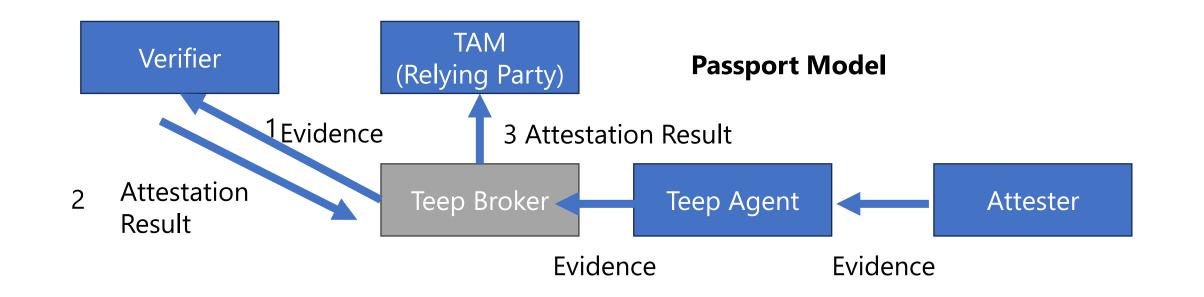
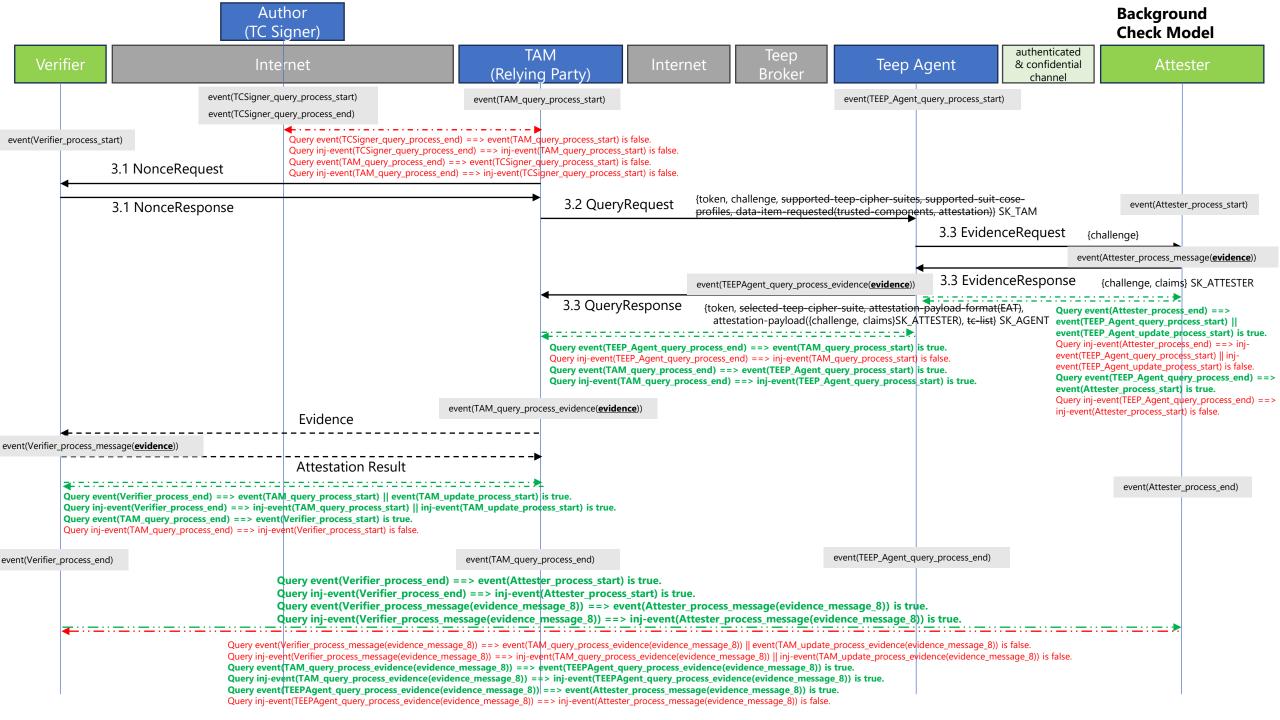
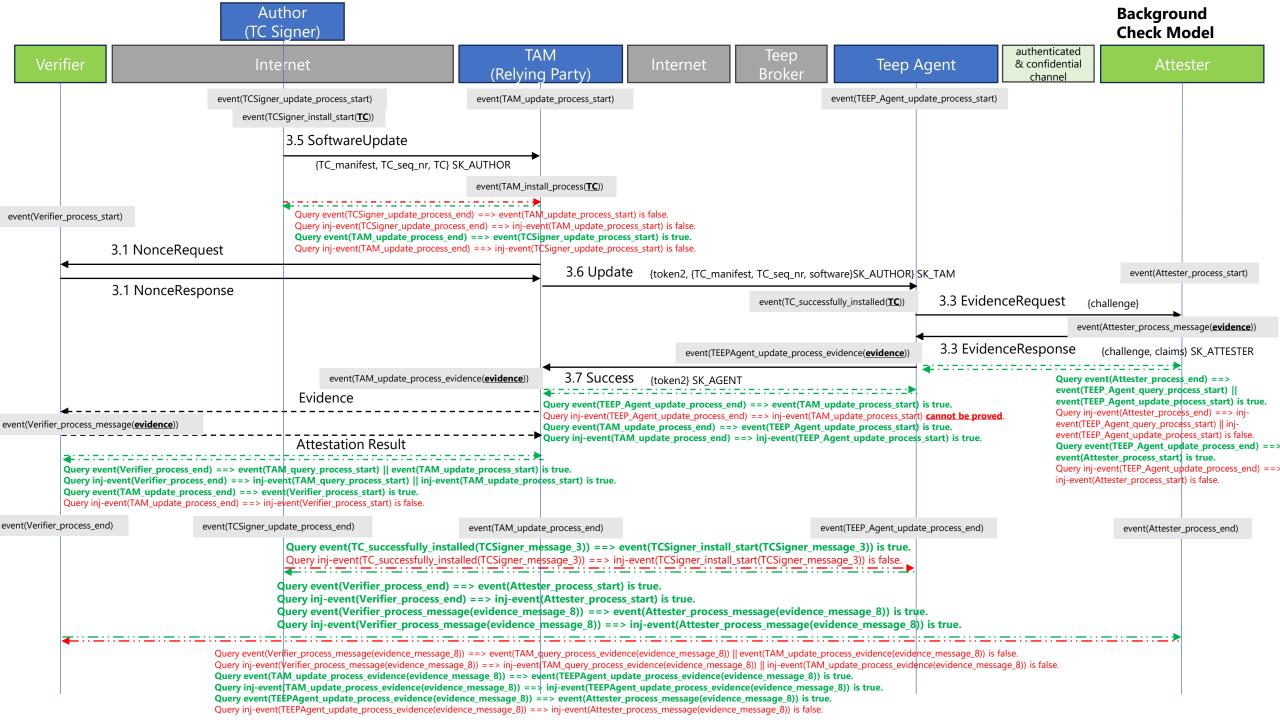
## Attestation Result Verifier TAM (Relying Party) Evidence I think this draft is based on Background Check Model A Usable Formal Methods Sample Problem from TEEP https://datatracker.ietf.org/doc/draft-mt-ufmrg-teep-sample/ Teep Broker Teep Agent Evidence Evidence Attester







## **Summary of Security Properties**

Target security properties	Target entities	Verification results	Consideration	Discussion
Authentication (between entities with explicit communication)	TC Signer ==> TAM TAM ==> TC Signer	False	can be true with SSH secure channel / out of scope in TEEP	(TC means Trusted Components.)
	Verifier ==> TAM	True(injective)	replay protection with nonce	If Verifier want to check the TAM who provides the evidence, Verifier needs extra authentication & authorization.
	TAM ==> Verifier	True(non-injective)		
	TAM ==> TEEP Agent	<u>True(injective)</u>	replay protection with token	
	TEEP Agent ==> TAM	True(non- injective)		
	TEEP Agent ==> Attester	True (non-injective)		TEEP Agent does not provide own freshness, even with challenge by TAM(= nonce by Verifier)
	Attester ==> TEEP Agent	True(non-injective)		
Integrity (message integrity / with implicit message exchange)	TEEP Agent(TC) ==> TC Signer(TC)	True(non-injective)		(TC means Trusted Components.)
	Verifier(evidence) ==> Attester(evidence)	<u>True(injective)</u>	replay protection with nonce / challenge	Although Verifier does know the TAM and the evidence itself, does not know which TAM provides the evidence.
Replay protection (described above, altogether)	-	-	-	_
Confidentiality (not mandatory)	Attestation Evidence	-	-	-
	Trusted Components	-	-	-