draft-ietf-cose-bls-key-representations

Key Representation Definitions for Barreto-Lynn-Scott Cryptographic Curves

Overview

- This draft registers the required parameters for both the JWK and COSE_Key cryptographic key representations for the Barreto-Lynn-Scott (BLS) family of curves (both the 12-381 and 48-581)
- The Barreto Lynn Scott curves (BLS) are said to be “pairing friendly” which enables usage of some novel algorithms. From the pairing friendly family the BLS curves are the most popular in use today.
- Formal definition of the BLS curves is a work item of the CFRG draft-irtf-cfrg-pairing-friendly-curves

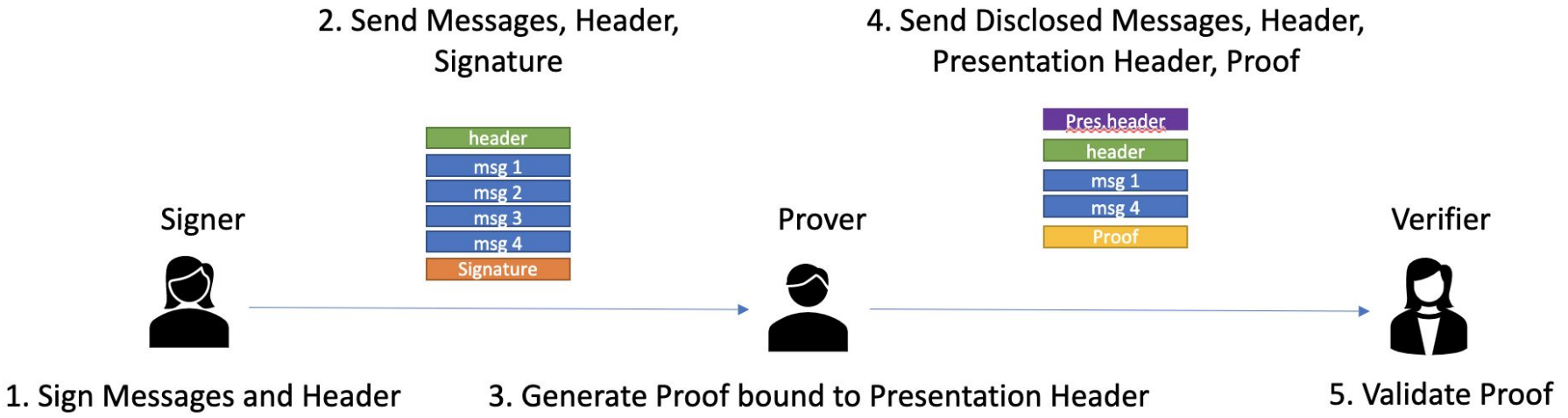
BLS Signatures

- An aggregate signature scheme
- It enables aggregating signatures over the same payload together where the aggregated result can still be checked against the individual signers public keys.
- Useful in blockchain applications where nodes in the network need to sign and confirm blocks
- Used by many blockchain networks, most notably Ethereum and Filecoin
- Work item of the CFRG draft-irtf-cfrg-bls-signature

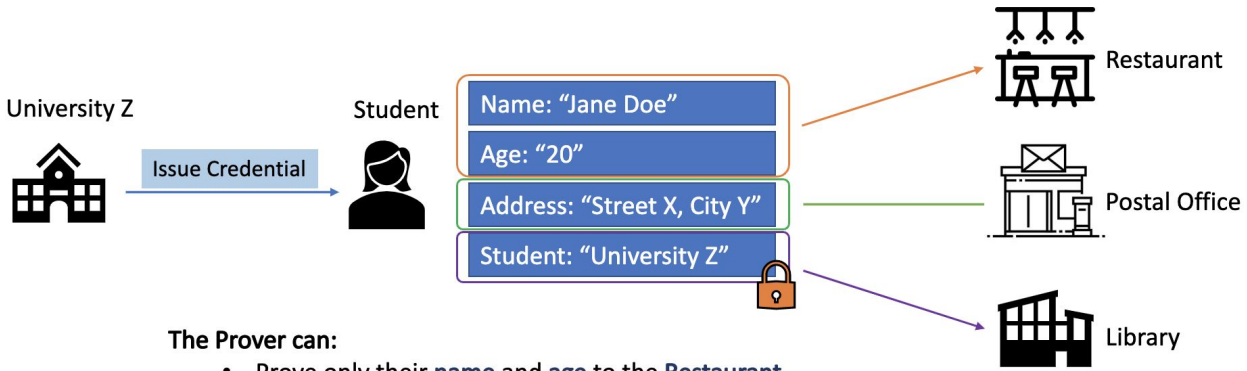
BBS Signatures

- A digital signature scheme supporting
  - Selective disclosure (multi message signing)
  - Proof of possession
  - Unlinkable proofs (via a ZKP protocol)
- Defined in draft-looker-cfrg-bbs-signatures, calling for adoption at the CFRG

BBS Signatures



Privacy Preserving Anonymous Credentials



The Prover can:

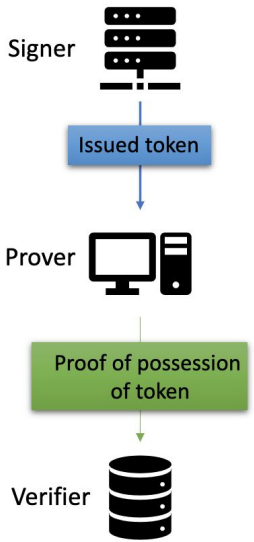
- Prove only their **name** and **age** to the **Restaurant**
- Prove only their **address** to the **Postal Office**.
- Prove only that they **are a student** to the **Library**.

➢ Only send the information that is relative to each Verifier

➢ The Verifiers cannot conspire to discover more information

(each proof is indistinguishable from random)

Proof of possession enabled security/access tokens



From the signers perspective:

- They can issue a single token that can be used multiple times by the prover.
- Does not require key material supplied by the prover ahead of time to issue.

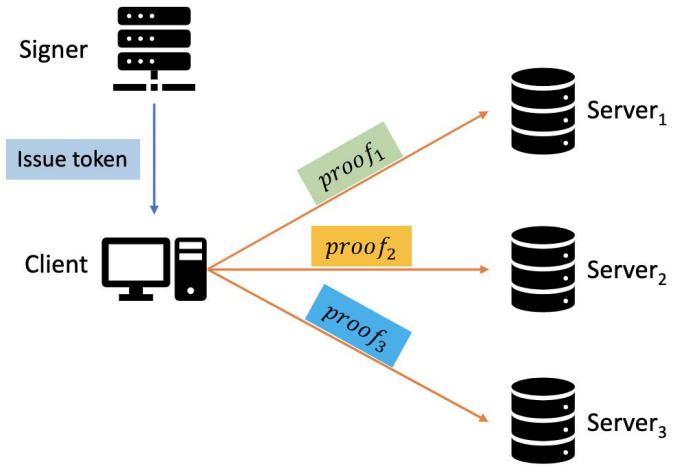
From the provers perspective:

- Can prover possession of the security token multiple times to different parties (verifiers).
- Does not require the prover to manage key material.
- Can scope generated proofs via the presentation header (e.g a generated proof is only valid for a particular verifier or has a TTL etc).

From the verifiers perspective:

- Validates the proof back to the original signer in a way that is inline with existing security tokens (e.g via the signers PK), also provides replay attack detection

Non-correlating security token proofs



During Proof Presentation:

- Each proof **cannot be correlated** to each other, the token or the client.
- Uncorrelatability holds even against **coalition between RPs** or **RPs and AS**.
- A unique **presentation header is NOT required** for un-correlatability to hold.