Integration of Remote Attestation with Key Negotiation and Distribution

draft-xia-rats-key-negotiation-integration-00

https://datatracker.ietf.org/doc/draft-xia-rats-key-negotiation-integration/

Liang Xia, Weiyu Jiang	Huawei
Muhammad Usama Sardar	TU Dresden
Henk Birkholz	Fraunhofer SIT
Jun Zhang, Houda Labiod	Huawei Technologies France S.A.S.U.

Motivation & Goal

- ✓ **Goal: Combine key management mechanisms (key distribution, key negotiation) and remote attestation.**

- ✓ **Advantages: lightweight integration avoiding extra steps, improved security, flexibility, performance enhancement.**

- ✓ **Comparison with Attested TLS:** Lightweight implementation can be provided.

Use Cases

- **Public cloud / computing network KMS (Key Management Service): KMS distribute application layer keys** (SK, ASK, ESK...) after remote attestation, they are used for file encryption, disk encryption, LLM parameters (weight...) encryption. There is no secure channel protocol here.

- **Data access: The end user sends his sensitive data to TEE for LLM inference**. Various security protocols can be used like TLS, IPsec, QUIC, OHTTP. **The user only requires basic end-to-end key negotiation which can then be utilized for specific secure channel protocols.**

Integration Scheme 1 -- Key Distribution Based on KMS Integrated with Remote Attestation

```
         .------------.
         |            | 2. Compare Evidence
         |  Verifier  | against appraisal policy
         |            |
         '--------+---'
              ^   |
1. Evidence   |   | 3. Attestation
  Raw public  |   | Result Raw public
  key/certificate|  v        key/certificate
         .---+--------.      Raw public         .------------.
         |            +------------------->|  Relying   | 5. Compare Attestation
         |  Attester  |4. key/certificate  |   Party    | Result against
         |            |   Attestation      |   & KMS    | appraisal policy
         '------------'   Result           '------------' + Distribute Keys
                        + SK/ASK/ESK

SK: Symmetric Key
ASK: Asymmetric Key
ESK: Encrypted Symmetric Key
```

The KMS can generate or distribute these keys accordingly **with the verifier endorsed public key pair**. With this, achieve **a strong binding** between RA and key distribution.

RATS passport model, background check model will be added soon.

Integration Scheme 2 -- Integrating E2E Key Negotiation Into Remote Attestation

```
         .------------.
         |            | 4. Compare Evidence
         |  Verifier  | against appraisal policy
         |            |
         '--------+---'
             ^    |
3 Evidence   |    | 5. Attestation
             |    | Result
             |    v     1. Attestation
       .---+--------. Request + pubC.-------------.
       |  Attester   <--------------->|  Relying    | 7. Compare Attestation
       |  & Server  | 6.Attestation   |  Party      | Result against
       |            | Result          |  & Client   | appraisal policy
       '------------' + pubS          '-------------' + SK = privC * pubS
    2. SK = privS * pubC

SK: Symmetric Key
(privC,pubC): Client's ECDHE key pair
(privS,pubS): Server's ECDHE key pair
```

This is RATS passport model, background check model will be added soon.

Suggest RATS to define attestation request

Attester (server) and Relying Party (client) perform **ECDHE key negotiation** within the remote attestation process.

Next Steps

- To be added:
  - ➢ Remote Attestation Protocol details and Message Extensions
  - ➢ Background check model
  - ➢ Others...

- Comments are warmly welcome 😃

Thanks