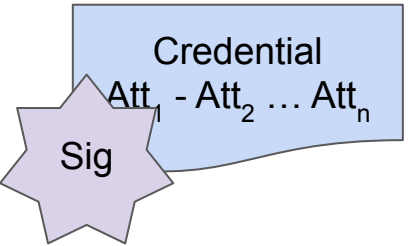
Self-Sovereign Identities



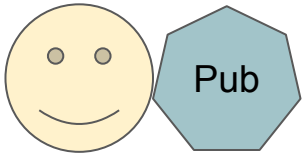
Self-Sovereign Identities - 3rd Problem



Bob learns all attributes

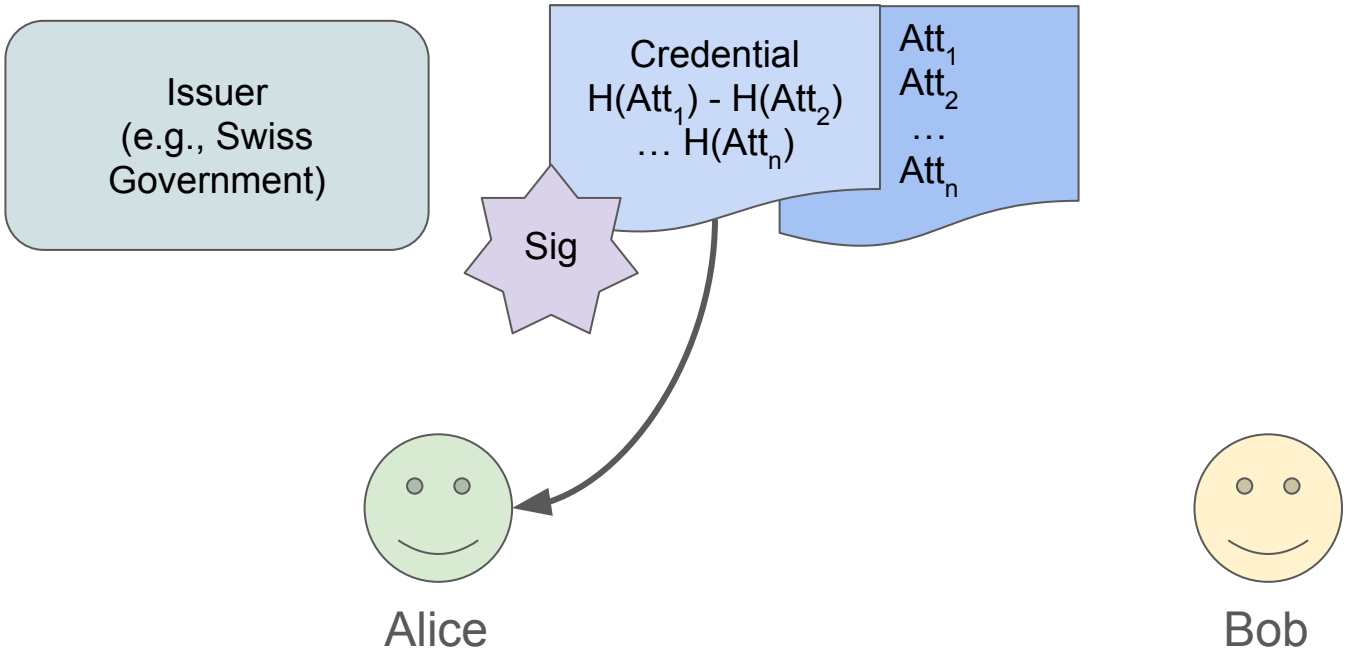


Alice

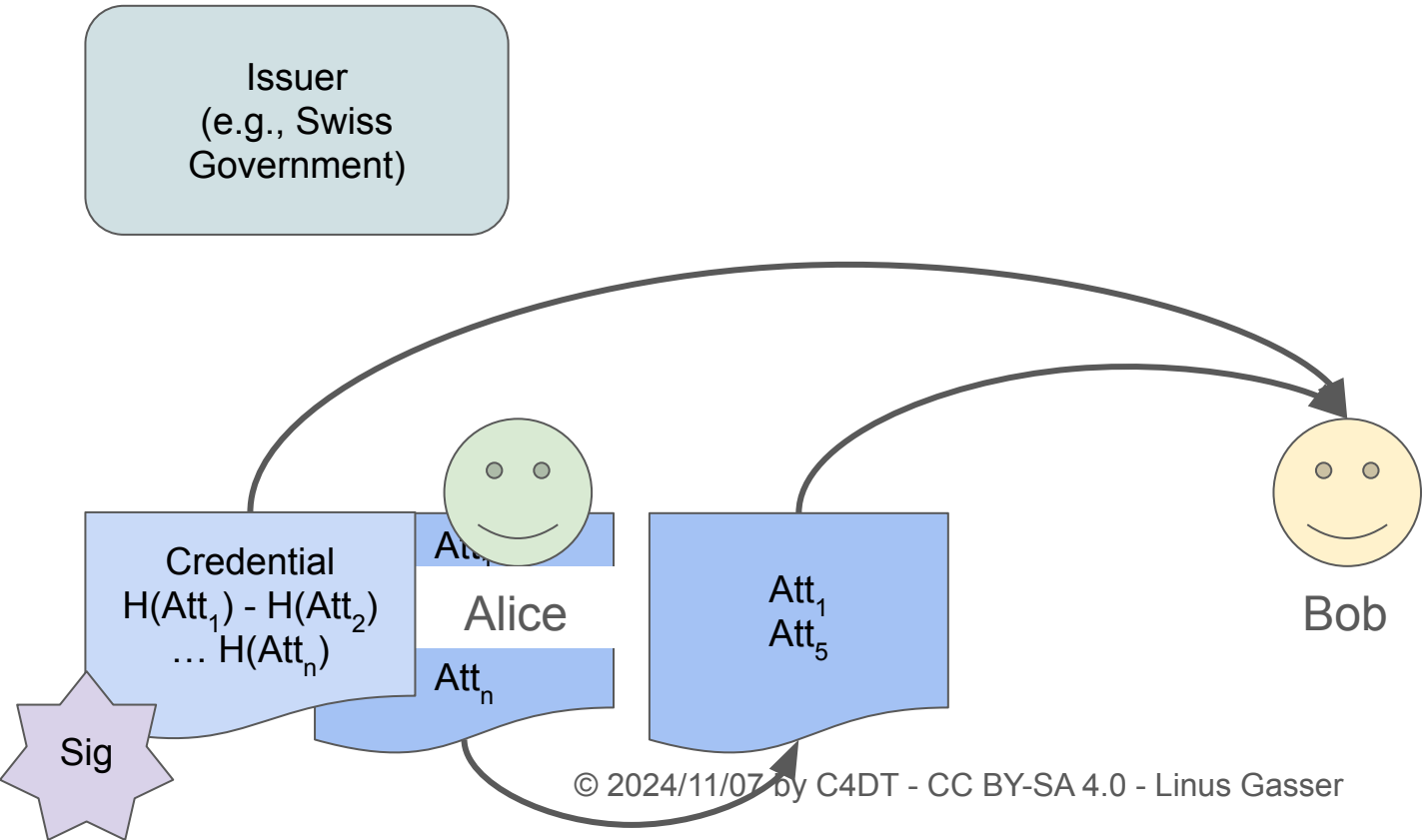


Bob

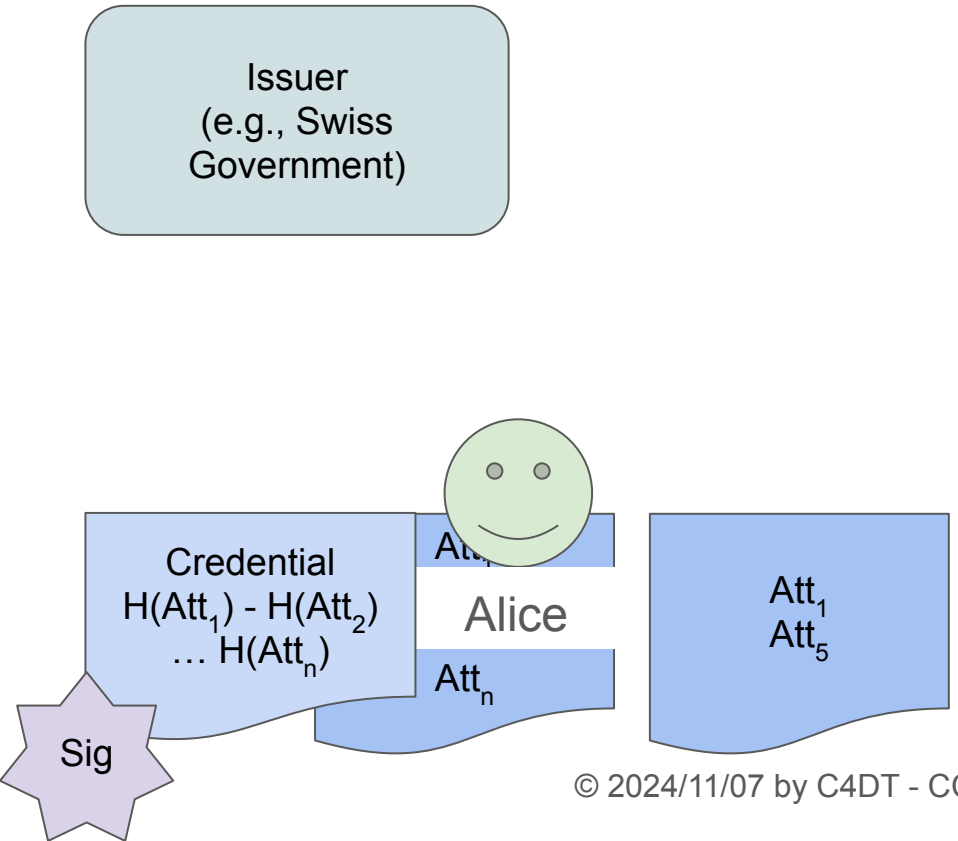
Selective Disclosure



Selective Disclosure



Selective Disclosure

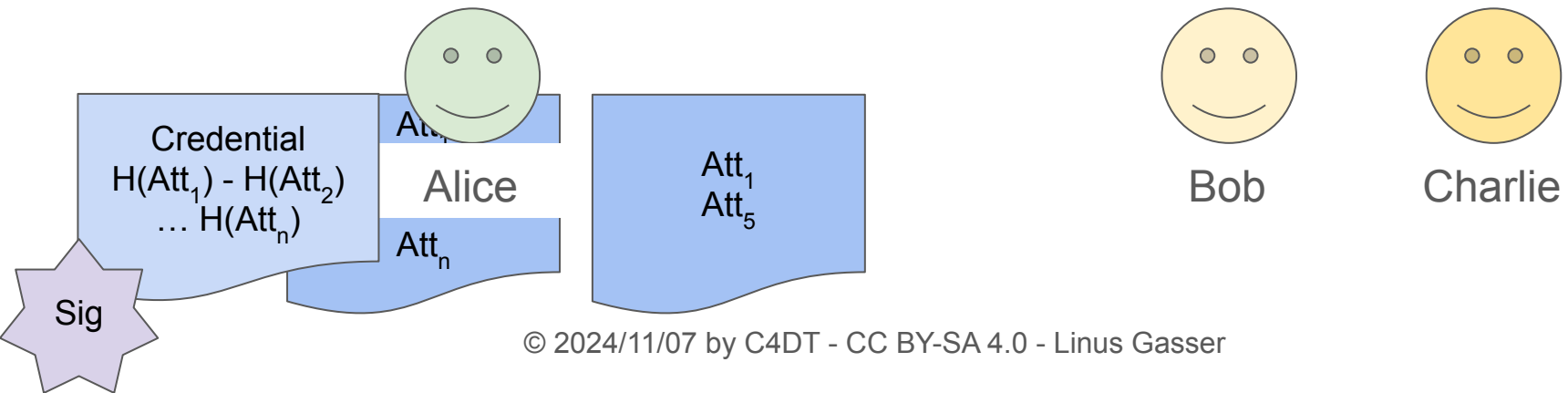


- Verifies signature
- Learns only disclosed attributes 1 and 5

Selective Disclosure - 4th Problem

Issuer
(e.g., Swiss Government)

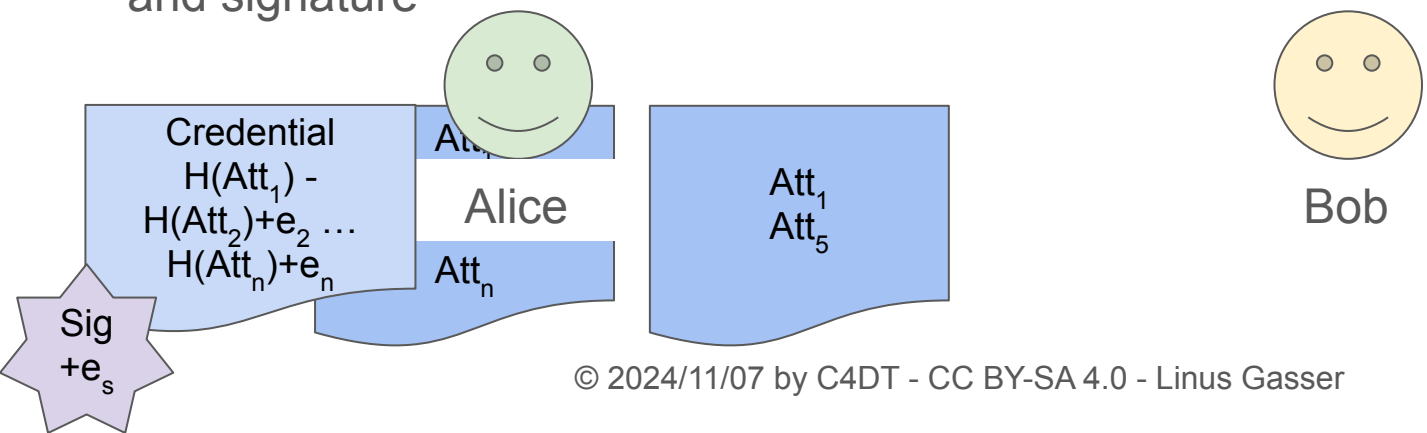
Linkability: Bob and Charlie can correlate Alice's signature



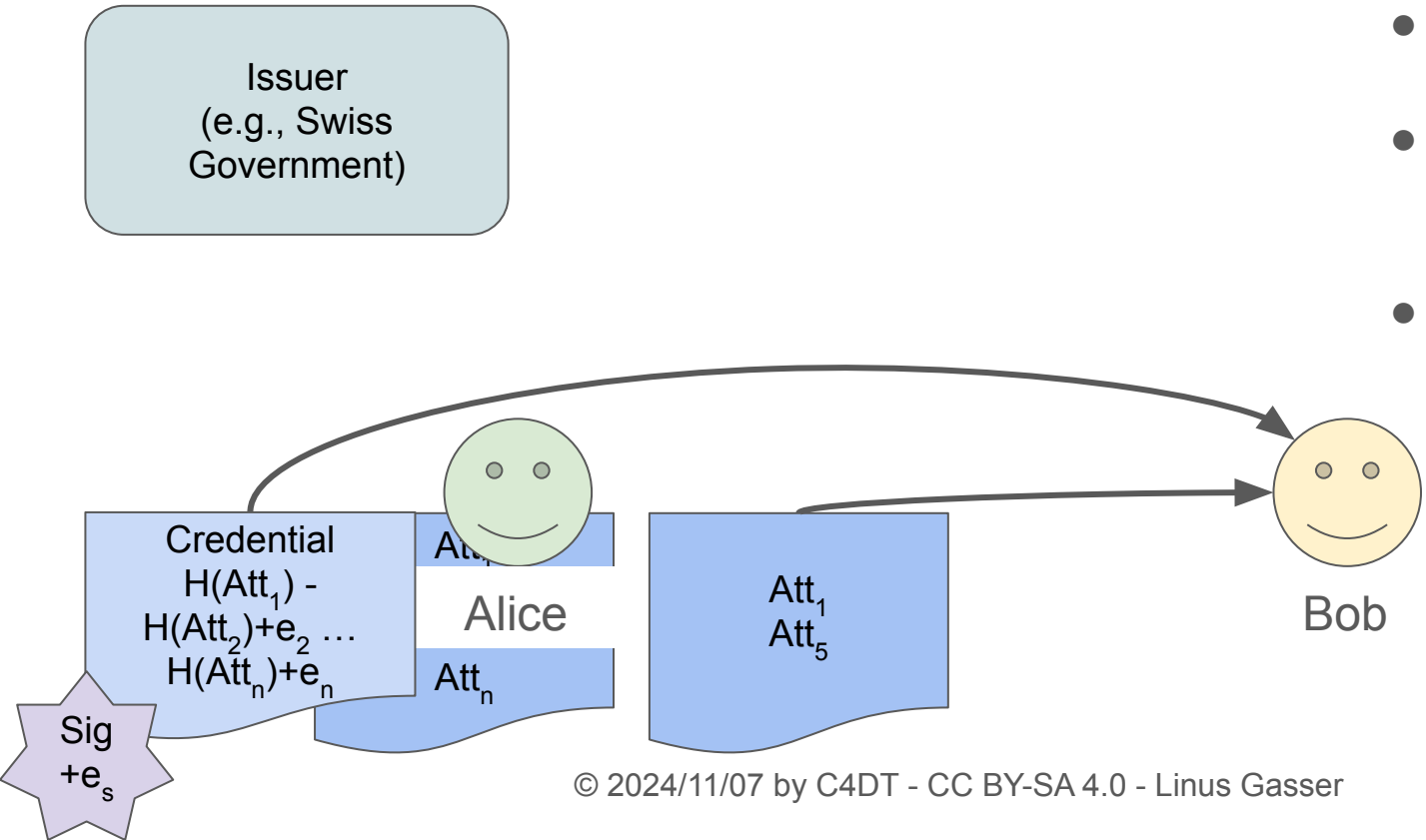
BBS+

Issuer
(e.g., Swiss Government)

- Blinds her hashes and signature



BBS+



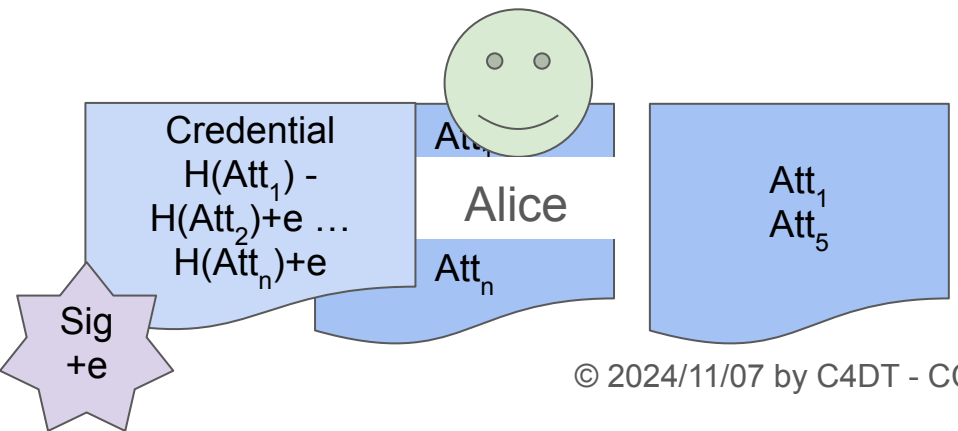
- Verifies blinded signature
- Learns only disclosed attributes 1 and 5
- Can send a "challenge" to avoid replaying attacks

BBS+ - 5th Problem

Issuer
(e.g., Swiss Government)

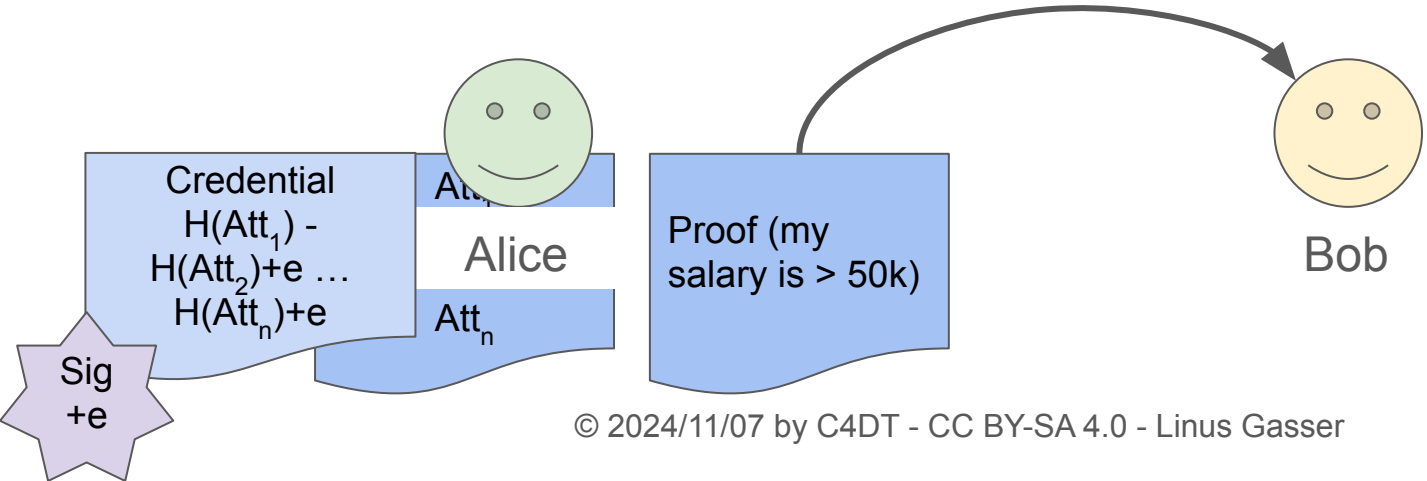
Too Much Information: Bob learns more than necessary.

- Verifies blinded signature
- Learns only disclosed attributes 1 and 5



Predicate Proofs - Zero Knowledge Proofs

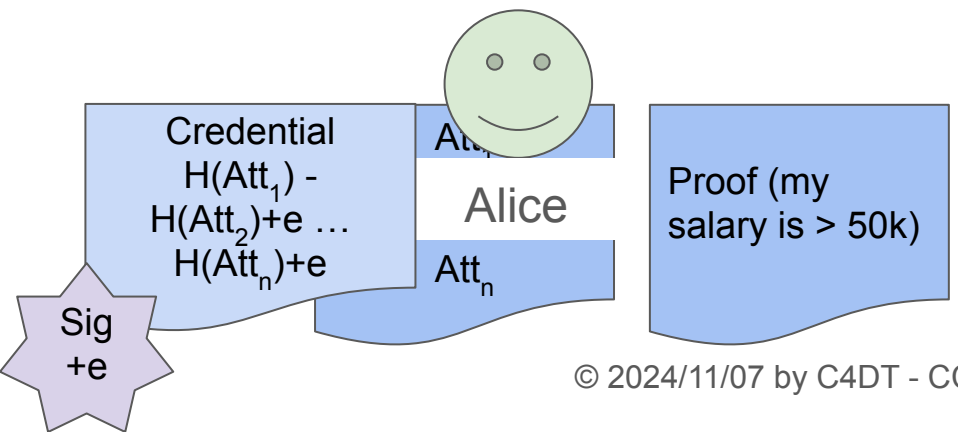
Issuer
(e.g., Swiss
Government)



Predicate Proofs - Zero Knowledge Proofs

Issuer
(e.g., Swiss Government)

- Verifies blinded signature
- Learns only predicates



Summary

The EUDI-Wallet will include at least these parts. For the CH E-ID, the final decision has not been taken yet.

- Trusted third party
  - Allows the verifier to trust the attributes
- 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 "holder binding", so you cannot copy your E-ID to another phone.

The following technologies create even more privacy for the user:

- BBS+
  - Modifies the signature and the hashes between proofs to avoid linking by the verifiers.
- Predicate proofs
  - Reduce the presentation to the minimum information necessary: salary below a given threshold, older/younger than x years, etc.

But they are difficult to implement while allowing to do a "holder binding". So further research is needed.