Assertions and Tokens
+
Path tracing

SPIFFE/SPIRE

Nov/2022

USP

UDESC

INSTITUTO FEDERAL
Catarinense

Hewlett Packard
Enterprise

Introduction

Main needs:

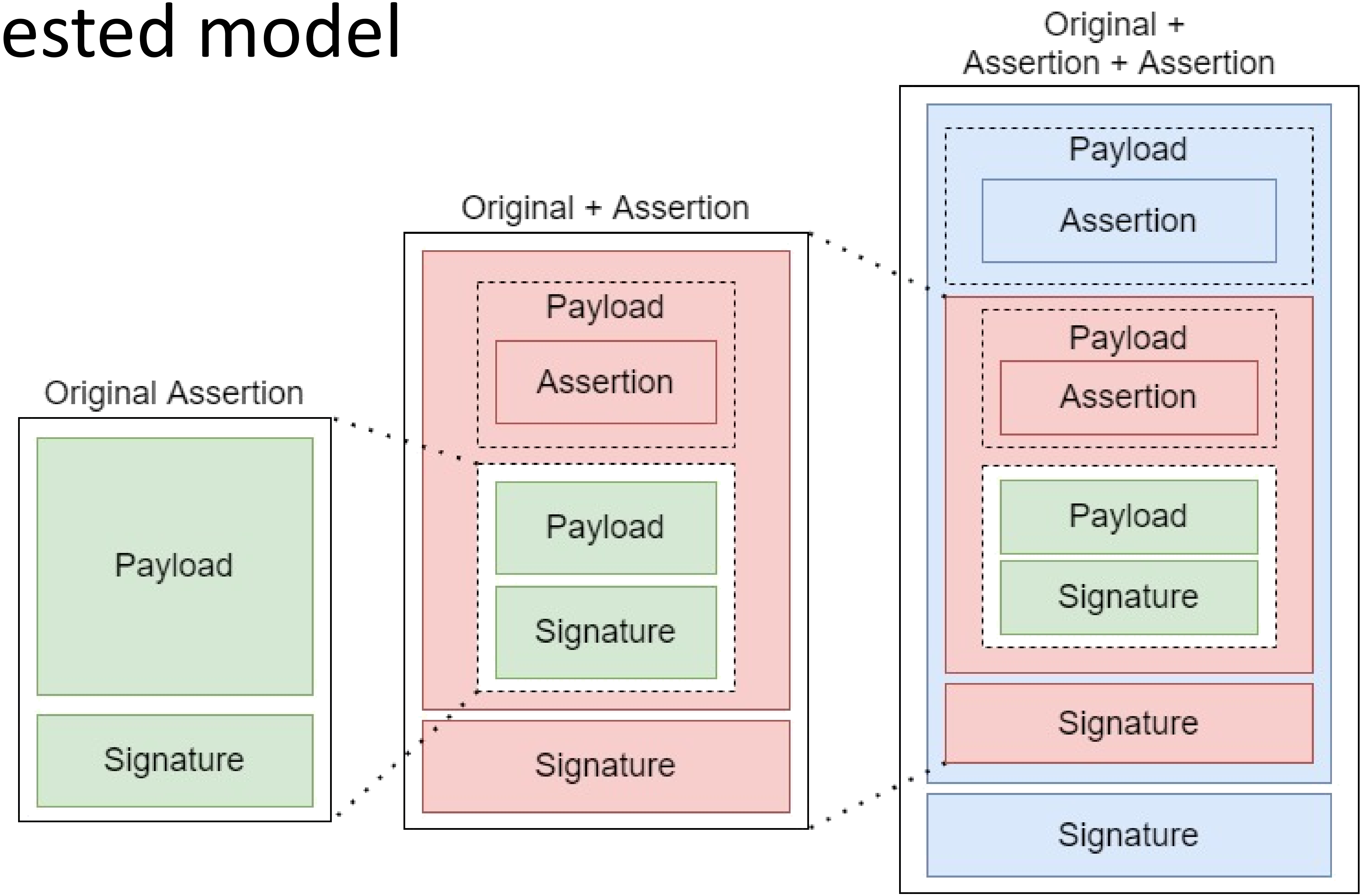
- A system that allow a subject to make arbitrary authenticated statements
- A token scheme that supports distributed signing, aggregate/concatenate signatures, and/or attenuations

Introduction – Use cases

Useful to define a minimal structure for assertions and tokens

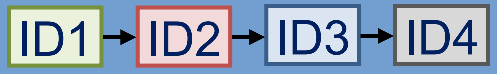
- Assert that a workload is entitled to act on behalf of a specific user
- Provide the path of workloads through which a request has passed

Nested model

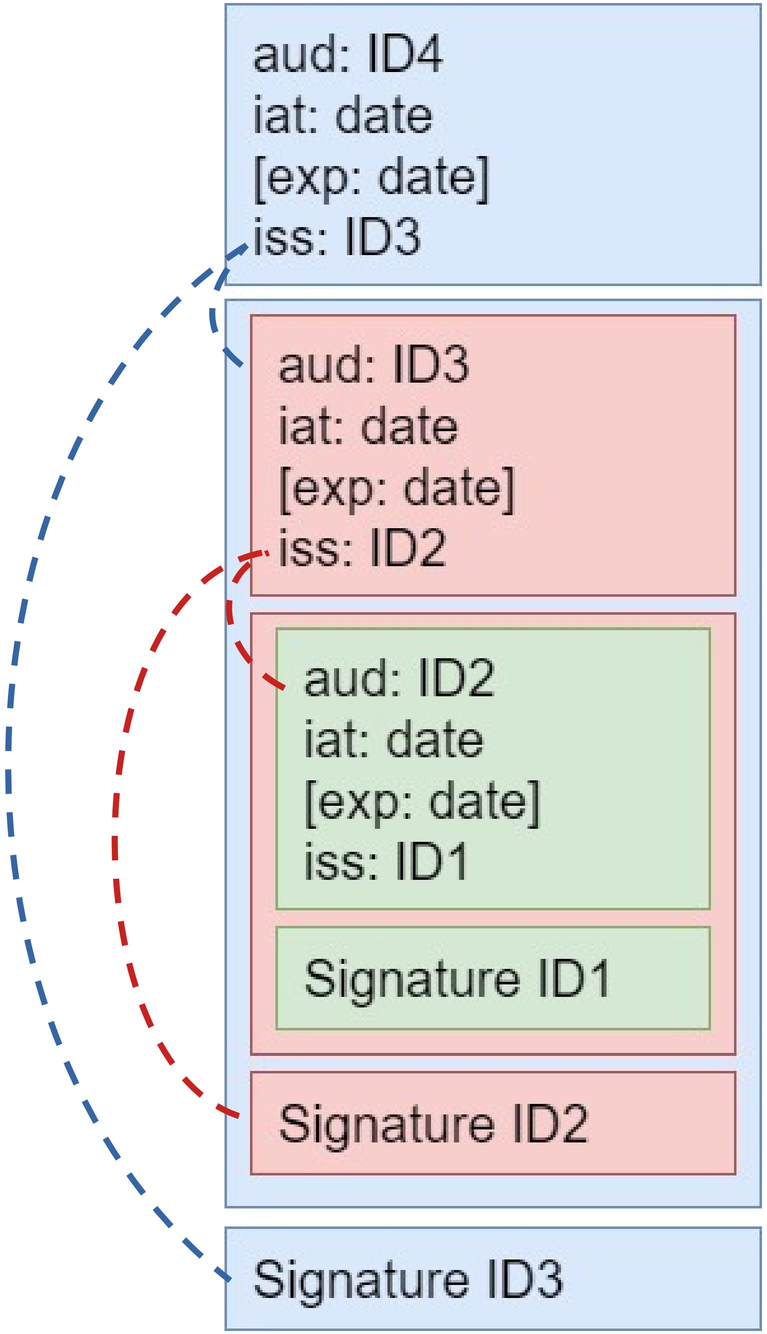


Token tracing

Link between issuer and audience



ID1 → ID2 → ID3 → ID4



aud: ID4
iat: date
[exp: date]
iss: ID3

aud: ID3
iat: date
[exp: date]
iss: ID2

aud: ID2
iat: date
[exp: date]
iss: ID1

Signature ID1

Signature ID2

Signature ID3

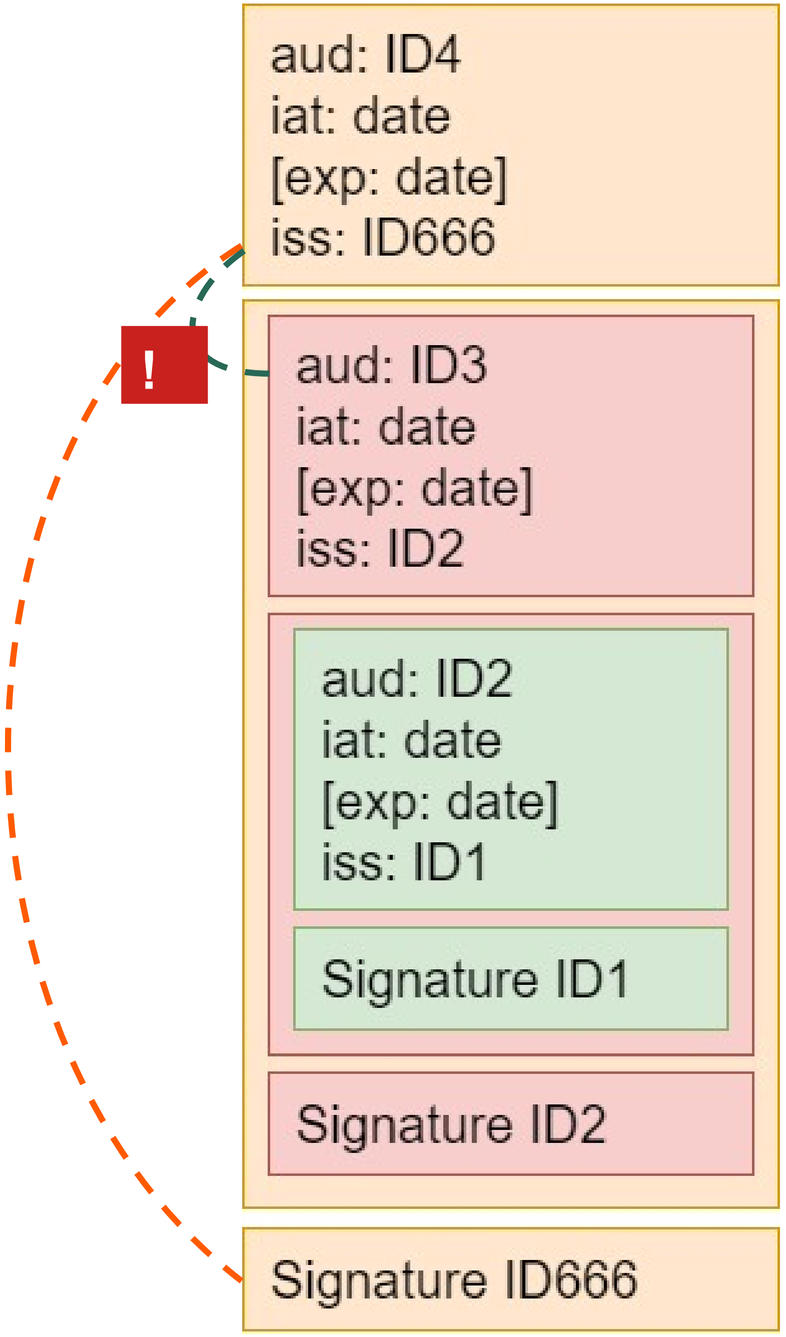
Attack model 1

Removal of last assertion

FAIL

issuer
bearer

!= audience



aud: ID4
iat: date
[exp: date]
iss: ID666

aud: ID3
iat: date
[exp: date]
iss: ID2

aud: ID2
iat: date
[exp: date]
iss: ID1

Signature ID1

Signature ID2

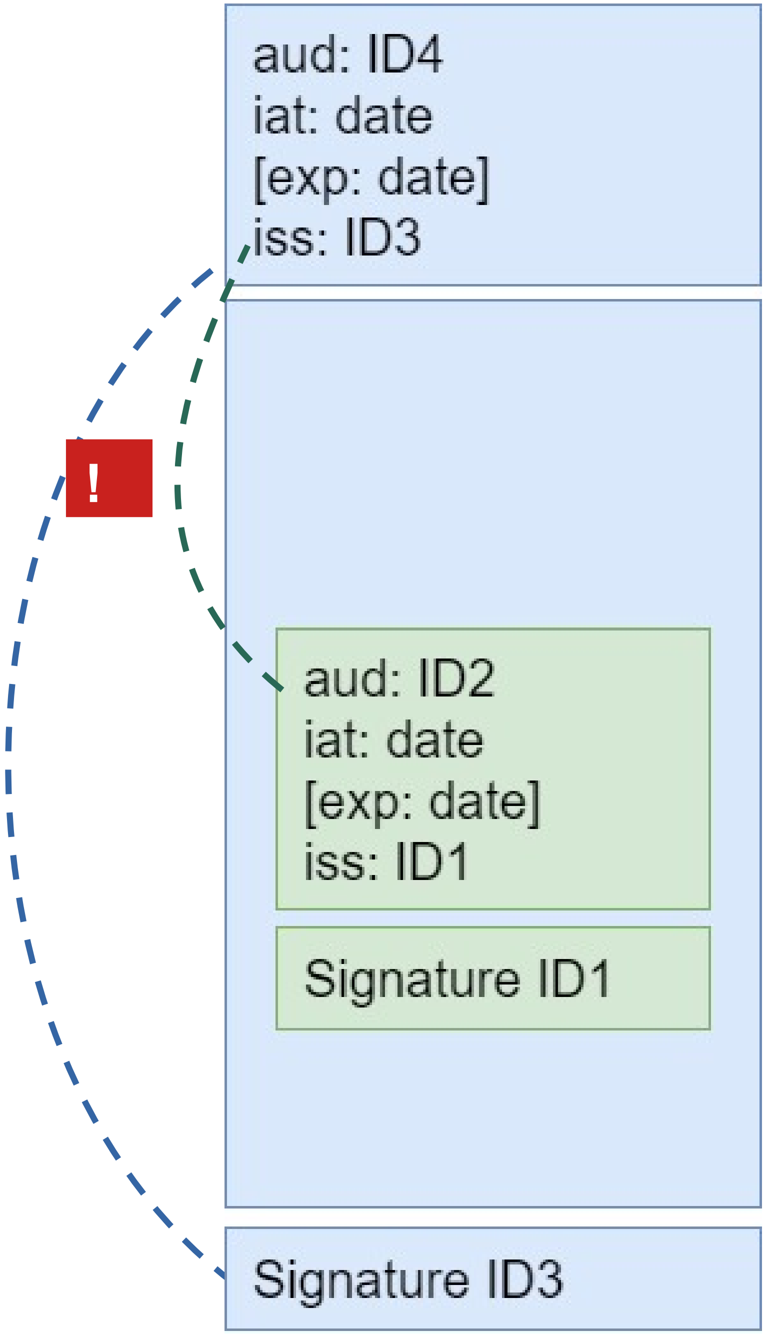
Signature ID666

Attack model 1

Removal of middle assertion

FAIL

issuer
bearer != audience



aud: ID4
iat: date
[exp: date]
iss: ID3

aud: ID2
iat: date
[exp: date]
iss: ID1

Signature ID1

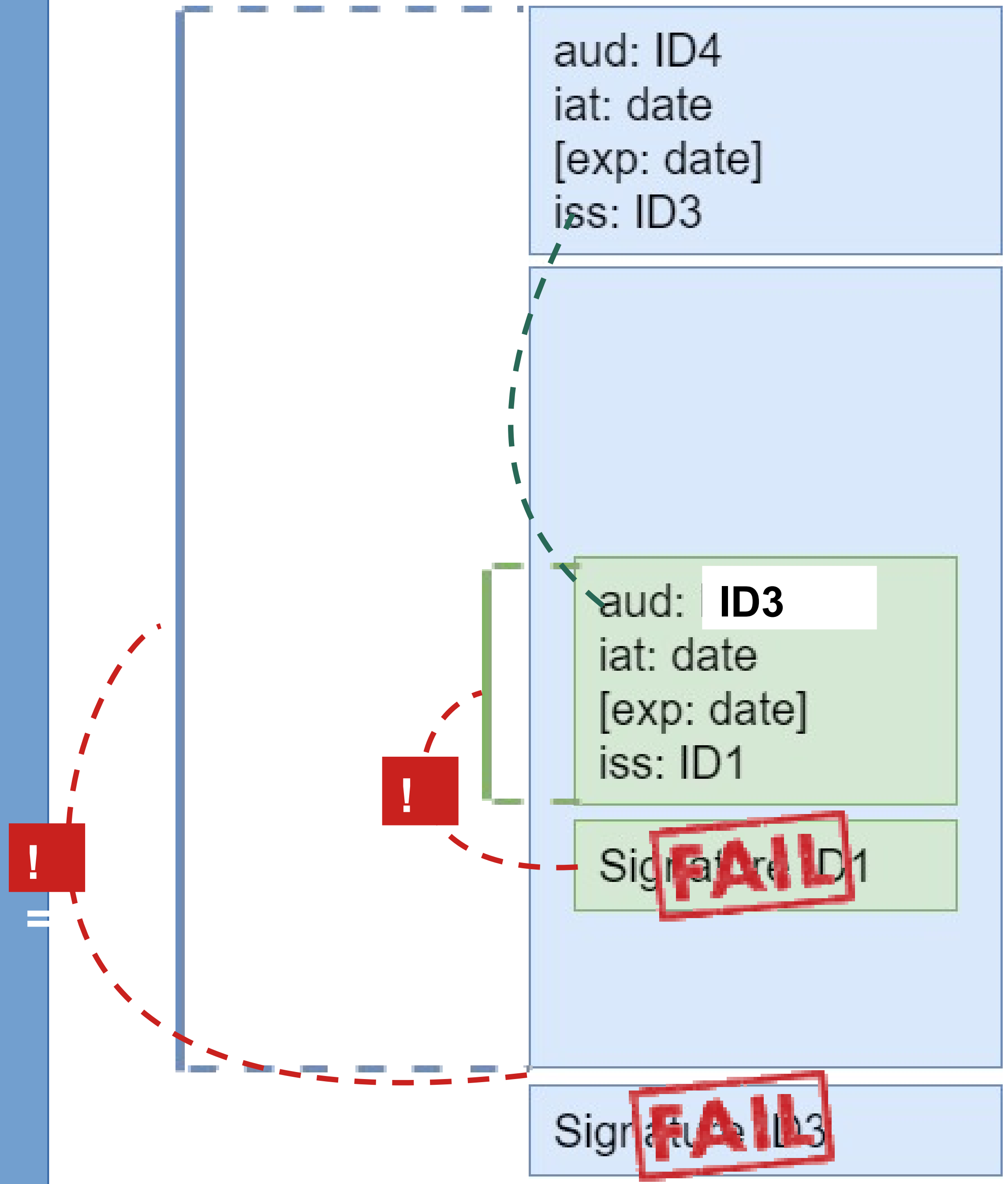
Signature ID3

Attack model 2

Token modification

FAIL

Hash chaining



aud: ID4
iat: date
[exp: date]
iss: ID3

aud: ID3
iat: date
[exp: date]
iss: ID1

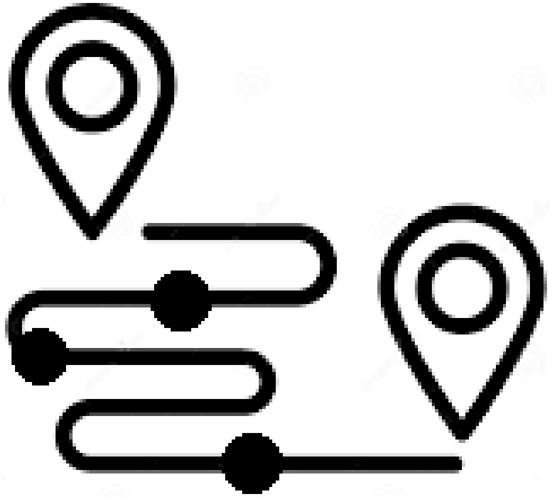
Signature ID1

FAIL

Signature ID3

FAIL

Token path tracing

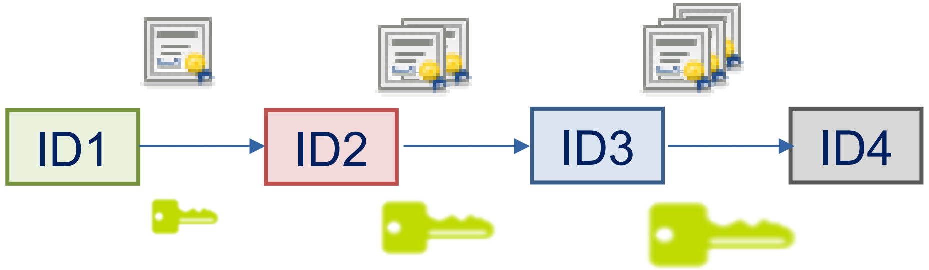


Provide the path of workloads that a request has passed

- **ID mode**:
  - Uses SVID private key to sign, sending necessary certificates to identify the workload and validate the signature and iss/aud link
- **Anonymous mode**:
  - No ID associated to keys
  - Uses concatenated Schnorr signatures that results in smaller tokens and faster validation

ECDSA – SVID

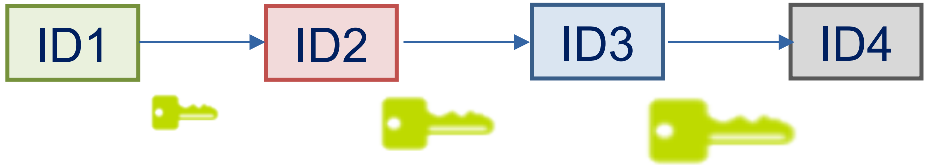
(ID mode)



Sign with SVID private key. Send SVID certificates with token

- Pros:
  - Certificates allow off-line validation and identification
  - Anonymous mode also available
- Cons:
  - ID mode requires more bandwidth
- Possibilities:
  - Use lightweight SVID

ECDSA – SVID
(Anonymous mode)



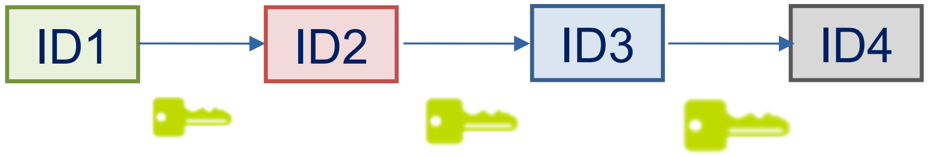
Sign with SVID private key. Add public keys in *iss/aud* claims

Pros:

- Uses SPIFFE/SPIRE infra

- Cons:
  - Token size
  - Validation runtime
- Possibilities:
  - Use Schnorr signature algorithm

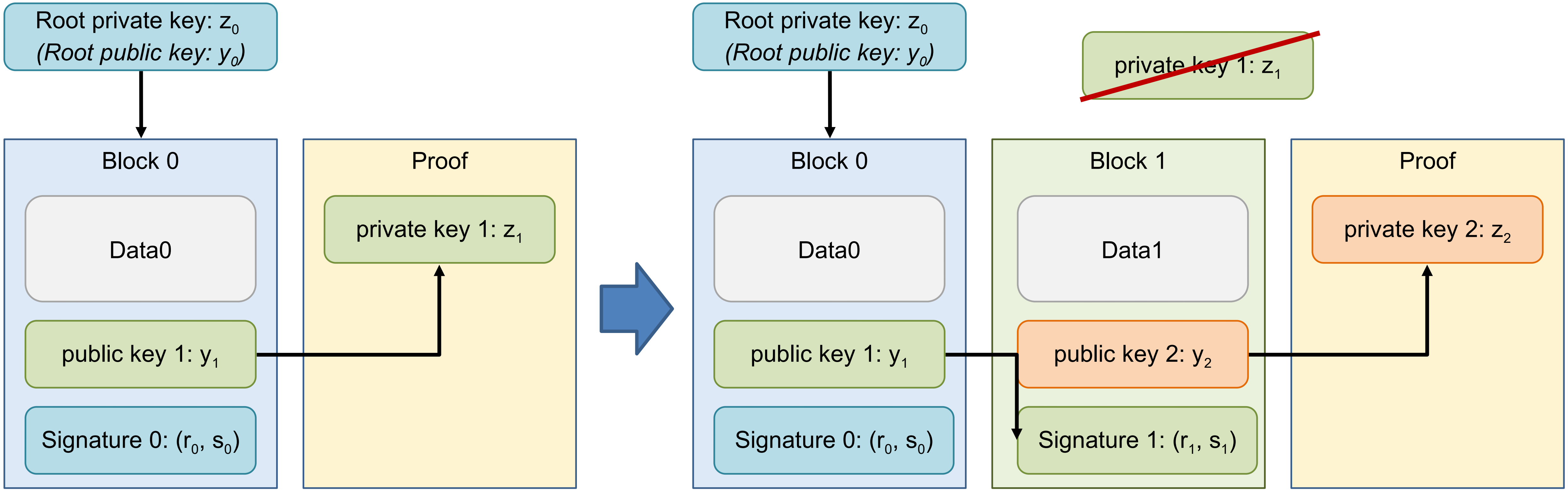
EdDSA – Schnorr Concatenated



Biscuits-based solution. Each hop uses part of previous signature as private key

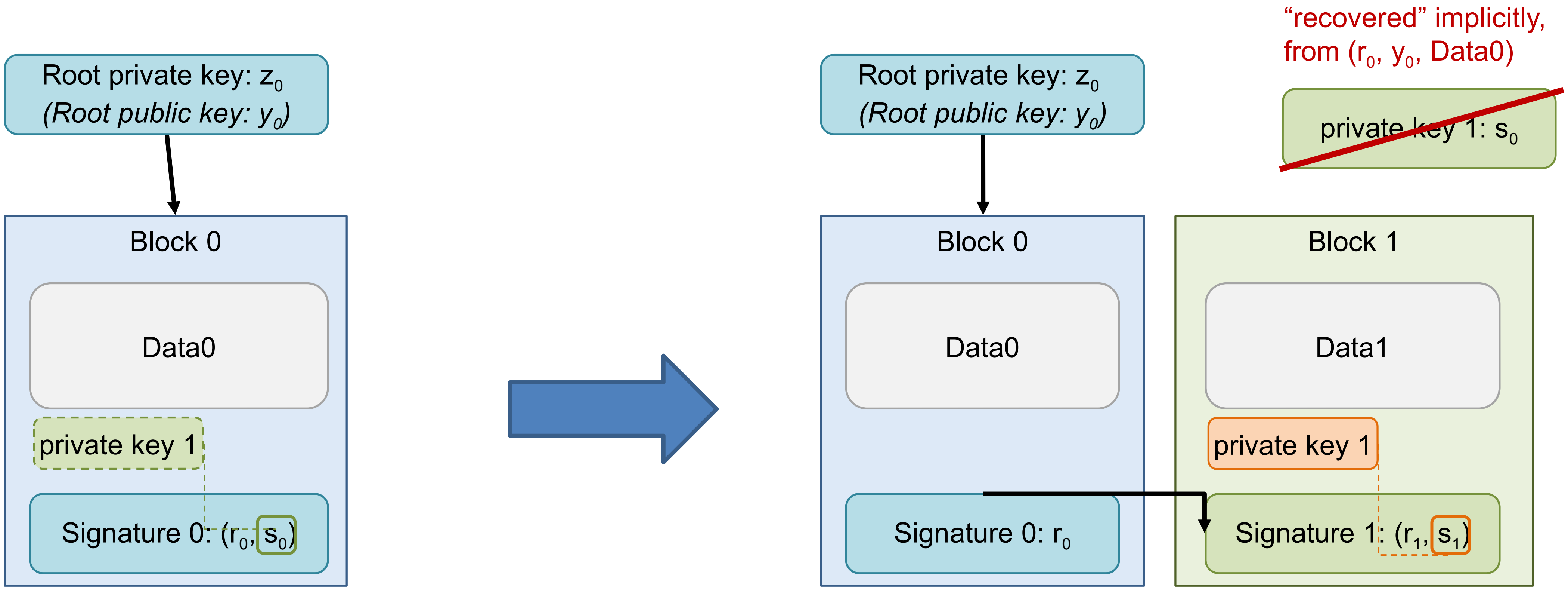
- Pros:
  - Smaller token size (compared to standard model and ECDSA)
  - Faster validation (using Galindo-Garcia) than sequencial model
  - Cryptographic-linked signatures
- Cons:
  - Only anonymous mode available
- Possibilities:
  - Study aggregated signatures state-of-art and ECDSA-Schnorr

Biscuits model reference

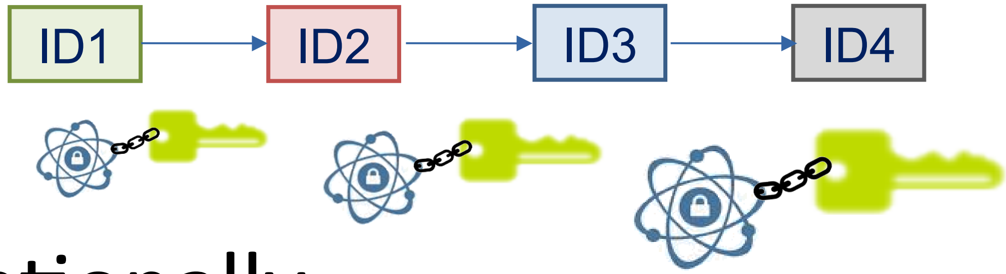


SchCo-Biscuits

(using concatenated Schnorr-based signatures: Galindo-Garcia-style)


Root private key: z_0
(Root public key: y_0)
Block 0
Data0
private key 1
Signature 0: (r_0, s_0)
Root private key: z_0
(Root public key: y_0)
"recovered" implicitly, from (r_0, y_0, Data0)
~~private key 1: s_0~~
Block 0
Data0
Signature 0: r_0
Block 1
Data1
private key 1
Signature 1: (r_1, s_1)

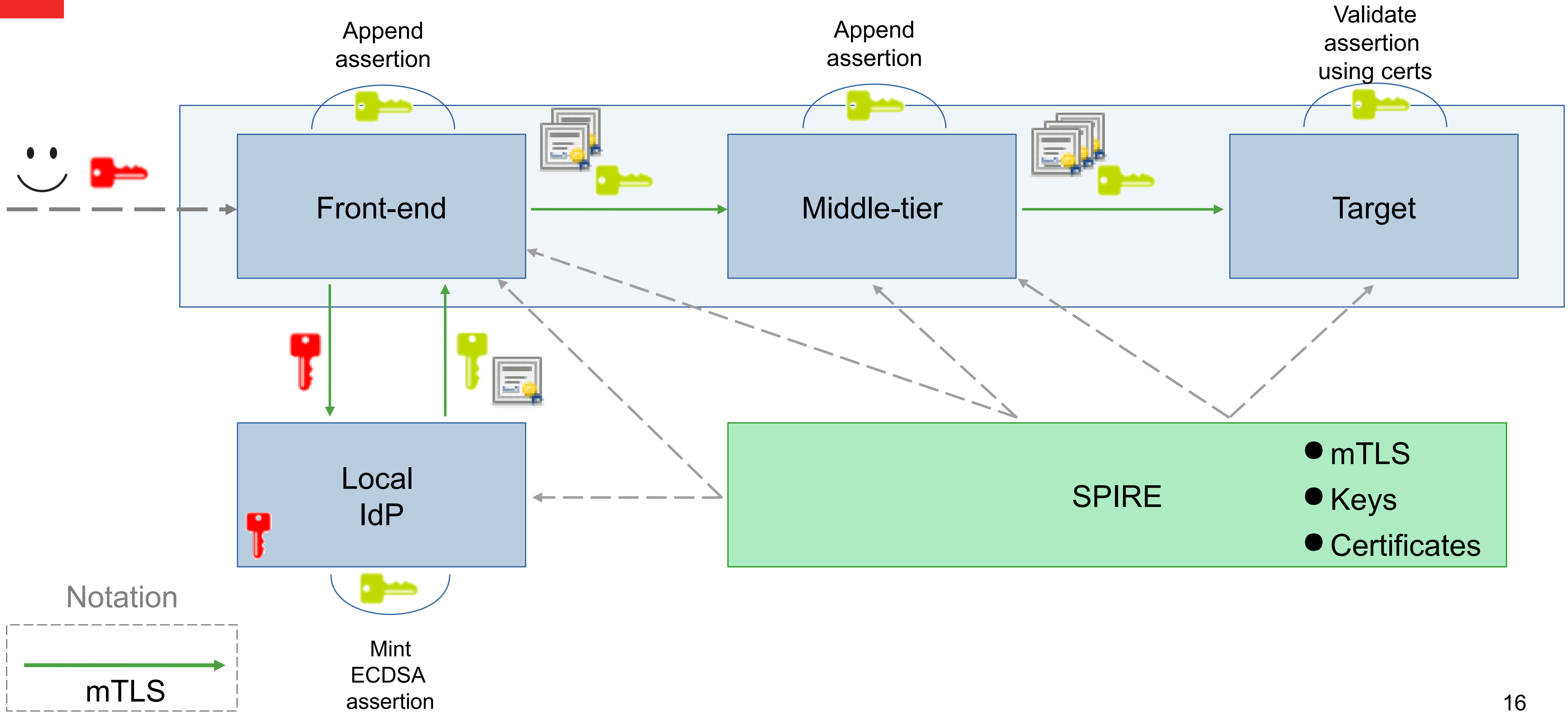
ECDSA – Dillithium



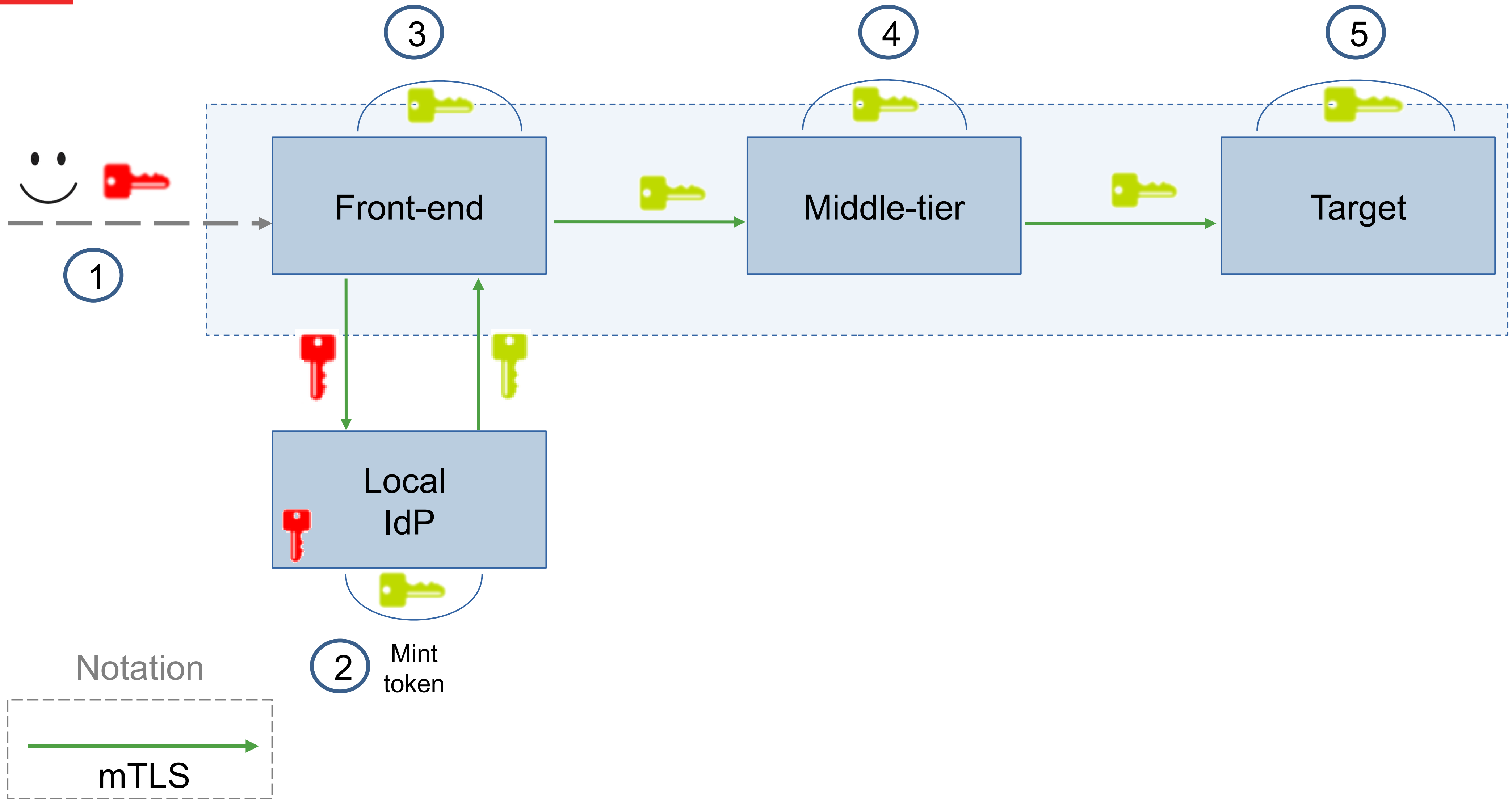
Sign with SVID private key adding, optionally, a post-quantum signature algorithm.

- Pros:
  - Improved security using post-quantum algorithm (ECDSA+Crystals)
- Cons:
  - Bigger keys/signatures
- Possibilities:
  - Optional to specific use cases
  - Follow-up state-of-art

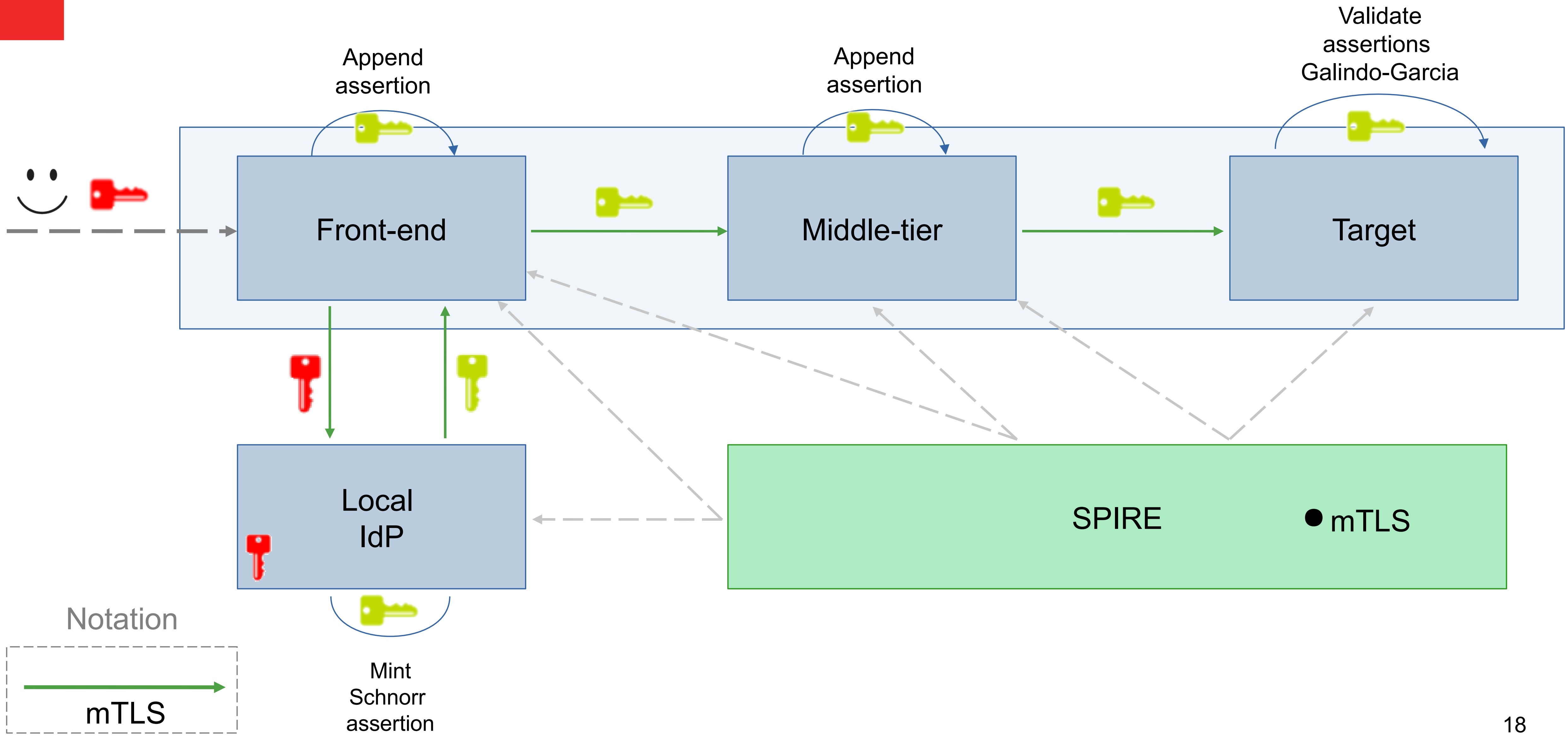
Demo 1: ECDSA – SVID (ID mode)



Demo 1: ECDSA – SVID (ID mode)



Demo 2: EdDSA – Schnorr (Anonymous mode)

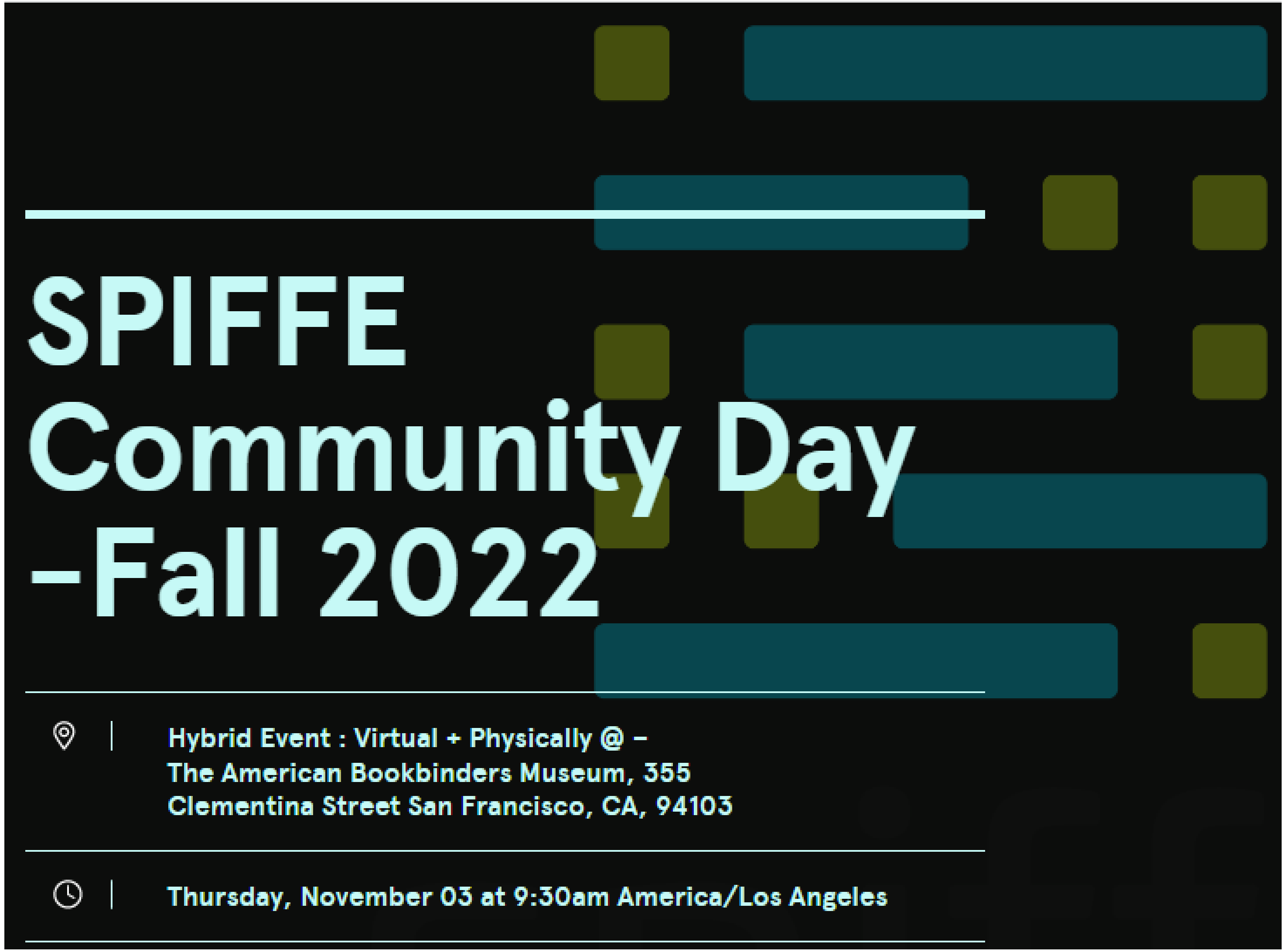


Demo 2: ECDSA – Dilithium

Prototype that generates 2 tokens:
ECDSA and Dilithium

SPIFFE Community Day

Opportunity to present the work to community and get feedbacks :)

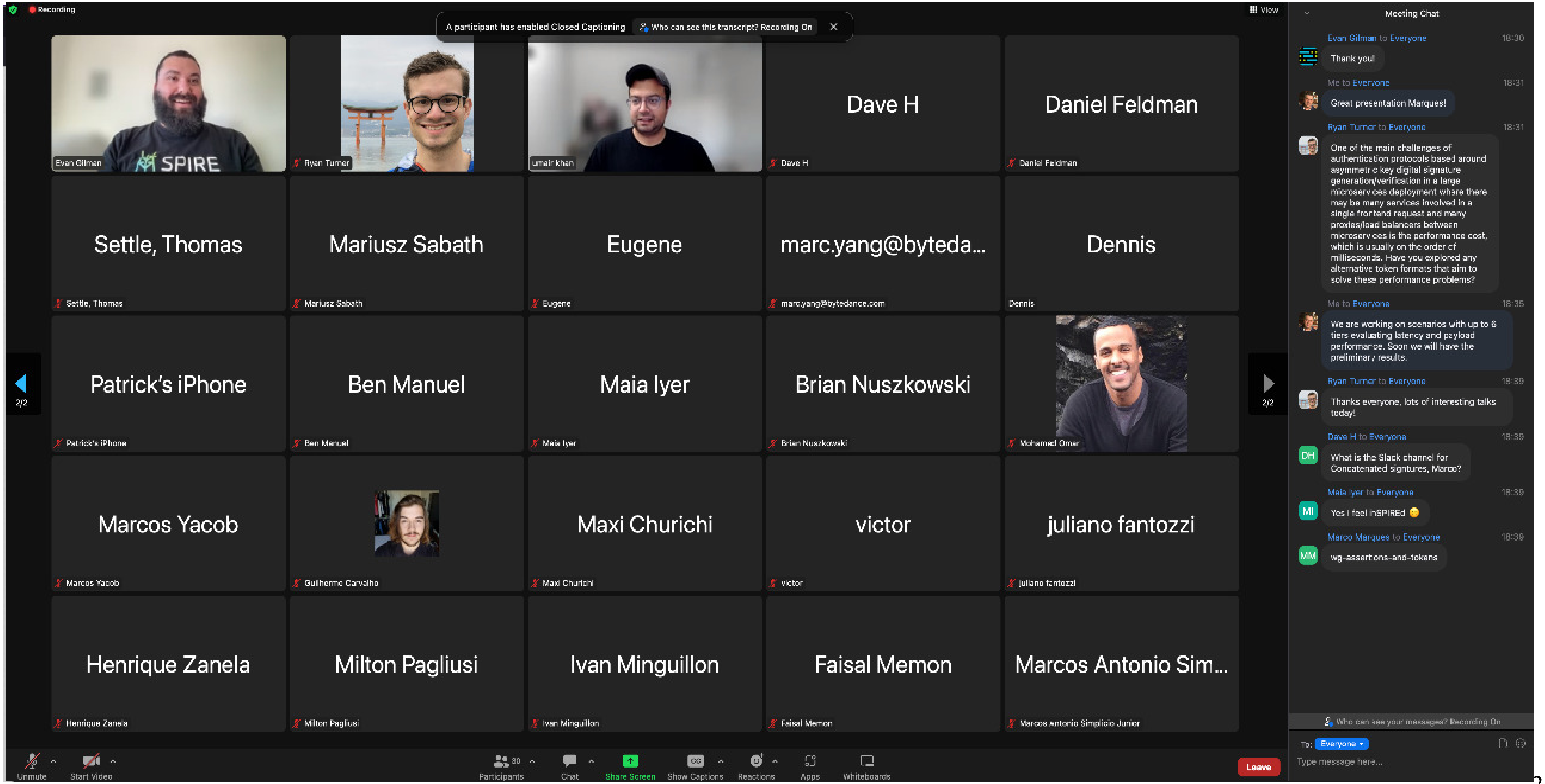


SPIFFE Community Day –Fall 2022

Hybrid Event : Virtual + Physically @ –
The American Bookbinders Museum, 355
Clementina Street San Francisco, CA, 94103

Thursday, November 03 at 9:30am America/Los Angeles

SPIFFE Community Day



Meeting Chat

Evan Gilman to Everyone 18:30
Thank you!

Me to Everyone 18:31
Great presentation Marques!

Ryan Turner to Everyone 18:31
One of the main challenges of authentication protocols based around asymmetric key digital signature generation/verification in a large microservices deployment where there may be many services involved in a single frontend request and many proxies/load balancers between microservices is the performance cost, which is usually on the order of milliseconds. Have you explored any alternative token formats that aim to solve these performance problems?

Me to Everyone 18:35
We are working on scenarios with up to 6 tiers evaluating latency and payload performance. Soon we will have the preliminary results.

Ryan Turner to Everyone 18:39
Thanks everyone, lots of interesting talks today!

Dave H to Everyone 18:39
What is the Slack channel for Concatenated signtures, Marco?

Maia Iyer to Everyone 18:39
Yes I feel inSPIREd 🫠

Marco Marques to Everyone 18:39
wg-assertions-and-tokens

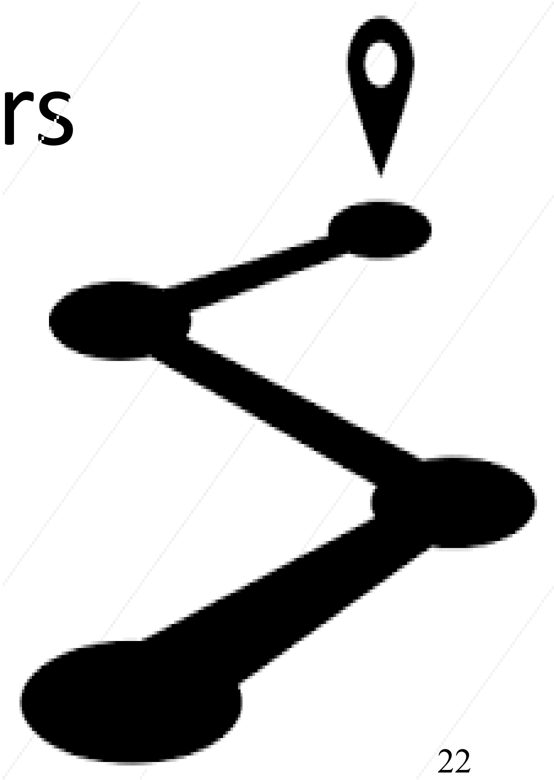
Who can see your messages? Recording On

To: Everyone

Type message here...

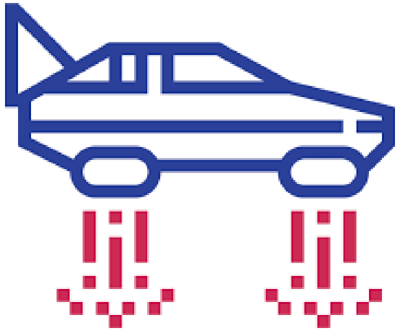
Next Steps

- Add proxy to PoC scenario
- Generate assertions using SPIRE selectors
- General solution benchmarks



Future Work

- Specify and implement lightweight SVID
- Identity-based SVID: lightweight SVID with Galindo-Garcia
- Post-Quantum algorithms (e.g. Crystals) analysis
- Protobuf / JSON analysis



WHO? WHERE?
WHEN? WHY? HOW?
HOW? WHAT? WHO?
WHERE?
WHO? WHERE?
WHAT?
WHY? WHAT?
WHEN?
WHERE? WHO?
HOW? WHAT?
WHERE?
WHY?
WHO? WHEN?
WHAT?
WHO? WHY? HOW?
HOW? WHERE?
WHY?
WHO? WHAT?
HOW?
WHAT? WHEN?
HOW? WHEN?
WHAT?
WHY? WHERE?
WHEN? HOW?
WHERE?