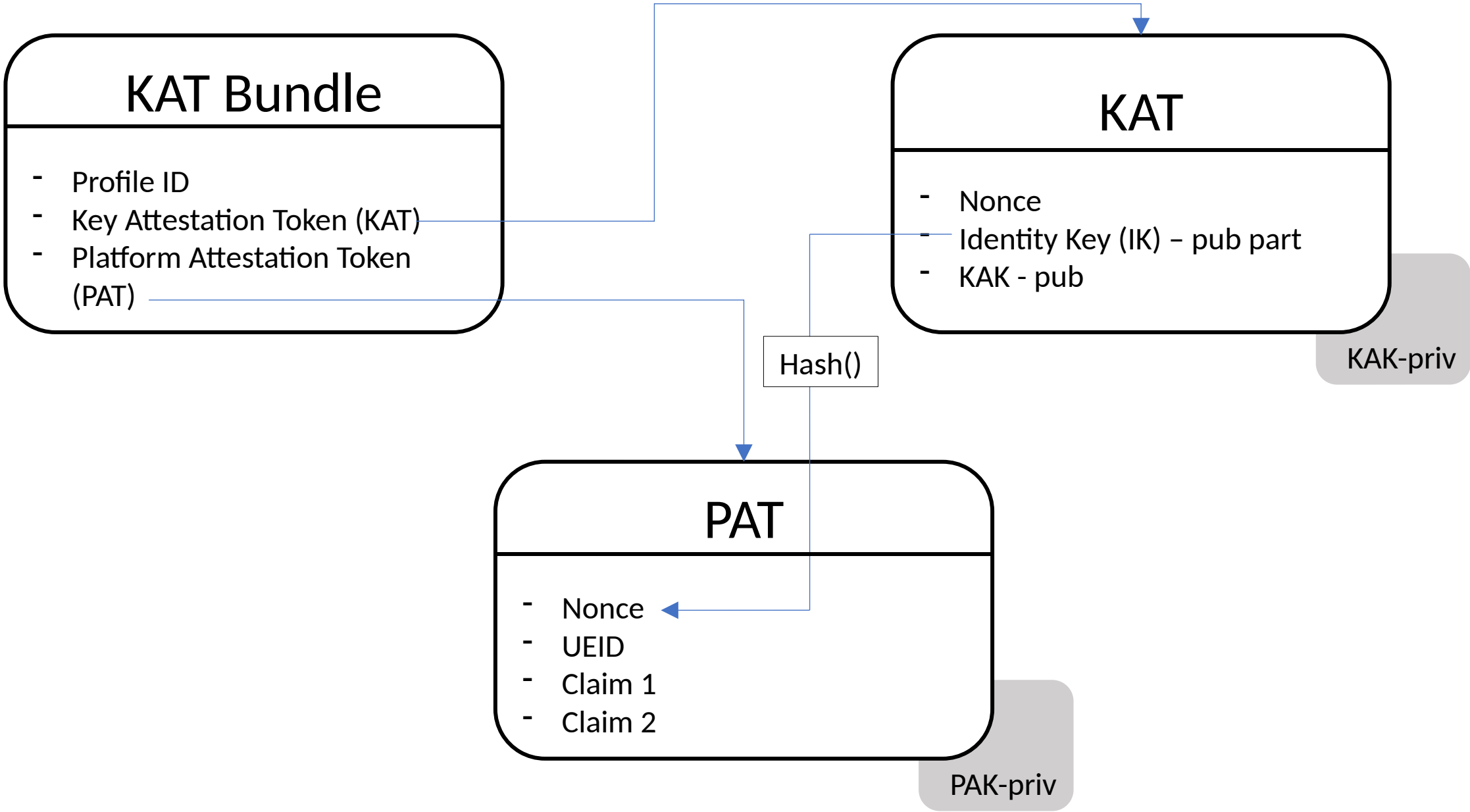
EAT-based Key Attestation Token and Attestation in TLS

draft-bft-rats-kat-00

draft-fossati-tls-attestation


KAT Bundle
- Profile ID
- Key Attestation Token (KAT)
- Platform Attestation Token (PAT)
KAT
- Nonce
- Identity Key (IK) – pub part
- KAK - pub
KAK-priv
Hash()
PAT
- Nonce
- UEID
- Claim 1
- Claim 2
PAK-priv

Using the KAT in TLS

- In draft-fossati-tls-attestation we describe how to use the KAT bundle with the TLS handshake.

- Steps:
  1. Generate IK key pair
  2. Obtain Nonce from peer
  3. Create KAT Bundle with IK and nonce
  4. Transmit KAT Bundle to peer
  5. Demonstrate possession of IK-priv

- draft-fossati-tls-attestation is agnostic to the attestation technology used thanks to draft-ftbs-rats-msg-wrap.

More Info

- Drafts:
  - https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/
  - https://datatracker.ietf.org/doc/draft-ftbs-rats-msg-wrap/
  - https://datatracker.ietf.org/doc/draft-bft-rats-kat/

- Prototyping code:
  - Veraison: https://github.com/veraison/services/tree/ietf-115-hackathon
  - Parsec: https://github.com/ionut-arm/parsec-se-driver/tree/attested-tls/
  - TLS extension: https://github.com/hannestschofenig/mbedtls/tree/tls-attestation