SPIFFE – Assertions and Tokens WG

https://spiffe.slack.com/archives/C03BS8JJYN4

Nested Token Model

Marco Antonio Marques

Nov/2023

Requirements and Goals

- **A descentralized mechanism to locally create authenticated statements**
- **A token scheme with support to extension and incremental signing (aggregation)**

- Can convey one or more **signed set of claims**
- **Size sensitive**
- **Cheap** signature and validation
- Support for **lightweight identity documents** and **pseudonyms**

Nested model

- Token construction is **technology-agnostic**. Proof of concept adopts a JSON-based model
- Three parts: **Payload, Signature, and Nested**
- Identity claims (e.g., issuer, audience, subject) can be:
  - **Common name:** A unique identifier (e.g., SPIFFE-ID)
  - **Public key:** A public key as unique identifier
  - **ID document:** An entire ID document (e.g., SVID)

Token structure

```
type Token struct {
    Nested      *Token
    Payload     *Payload
    Signature   [ ]byte
}
```

```
type Payload struct {
    Ver         int8
    Alg         string
    Iat         int64
    Iss         *IDClaim
    Sub         *IDClaim
    Aud         *IDClaim
}
```

```
type IDClaim struct {
    CN          string
    PK          [ ]byte
    ID          *Token
}
```

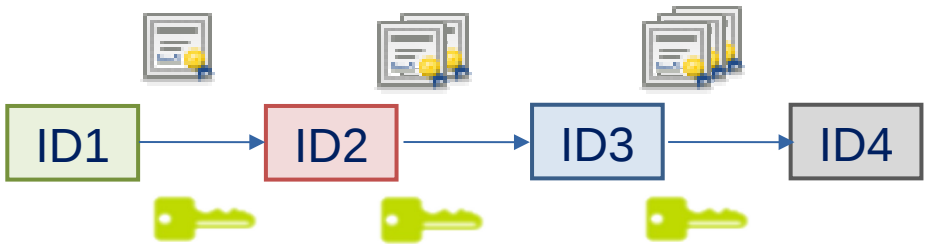
Signature schemes

ID-mode: Backed by an Identity Provider, allow **signer identification, binding the issuer to an unique audience**

Anonymous mode: Uses ephemeral keys and aggregation scheme to **create smaller tokens and a signature chain**

ID mode

- Identify and link **issuer** and **audience**
- **Bearer** must math the **audience** value
- Issuer claim with ID: **Signer identification & signature validation**
- Check signatures and $\mathbf{aud_i \rightarrow iss_{i+1}}$ correspondence, for all **i**

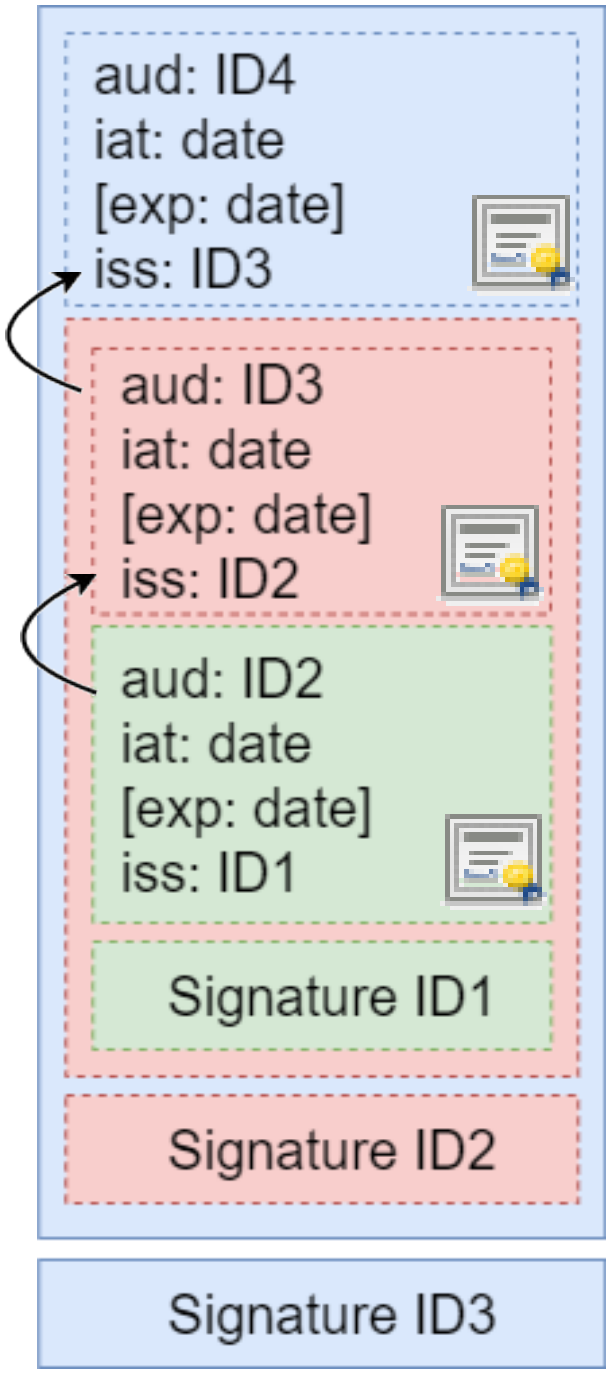


Proof of Concept: ECDSA + SHA256

ID Mode

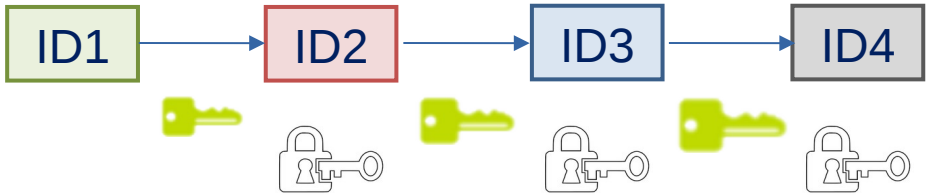
Link between issuer and audience

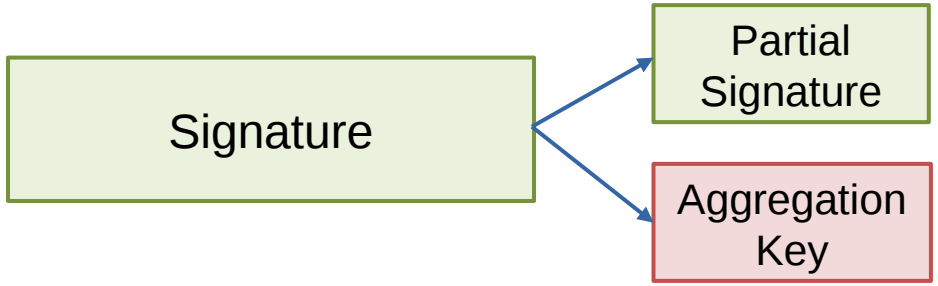
Bearer must match audience



Anonymous mode

- Does **not require audience** claim to bind sender and receiver
- Aggregate the signatures reducing the token size
- Based on **Schnorr signature concatenation (SchoCo)**



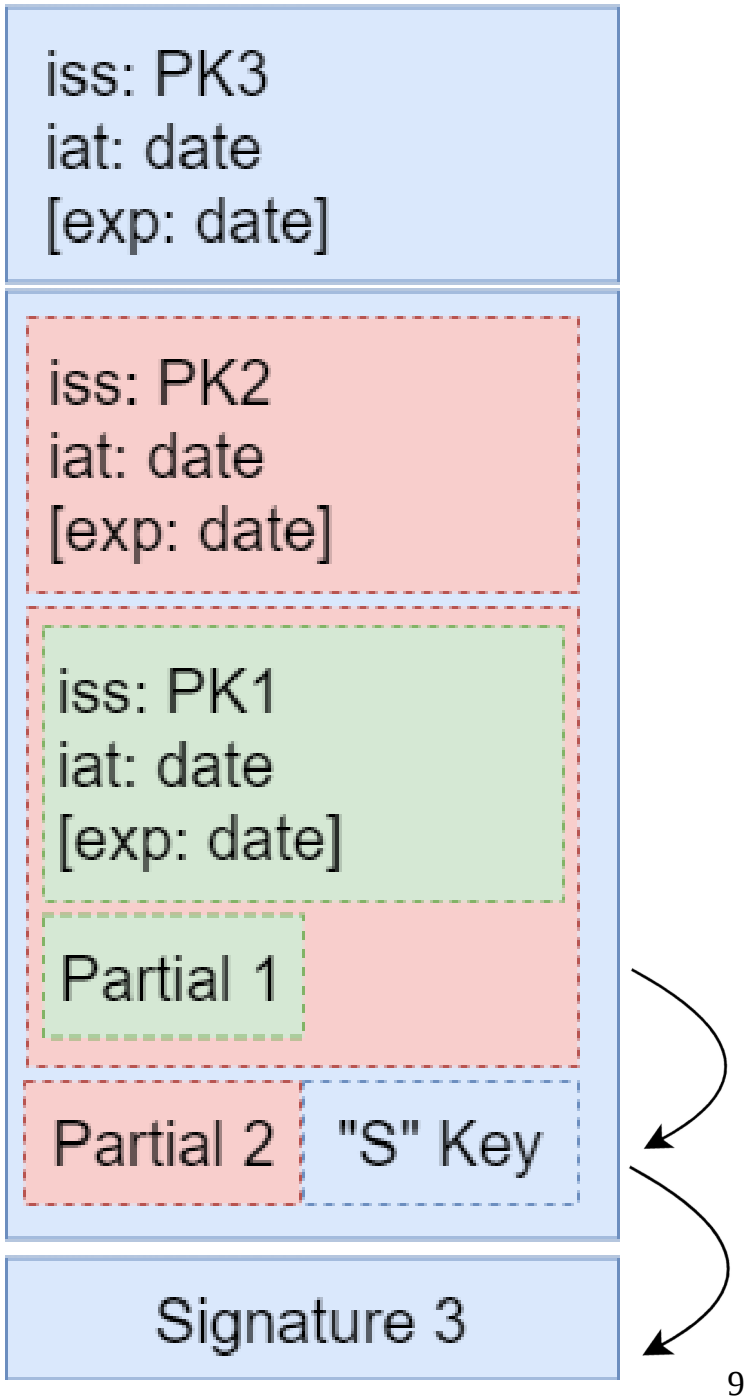


Proof of Concept: Schnorr EdDSA (Ed25519) + SHA256

Anonymous mode

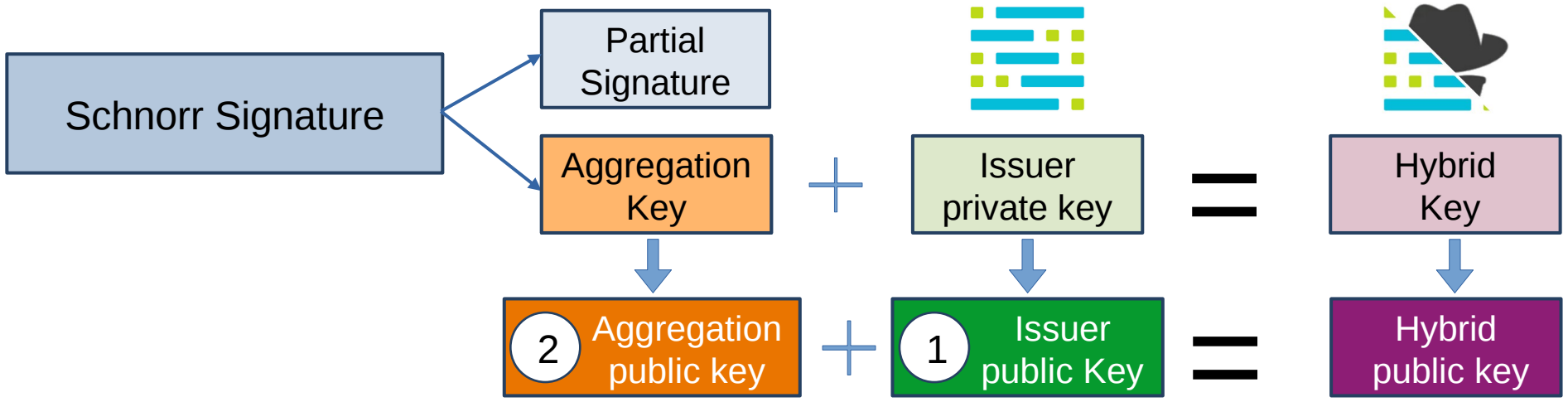
Link and aggregate signatures

Reduces up to 50% signature size



Future work: Hybrid mode

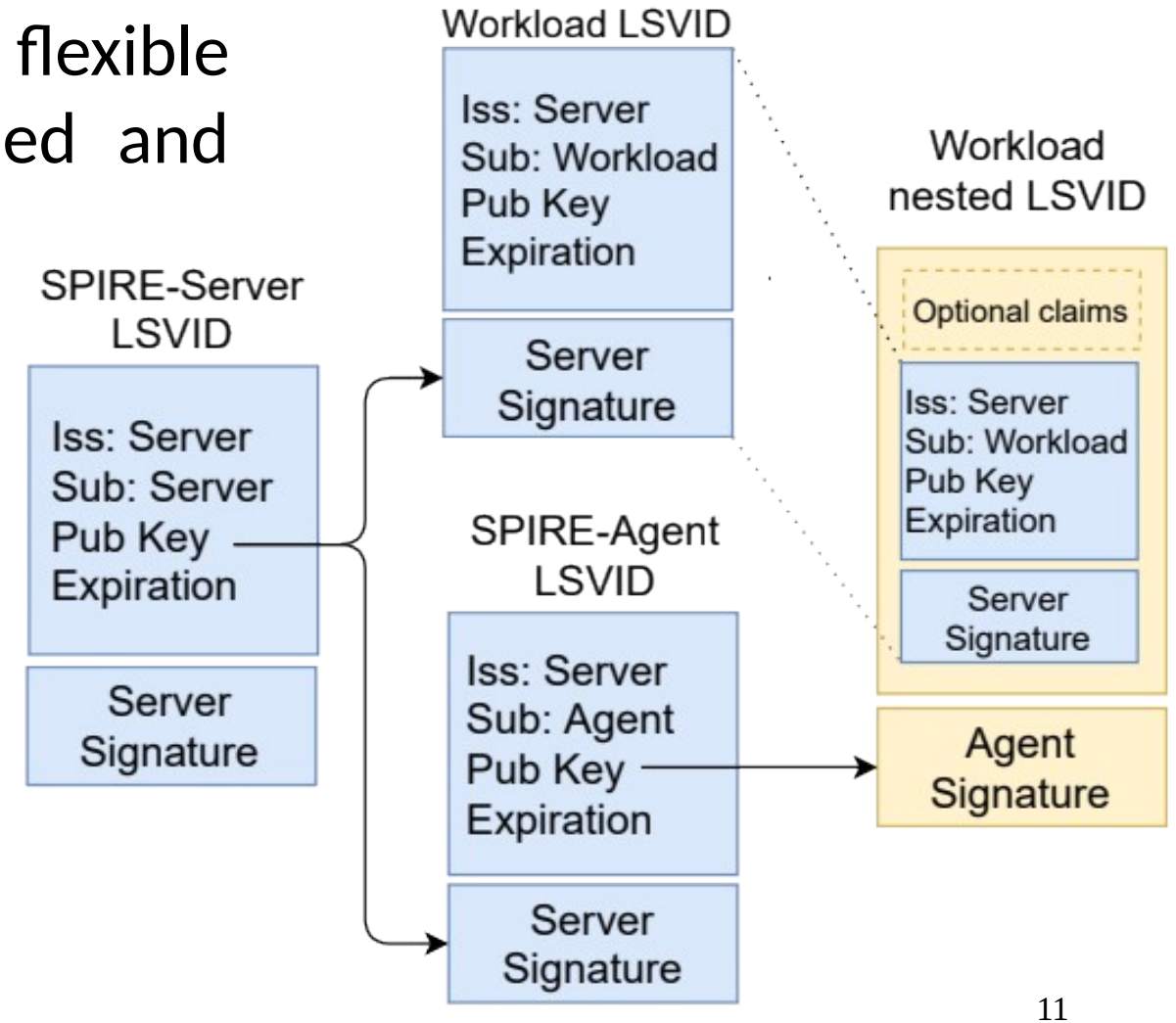
- **ID-mode with smaller tokens and signature chain**
- **Issuer must have** two values:
  1. An **ID document (ID)**, for issuer identification
  2. A **Public Key (PK)** derived from aggregation key
- Audience is optional



Use case: Lightweight SVID

Lightweight **SVID** (LSVID) is a small and flexible identity document that can be extended and used as a token

- Created by SPIRE-Server
- Can be extended to attenuate, delegate, or other application lvl functionality
- Can embed another LSVID in the Identity claims



Proof-of-Concept requirements

- **User token: Delegate** OAuth permissions to workload
- **Token tracing:** Validate the **token chain of custody**
- **Security:** Ensure **token integrity** and **link between hops**
- **Selector claims:** Add selectors from **attestation process**

References

- Nested Token Model Specification Document. https://docs.google.com/document/d/1nQYV4wf8wiogpxboIVbwtFZyZjLNRejyguHoGZIZLQM

- Lightweight Secure Verifiable Identity Document: LSVID Specification Document. https://docs.google.com/document/d/15rfAkzNTQa1ycs-fn9hyIYV5HbznPBsxB-f0vxhNJ24

Slack Channel:
https://spiffe.slack.com/archives/C03BS8JJYN4

Thanks!