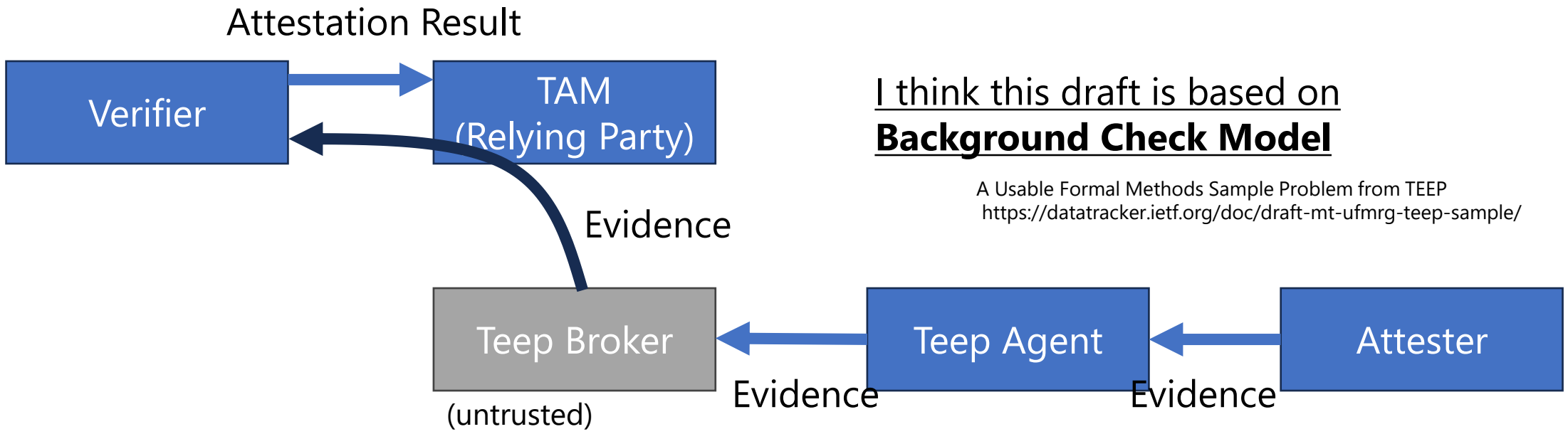
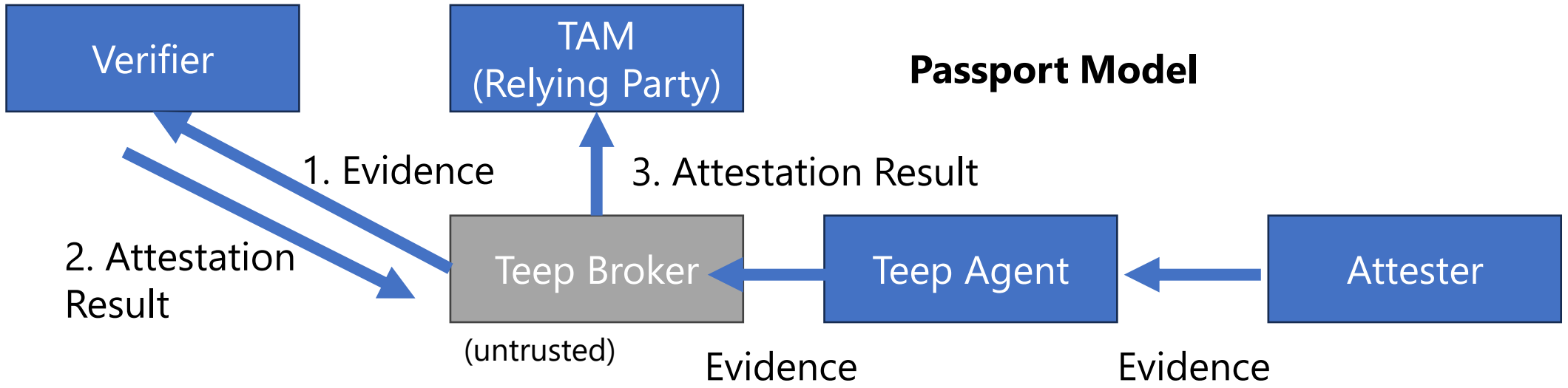


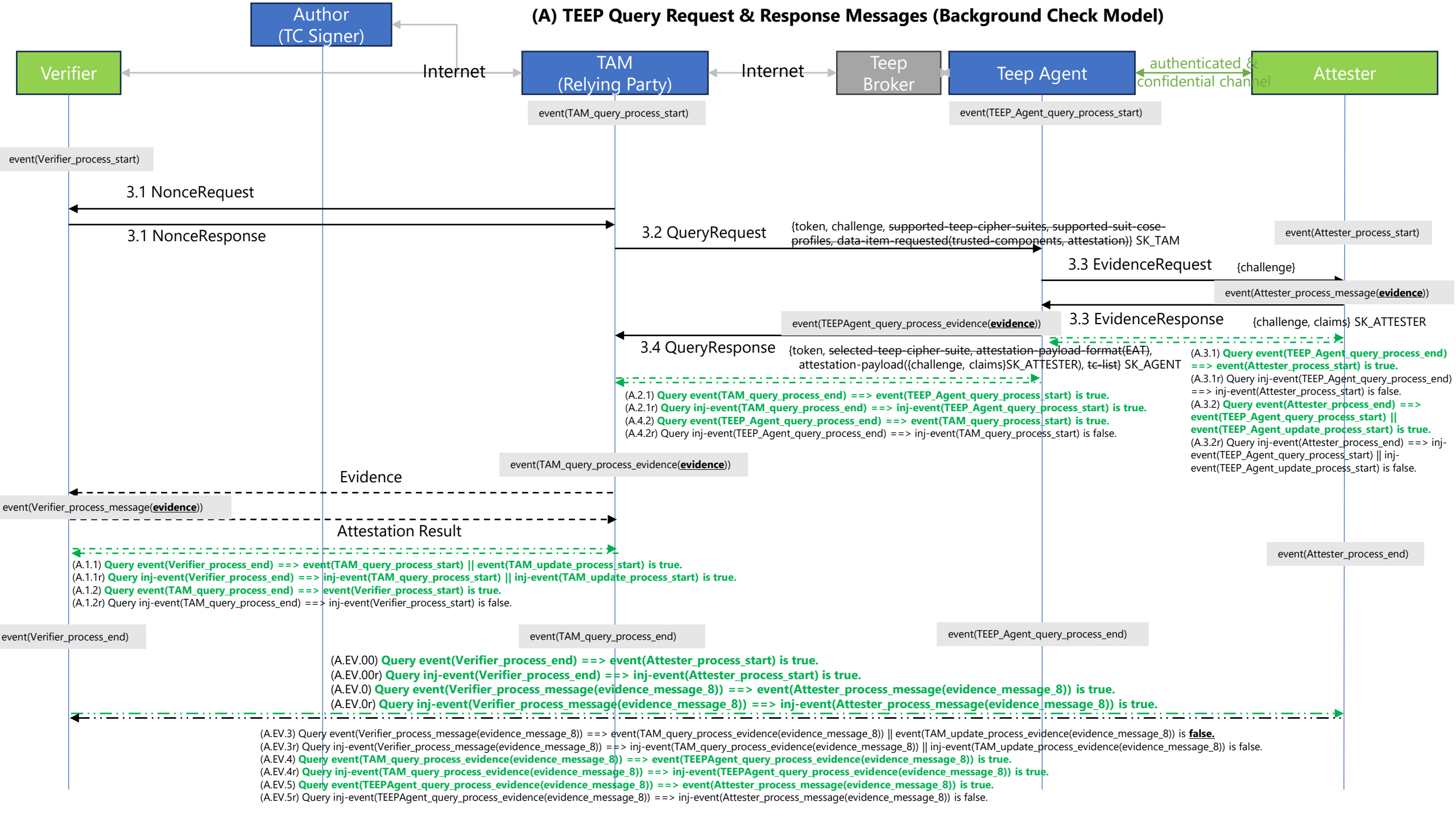
I think this draft is based on
Background Check Model

A Usable Formal Methods Sample Problem from TEEP
https://datatracker.ietf.org/doc/draft-mt-ufmrg-teep-sample/

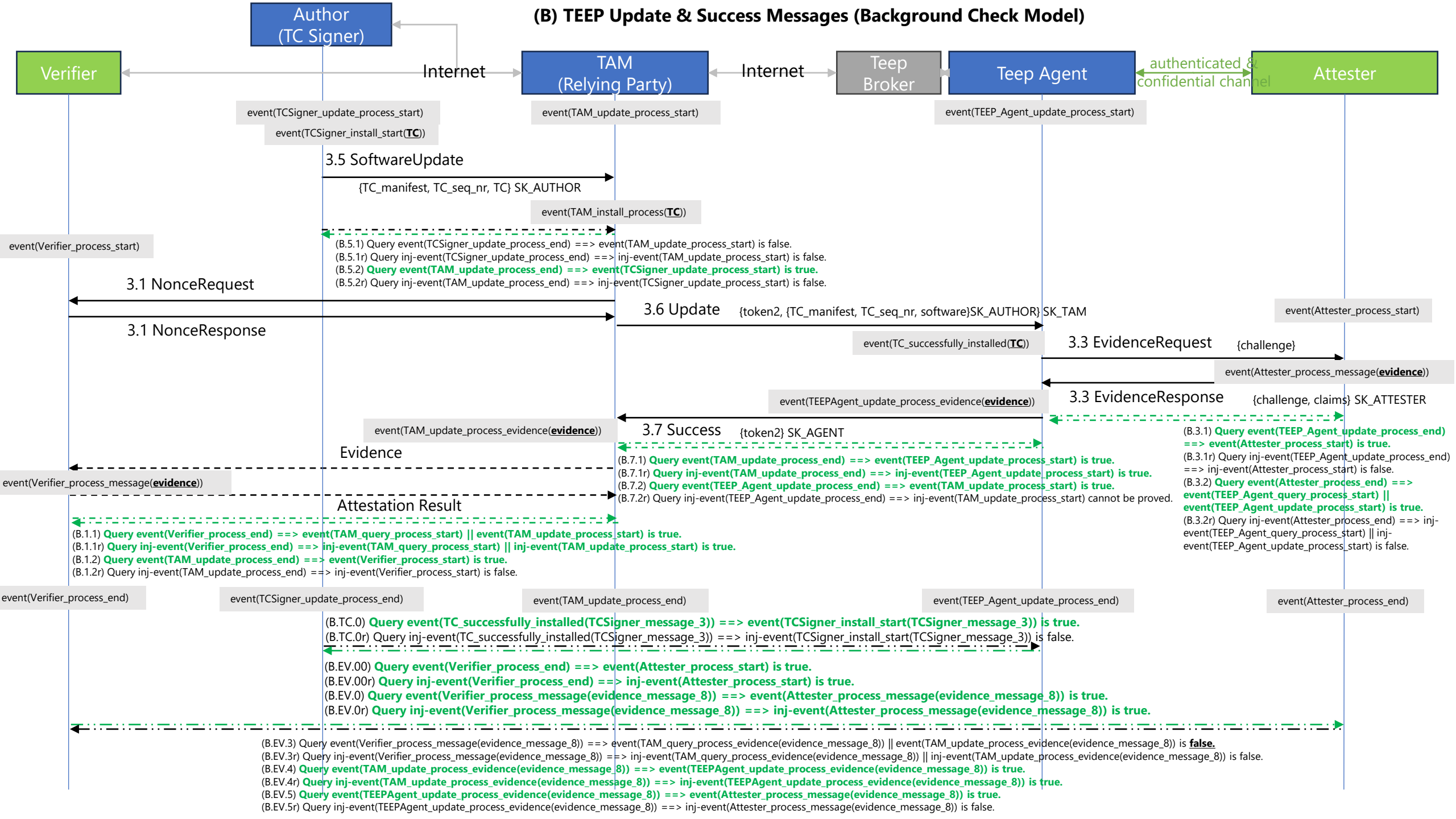


Passport Model

(A) TEEP Query Request & Response Messages (Background Check Model)



(B) TEEP Update & Success Messages (Background Check Model)



Summary of Security Properties

Target security properties	Target entities	Verification results	Consideration	Discussion
Authentication (between entities with explicit communication)	(B.5.1) TC Signer ==> TAM (B.5.2) TAM ==> TC Signer	(false)	can be true with SSH secure channel / out of scope in TEEP	(TC means Trusted Components.)
	(A.1.1 / B.1.1) Verifier ==> TAM	**True(injective)**	**replay protection with nonce**	If Verifier wants to check the TAM who provides the evidence, Verifier needs extra authentication & authorization of TAM.
	(A.1.2 / B.1.2) TAM ==> Verifier	**True**(non-injective)	(with no replay protection) out of scope in TEEP	If TAM wants to check the Verifier, TAM needs extra authentication & authorization of Verifier.
	(A.2.1 / B.7.1) TAM ==> TEEP Agent	**True(injective)**	**replay protection with token**	
	(A.4.2 / B.7.2) TEEP Agent ==> TAM	**True**(non-injective)	(with no replay protection)	
	(A.3.1 / B.3.1) TEEP Agent ==> Attester	**True** (non-injective)	(with no replay protection)	TEEP Agent does not provide own freshness, even with challenge by TAM(= nonce by Verifier)
	(A.3.2 / B.3.2) Attester ==> TEEP Agent	**True**(non-injective)	(with no replay protection)	
Integrity (message integrity / with implicit message exchange)	(B.TC.0) TEEP Agent(TC) ==> TC Signer(TC)	**True**(non-injective)	(with no replay protection) out of scope in TEEP	(TC means Trusted Components.) This depends on the SUIT Manifest specification.
	(A.EV.0 / B.EV.0) Verifier(evidence) ==> Attester(evidence)	**True(injective)**	**replay protection with nonce / challenge**	(B.EV.3) **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	-	-	-