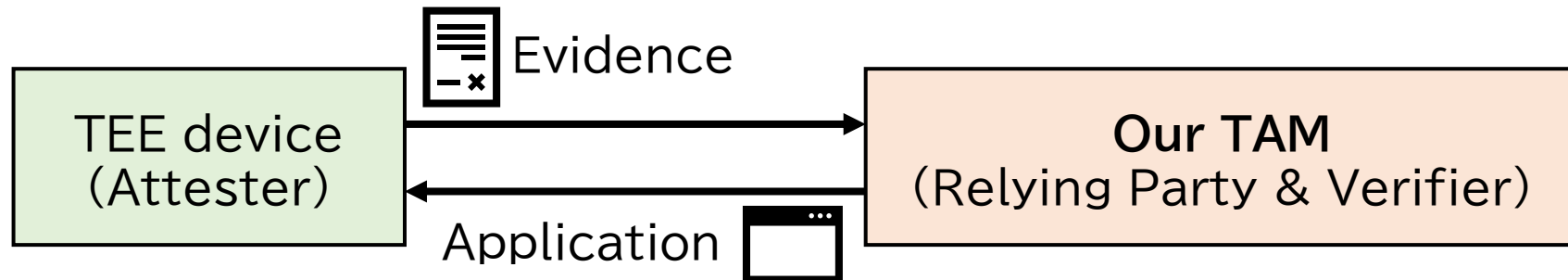


Hackathon Report: Separating Verifier and Relying Party Responsibilities in TEEP

Ken Takayama, Shinichi Miyazawa,
Kazuki Zenba, Yuma Nishihira and
Masahiro Matsunaga
SECOM CO., LTD.

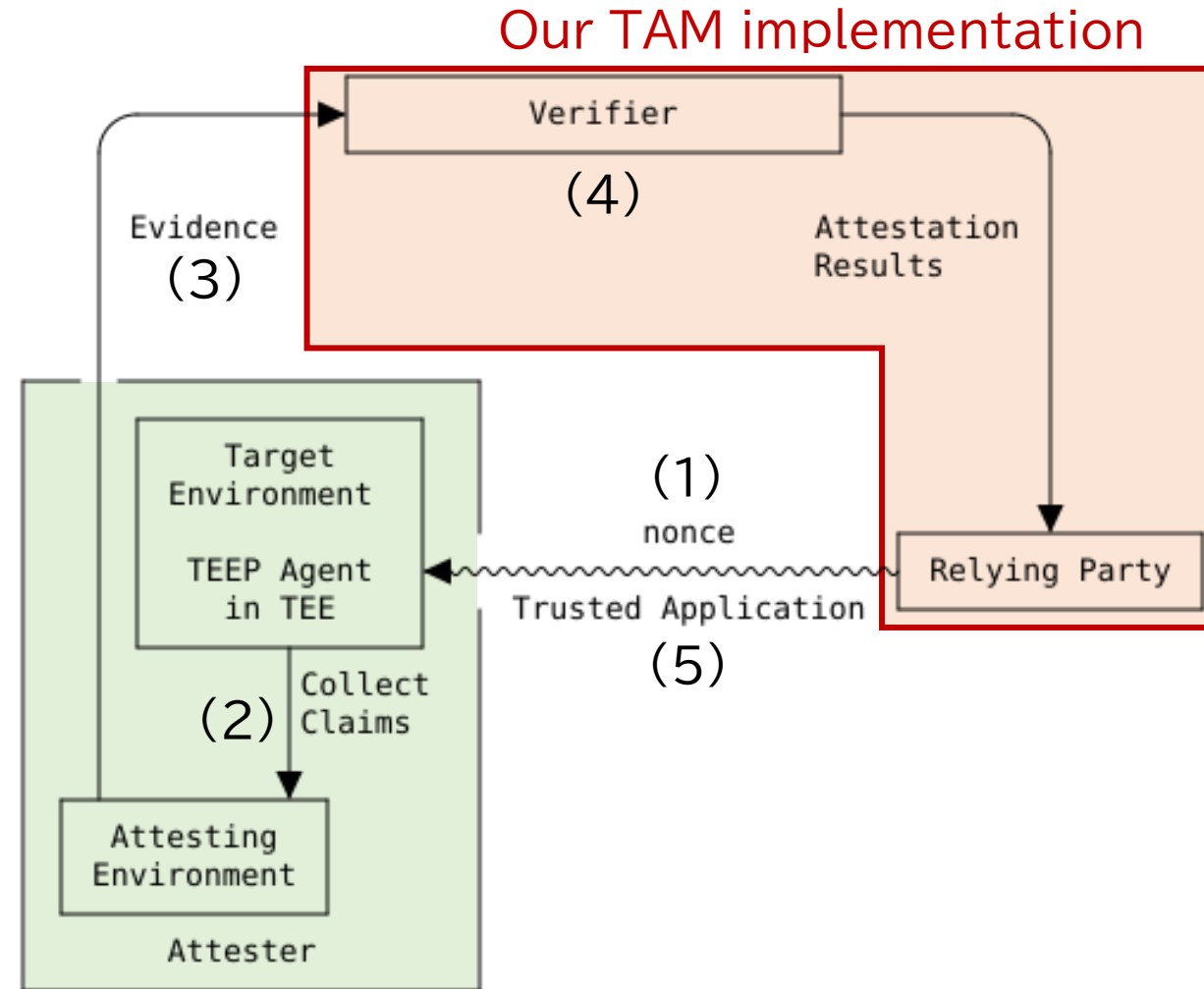
Why We Built This, and What We Learned

- TEEP can carry Remote Attestation, but does not define each appraisal step in detail
- We implemented a TAM that uses Evidence for provisioning
 - In RATS terms, the TAM is the Relying Party, while our implementation also includes Verifier-like functionality
- By implementing those appraisal steps in one TAM, we were able to identify a possible boundary between reusable Evidence appraisal and TEEP-specific appraisal



Attestation Flow in our TAM

1. TAM sends a nonce to the Attester
2. TEEP Agent generates Evidence
 - binding the nonce and the Agent public key
3. Attester sends the Evidence to the TAM
4. TAM verifies the Evidence
5. TAM decides whether to provision the App



in RFC 9334: RATS Arch. style

What Did the TAM Need to Check?

- Evidence format and syntax validation
- Evidence integrity and authenticity verification
- Attestation key validation
- Attesting Environment evaluation
- TCB evaluation
- Measurement-to-Agent mapping
- Nonce and Agent public-key binding verification
- Freshness check
- Agent public-key acceptance
- Final provisioning decision

Possible Responsibility Split

Verifier-like responsibility

- Evidence format and syntax validation
- Evidence integrity and authenticity verification
- Attestation key validation
- Attesting Environment evaluation
- TCB evaluation

TAM / Relying Party responsibility

- Measurement-to-Agent mapping
- Nonce and Agent public-key binding verification
- Freshness check
- Agent public-key acceptance
- Final provisioning decision

Needs broader experience across other TEEs and other RATS use cases before drawing more general conclusions.

Takeaways and Next Step

- **Observation:** TAM contained both generic appraisal and TEEP-specific policy
- **Next:** Check whether the same split appears with other TEEs
- **Beyond TEEP:** SGX Quote appraisal may fit a shared Verifier framework
- **Status:** Initial discussion with the VERAISON project has started