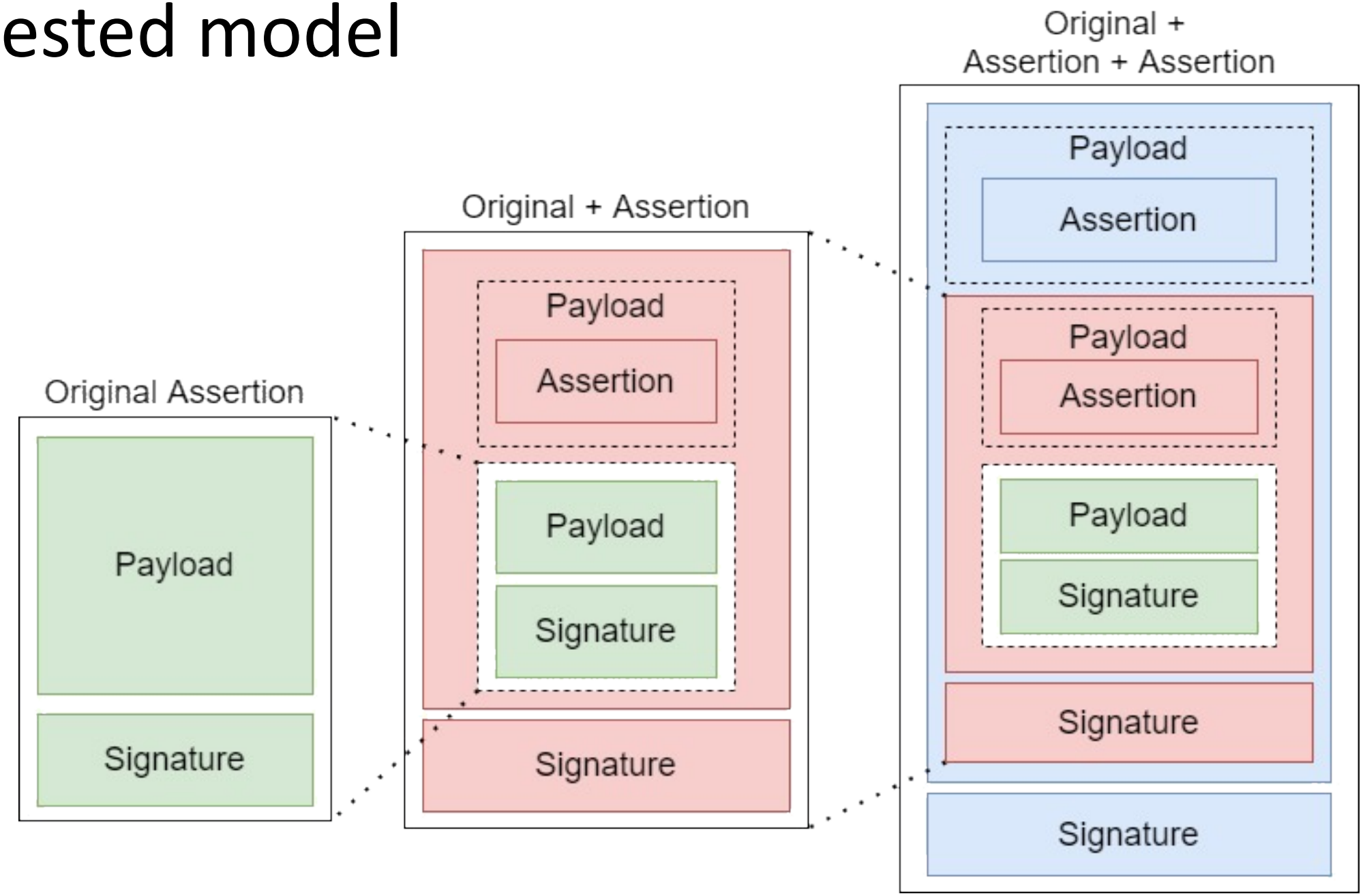
Assertions and Tokens
+
Path tracing

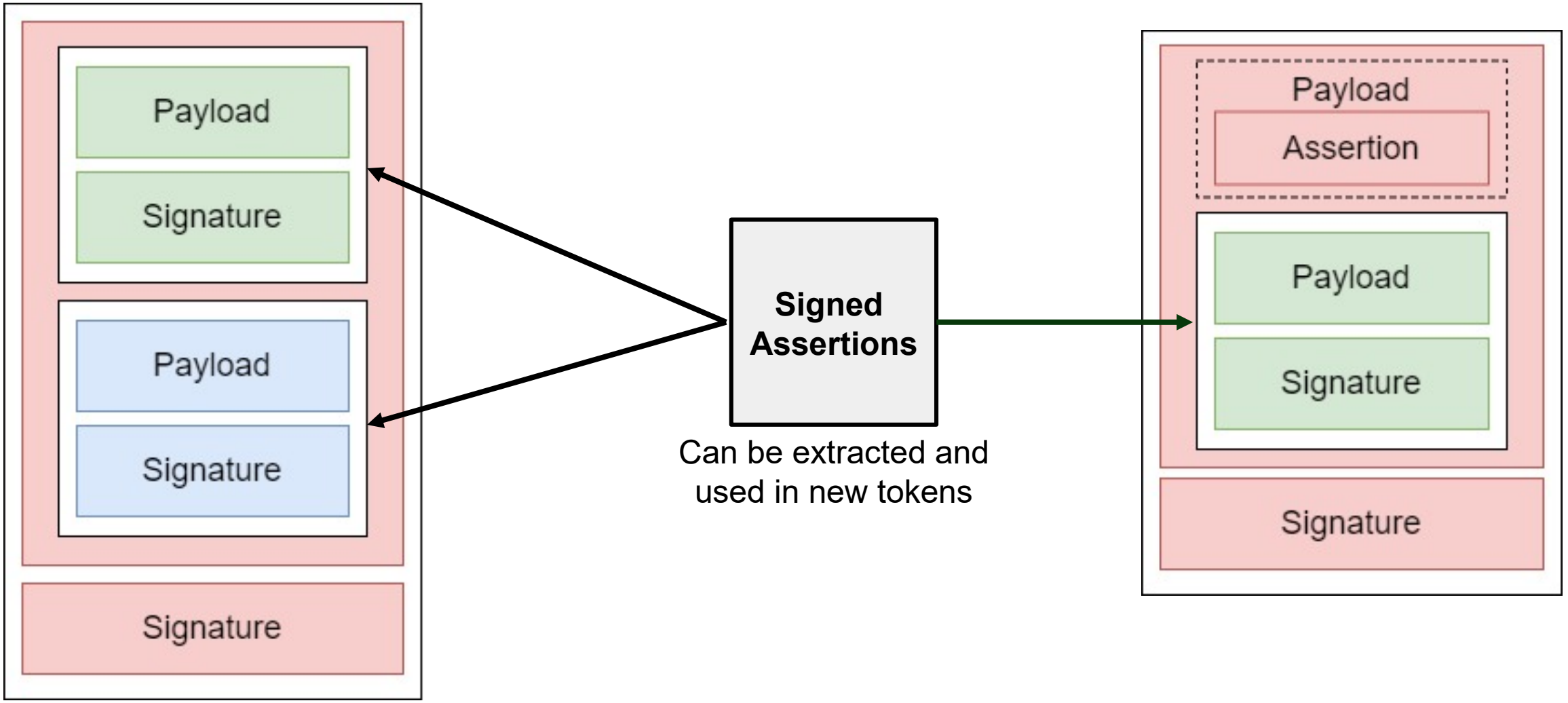
SPIFFE/SPIRE

Aug/2022

Nested model

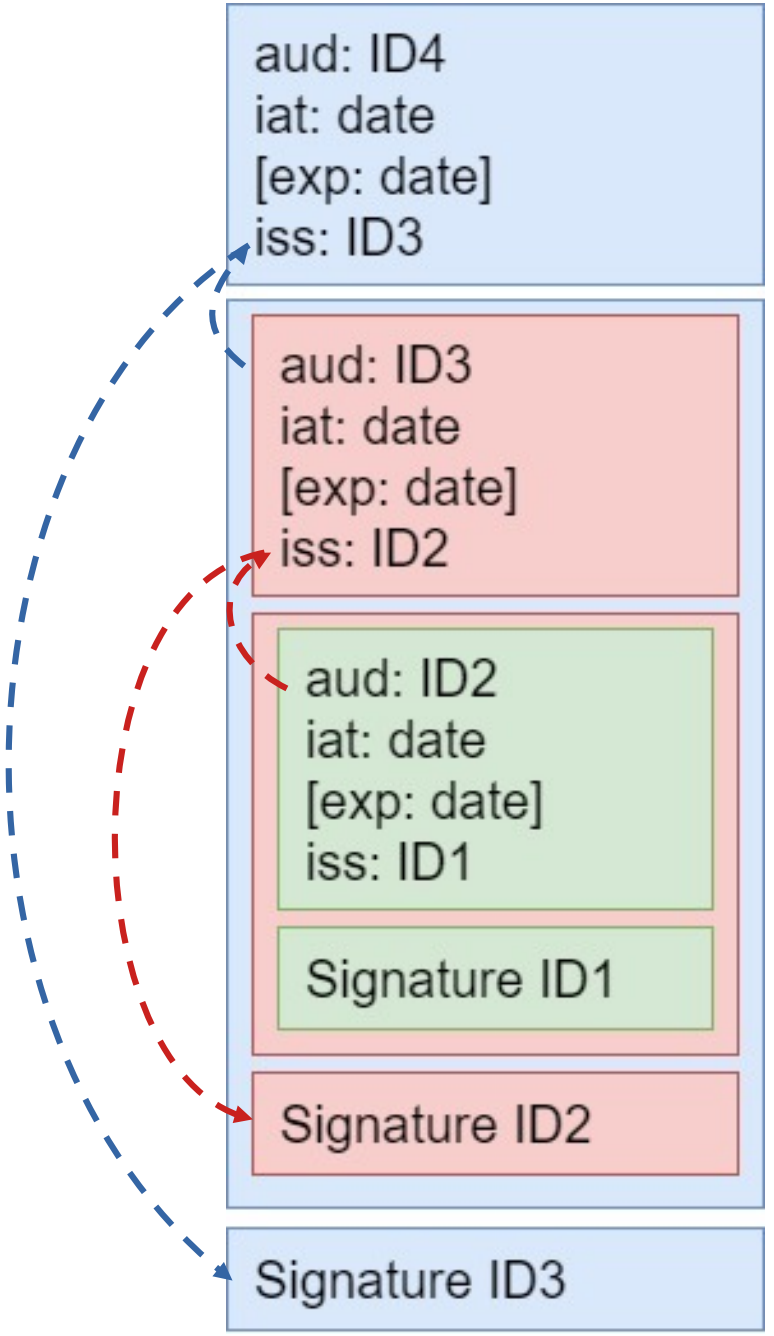


Group signed assertions



Token tracing

Link between issuer and audience



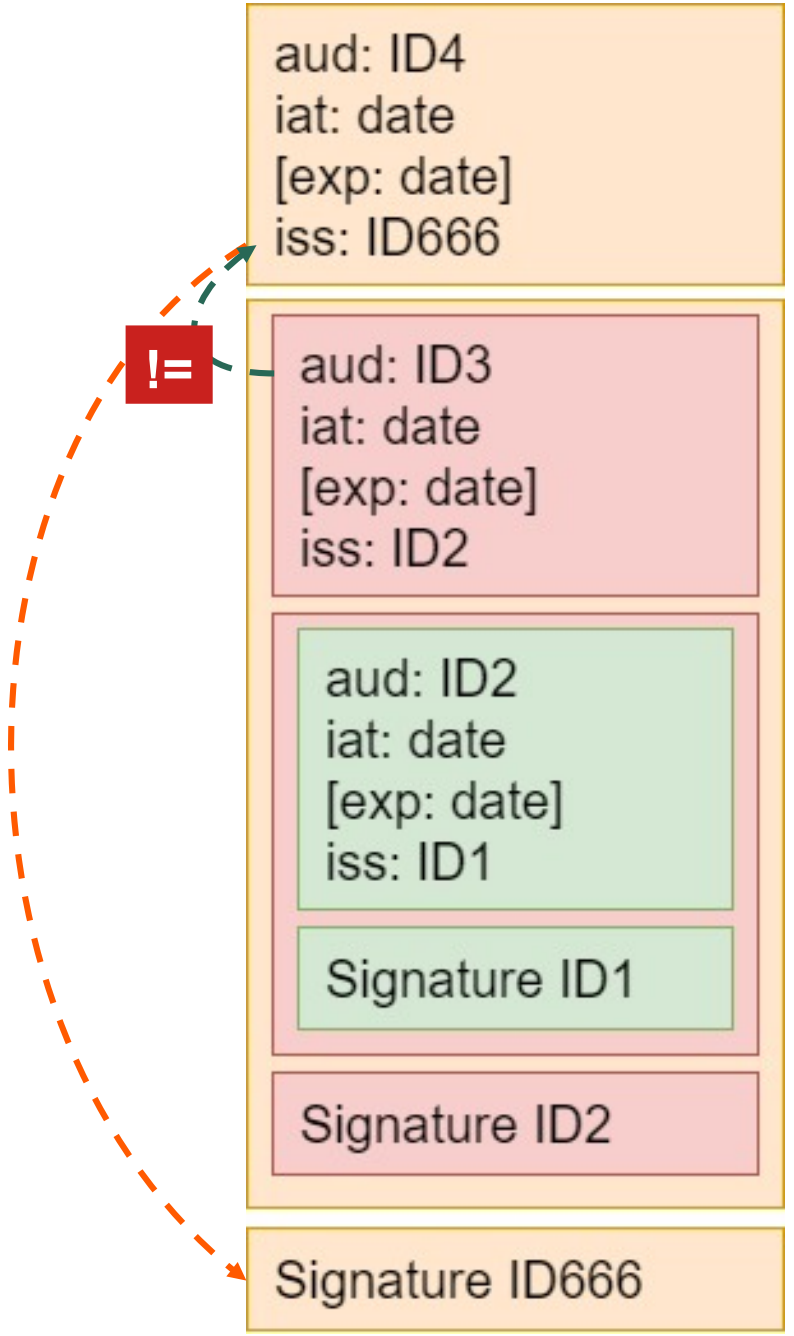
Attack model 1

Re-validation of last assertion

FAIL

issuer != audience

bearer

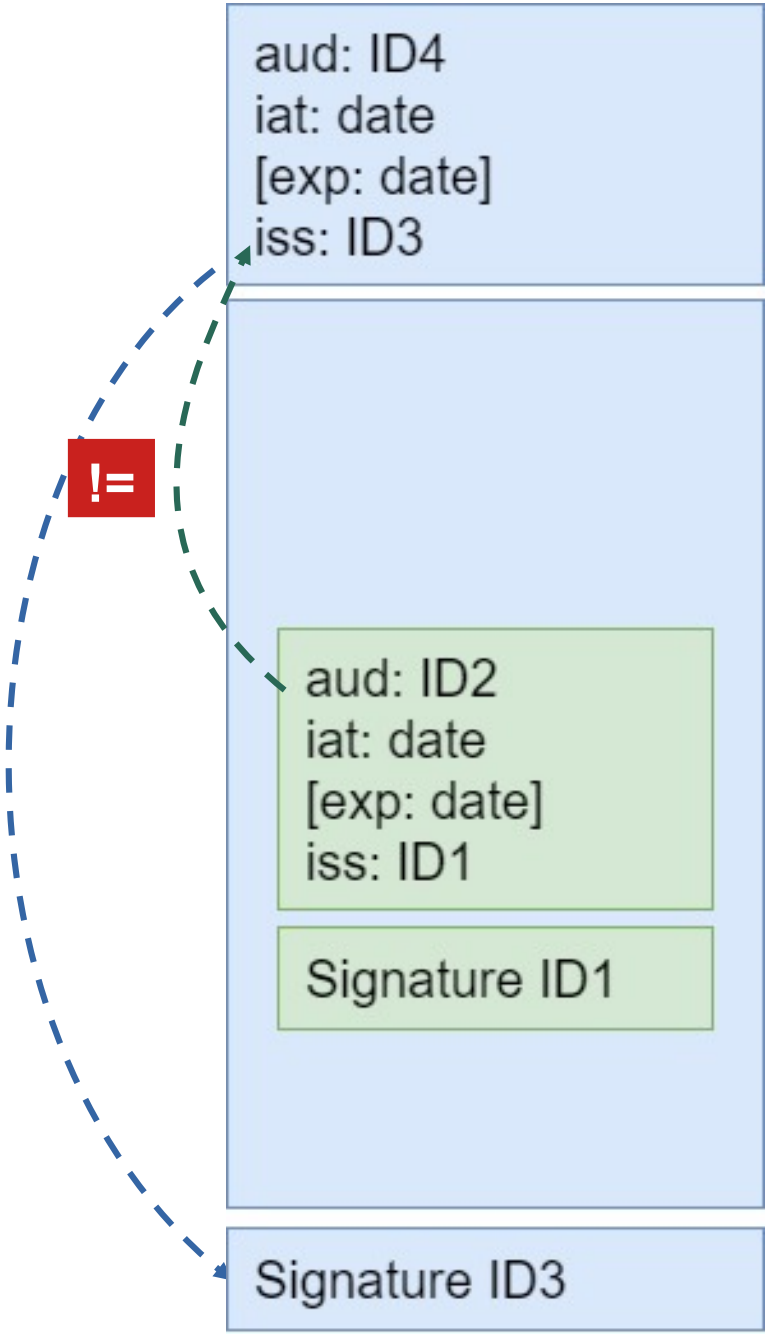


Attack model 1

Removal of middle assertion

FAIL

issuer != audience
bearer

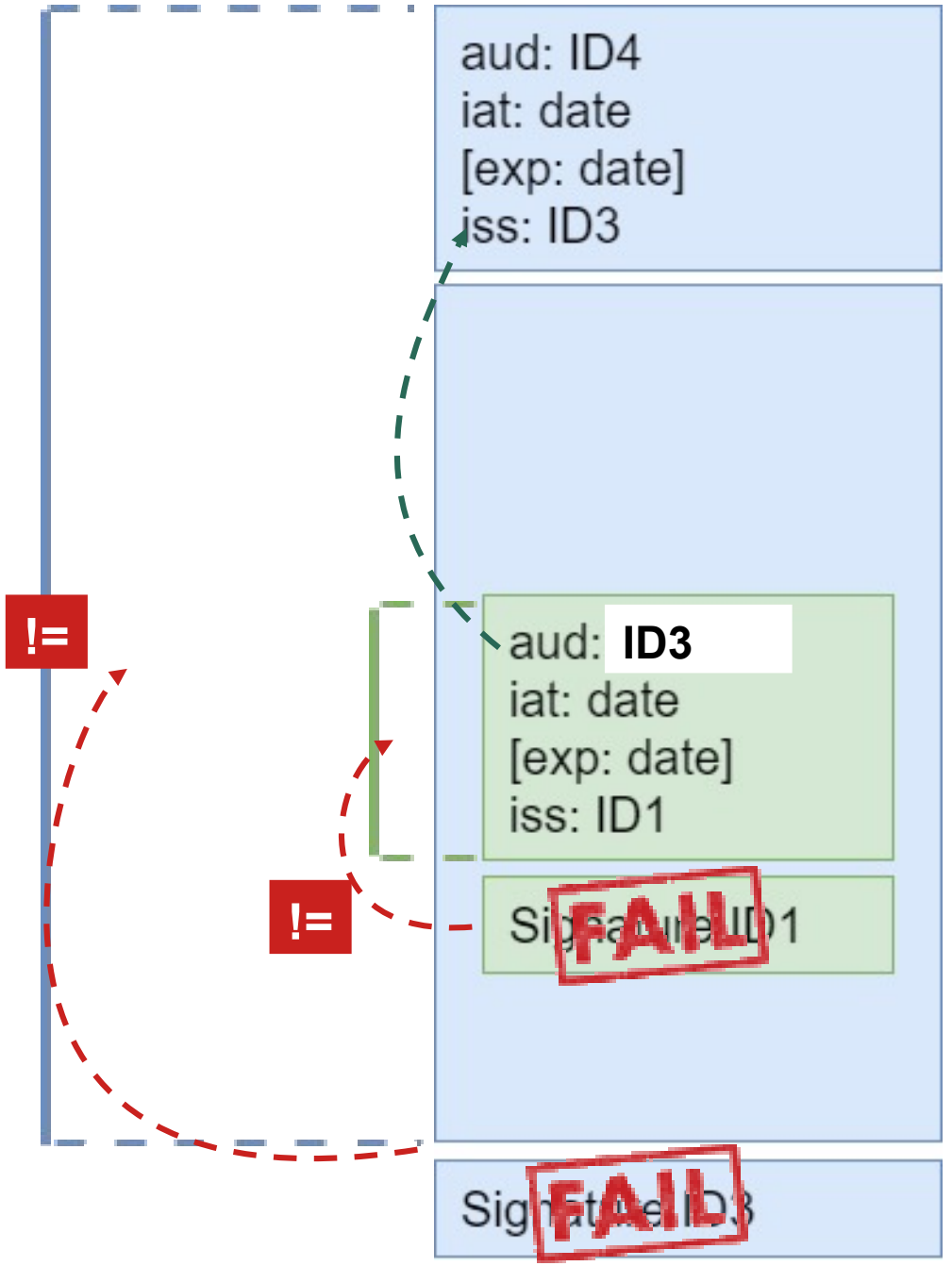


Attack model 2

Token modification

FAIL

Hash chaining



ID Possibilities

- **Anonymous mode:** Assertion issuer/audience are public keys with no ID reference
- **Cert-ID:** Assertion issuer/audience are a lightweight certificate containing ID details and public key
- **Directory Service:** Assertion issuer/audience are IDs used to retrieve certificates from a directory service

Assertion size and execution time

*preliminary results

Size of nested assertions		
	SPIFFE-ID (Bytes)	**SVID (Bytes)**
x1	205	2.107
x2	412	4.216
x3	620	6.324
x4	827	8.434
x5	1.036	10.543
x6	1.244	12.653

Execution time	
Generate Assertion	0.35 ms
Append Assertion	0.35 ms
Validate Assertion	1.90 ms

Thanks!!

mmarques@larc.usp.br

USP UDESC INSTITUTO FEDERAL Catarinense Hewlett Packard Enterprise