Lightweight tokens and path tracing

Marco Antonio Marques

PhD Student – Universidade de São Paulo

Escola Politécnica

USP

UDESC

INSTITUTO FEDERAL
Catarinense

Hewlett Packard
Enterprise

Agenda

- Introduction and objectives
- Nested model scheme
- Token path tracing models
- Demonstration

Introduction

Assertions (or "claims") have long been a debated topic in the SPIFFE community

Main needs:

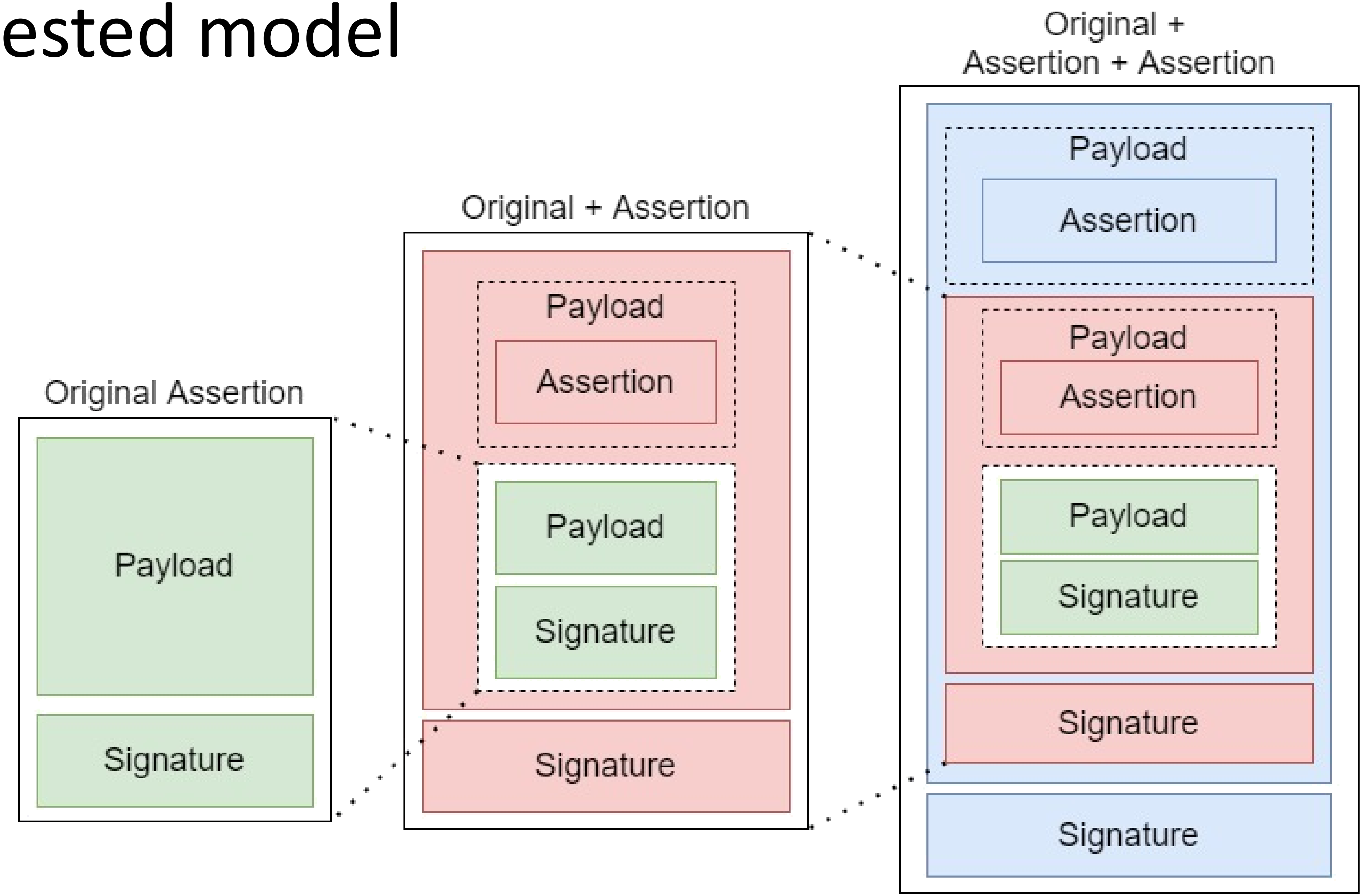
- A system by which a subject can make arbitrary authenticated statements
- A token scheme supporting distributed signing, and the ability to aggregate/concatenate signatures and/or attenuations

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

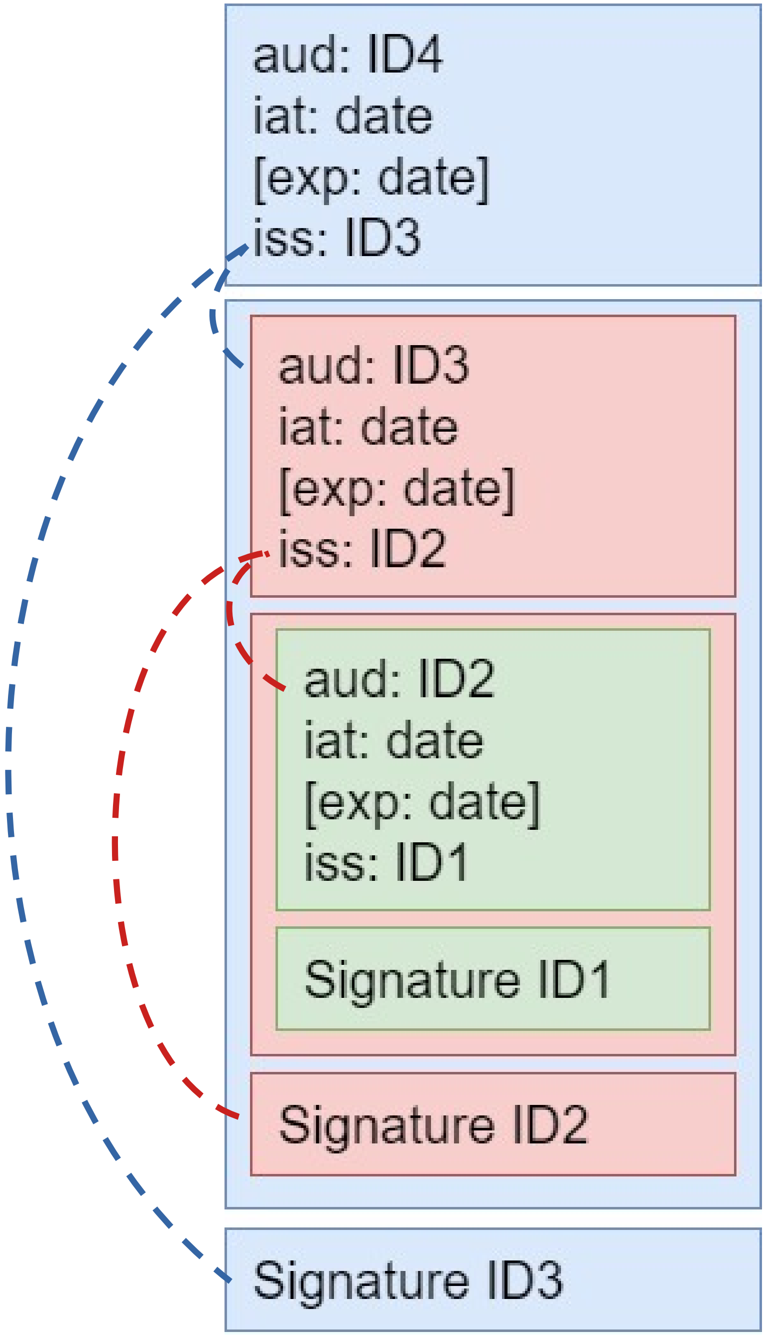
Nested model



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

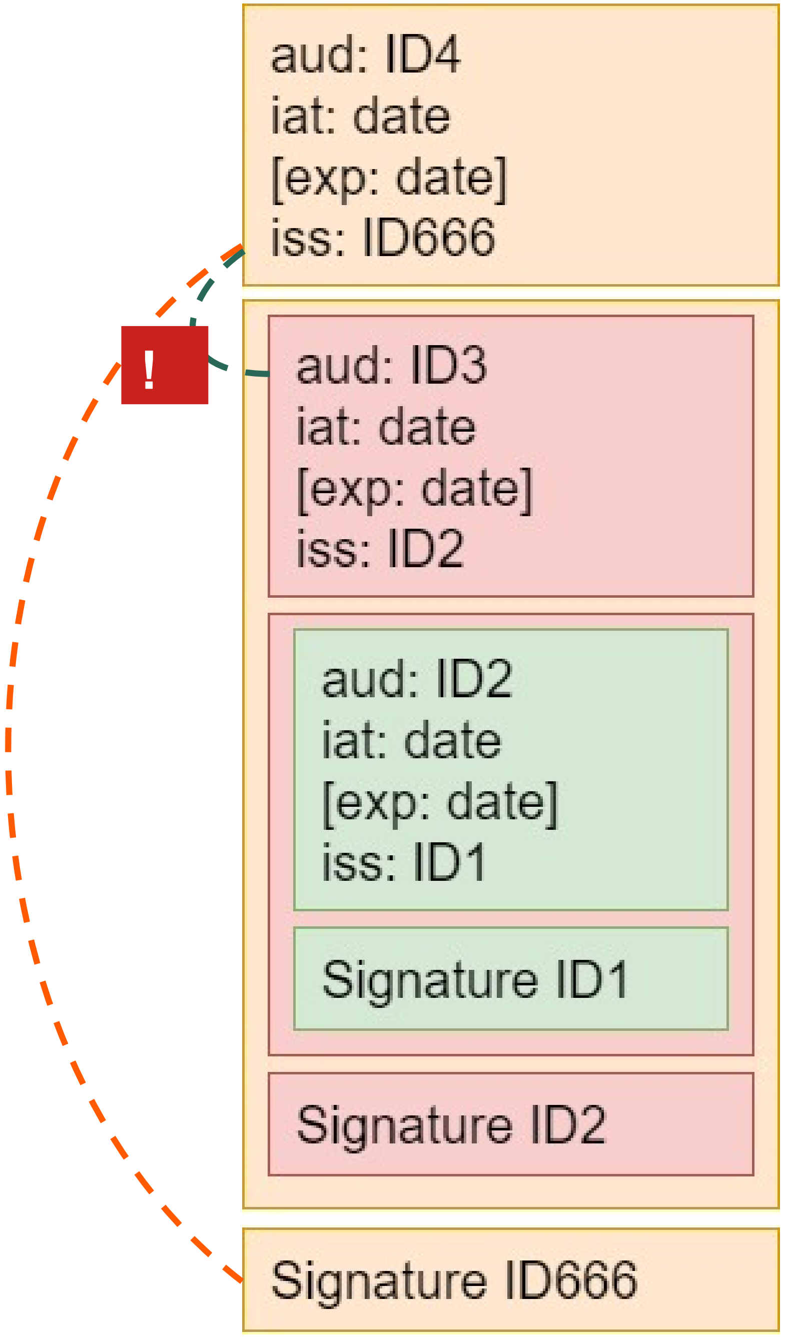
Attack model 1

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

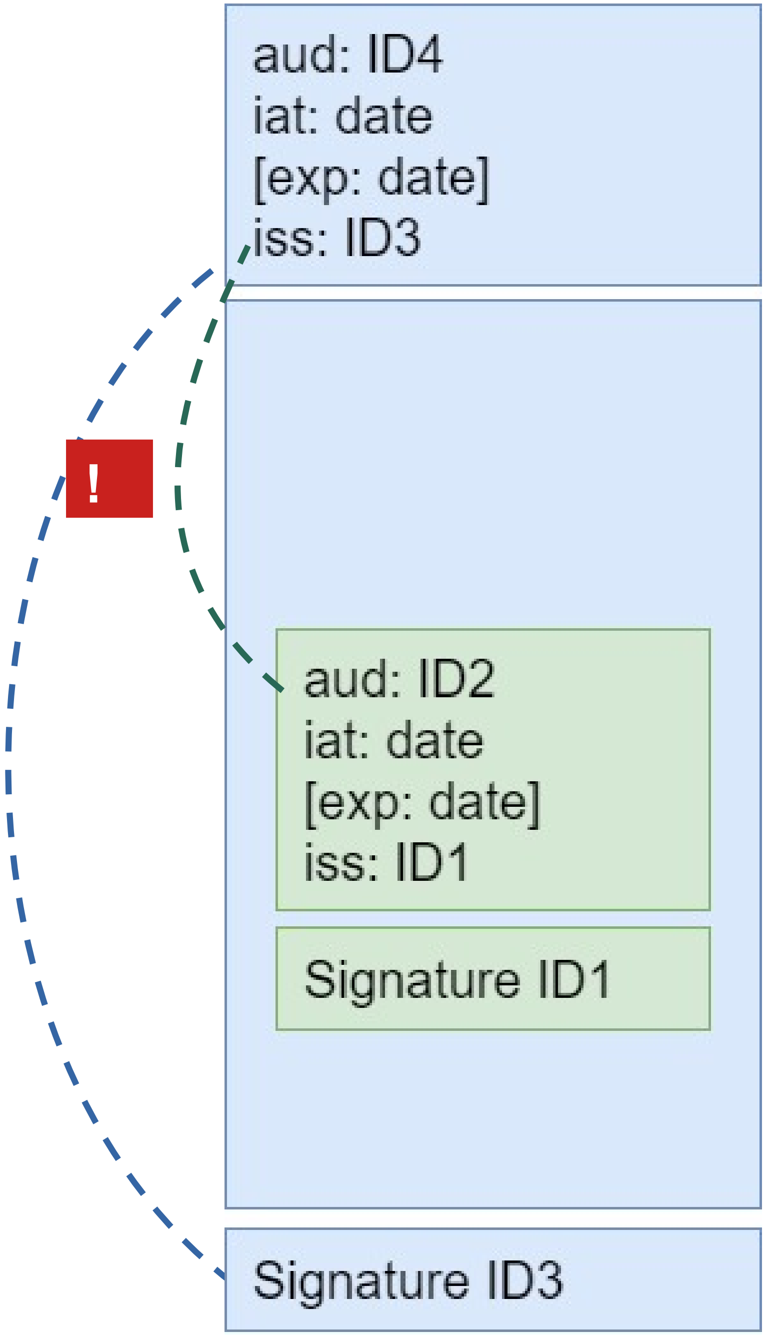
Attack model 1

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

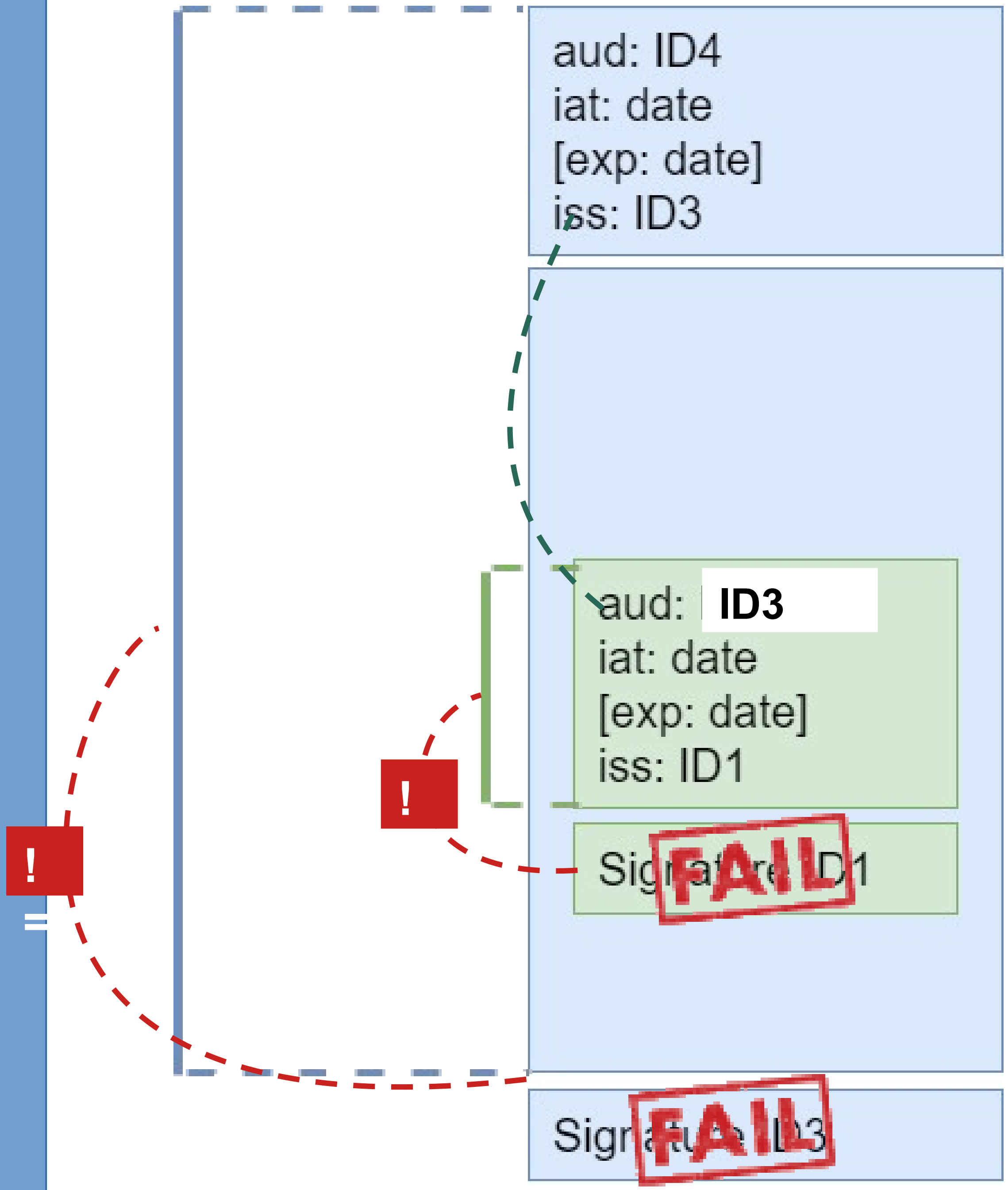
Signature ID3

Attack model 2

Token modification

FAIL

Hash chaining

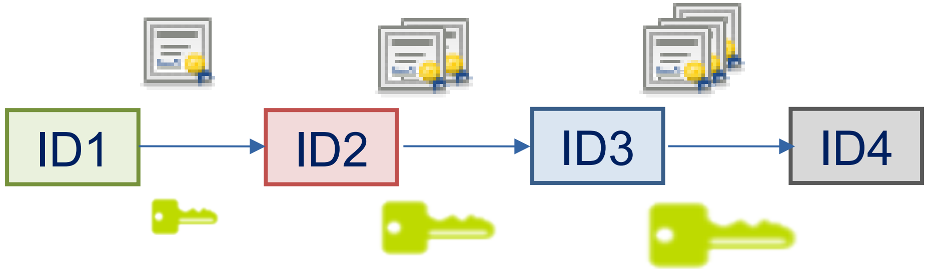


Token path tracing

Provide the path of workloads through which 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

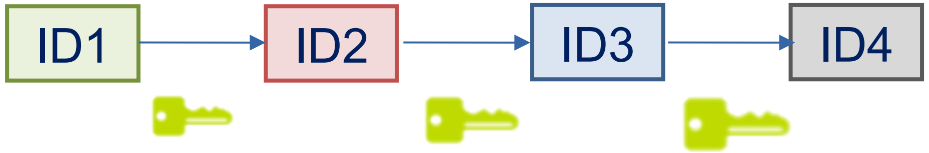
ECDSA – SVID (ID mode)



Sign with SVID private key and 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

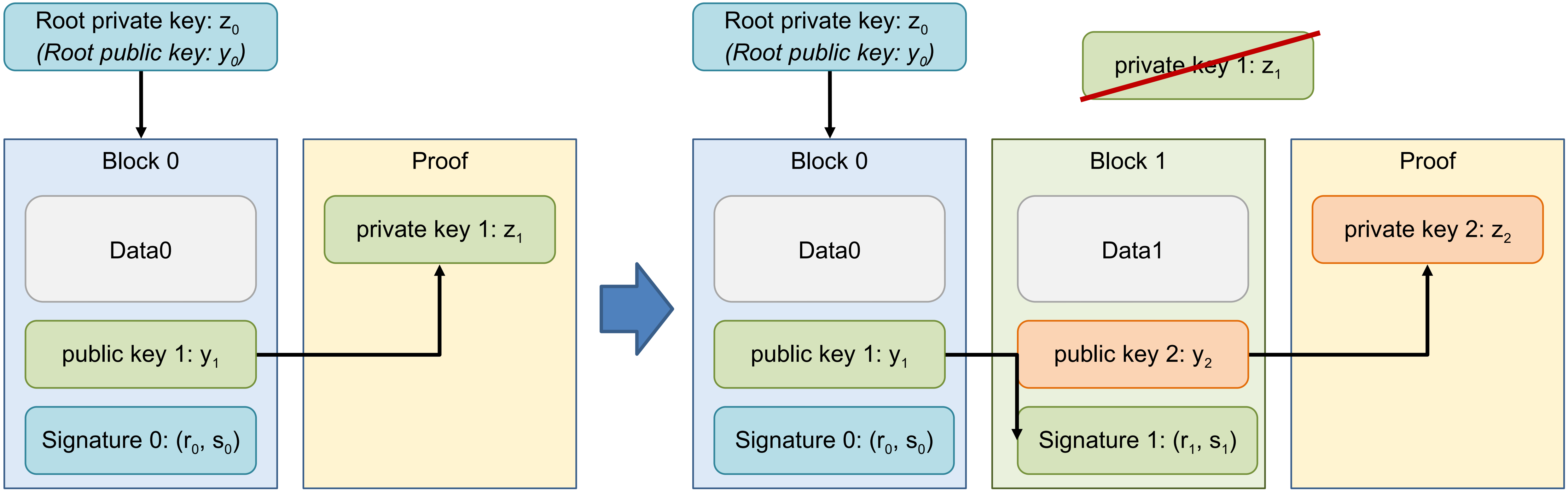
EdDSA – Schnorr Concatenated



SchCo-biscuits. Biscuits-based solution, where each hop uses part of previous signature as private key

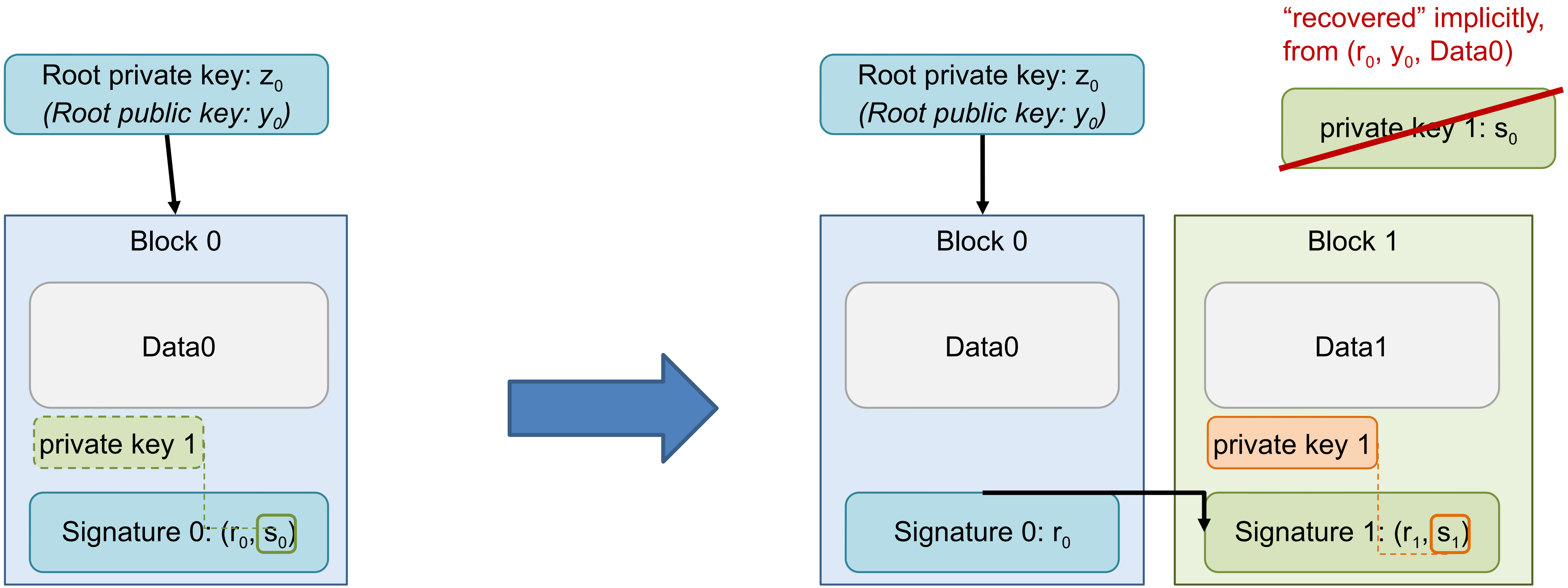
- Pros:
  - Smaller token size when compared to standard model
  - Faster validation (using Galindo-Garcia) than sequencial model
  - Cryptographic-linked signatures
- Cons:
  - Only anonymous mode available
- Possibilities:
  - Study aggregated signatures state-of-art and ECDSA-Schnorr

Biscuits model



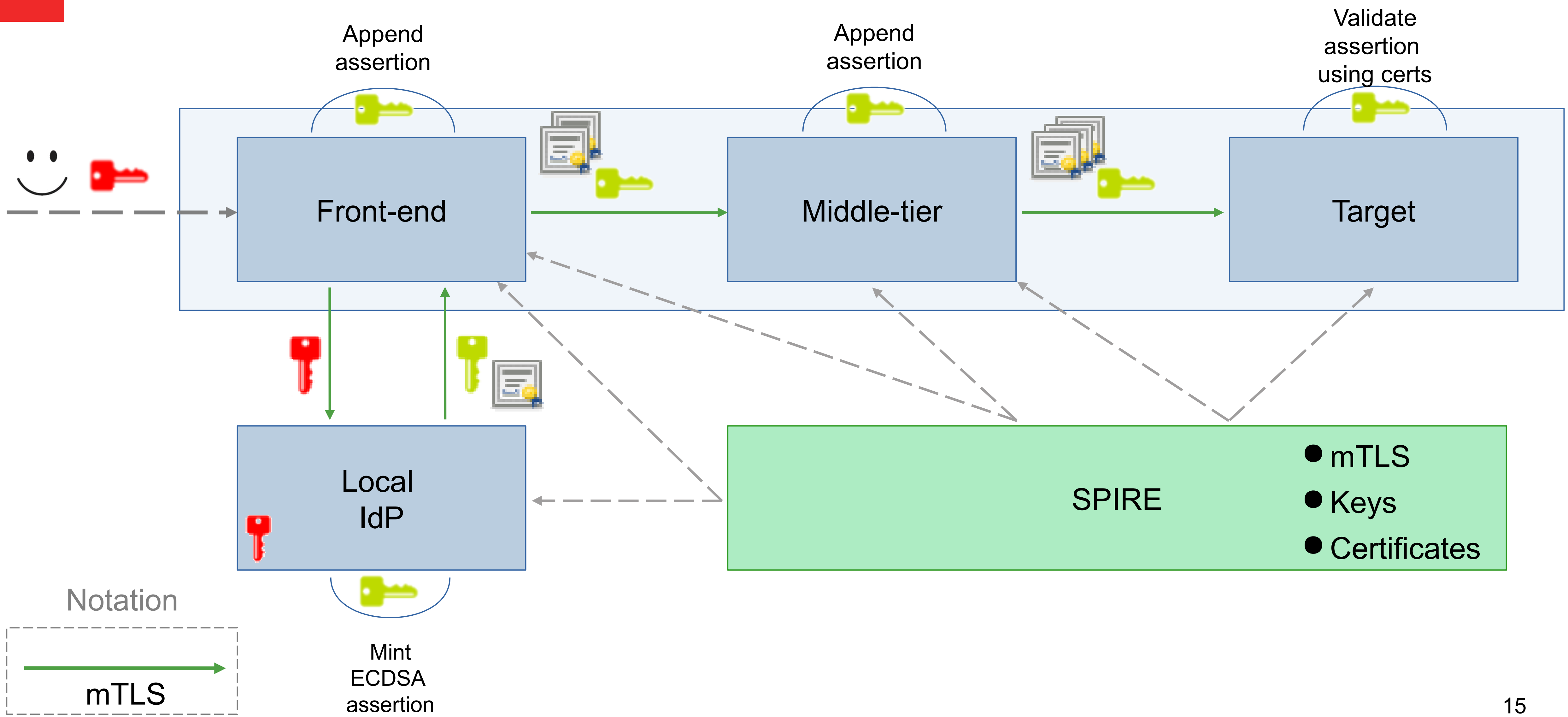
SchCo-Biscuits

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

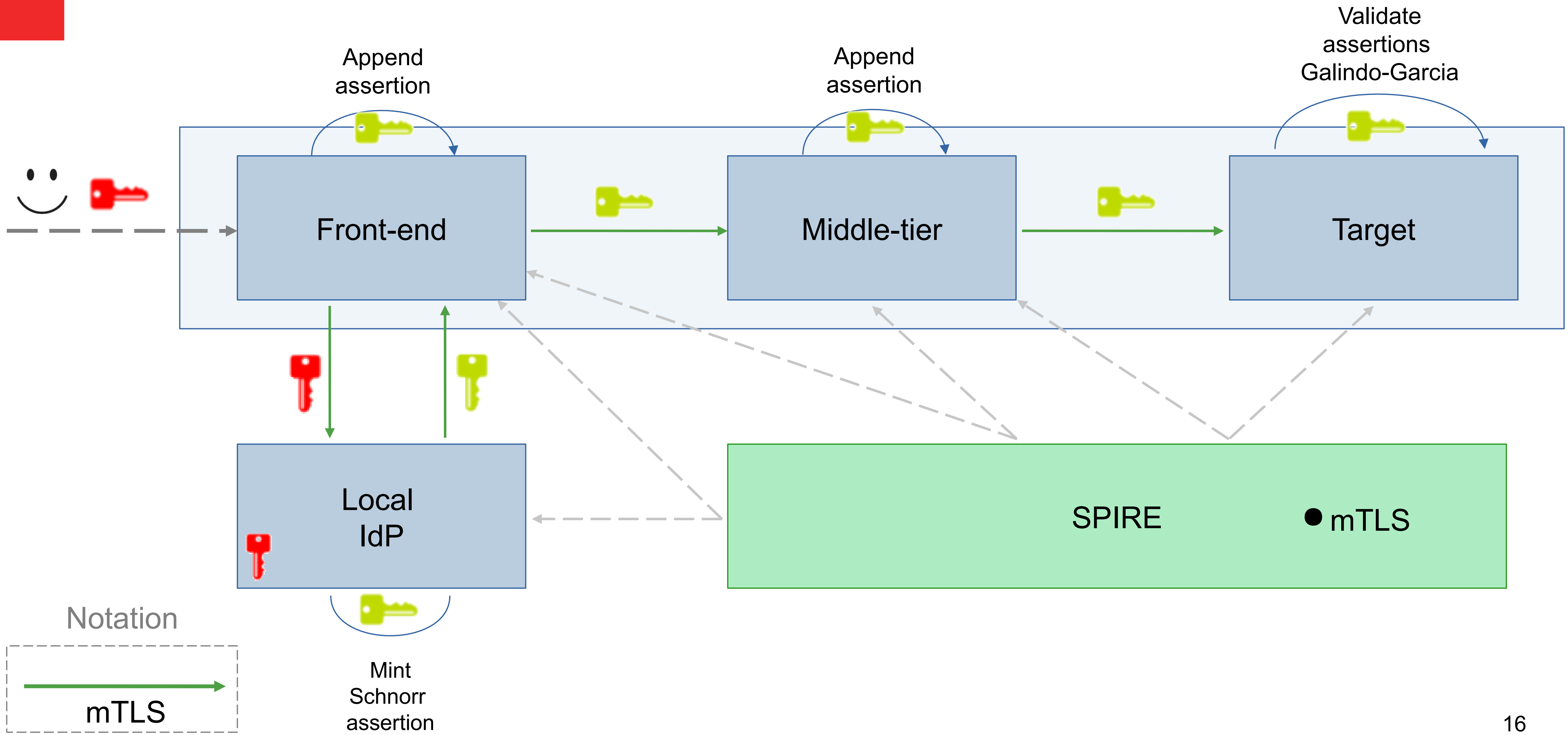


Root private key: z_0
(Root public key: y_0)
Block 0
Data0
private key 1
Signature 0: (r_0, s_0)
Root private key: z_0
(Root public key: y_0)
Block 0
Data0
Signature 0: r_0
"recovered" implicitly, from $(r_0, y_0, \text{Data0})$
~~private key 1: s_0~~
Block 1
Data1
private key 1
Signature 1: (r_1, s_1)

Demo 1: ECDSA – SVID (ID mode)

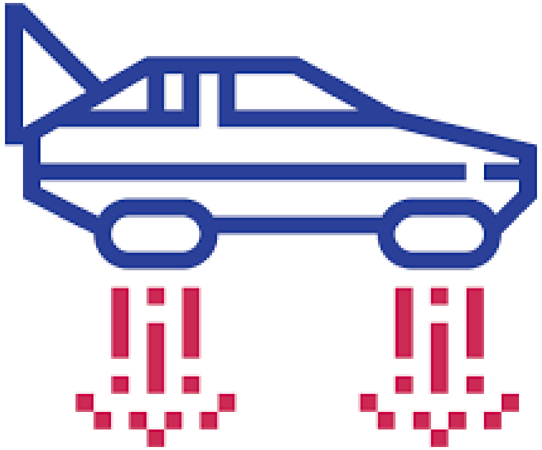


Demo 2: EdDSA – Schnorr (Anonymous mode)



Future Work

- Specify and implement lightweight SVID
- Identity-based SVID: lightweight SVID with Galindo-Garcia
- Biscuits prototype with support to Galindo-Garcia
- Protobuf / JSON analysis



Thanks!!

mmarques@larc.usp.br

USP UDESC INSTITUTO FEDERAL Catarinense Hewlett Packard Enterprise