Network Attestation for Secure Routing
IETF120 - Vancouver - 2024-07-25
An architectural overview and gap analysis

Michael Richardson*
<mcr+ietf@sandelman.ca>

Liuchunchi (Peter)
<liuchunchi@huawei.com>
Customer (Relying Party)

Path Evidence (PE)

Update PE With AR/RE/PoT

Orchestrator

Verifier

Attester

Verifier

Attester

Verifier

Attester

Customer A

Network Operator

Report

Path Attestation Result (PAR)

Path (path request/answer)

Network Operator

Attester

Veriﬁer

Attester

Veriﬁer

Attester

Attester

Attester
Customer (Relying Party)

Orchestrator

Attester

Verifier

Path Evidence (PE)

Update PE With AR/RE/PoT

Network Operator

Verifier

Attester

Customer A

Customer B

Path Attestation Result (PAR)

Report

PR/A
(path request/answer)

Path Evidence (PE)
Orchestrator

Customer (Relying Party)

Path Evidence (PE)

Verifier (green router vendor)

Background check, protocol TBD

Vendors

Verifier (blue router vendor)

Path Evidence (PE)

Path Attestation Result (PAR)

Verifier

Network Operator

Customer A

Customer (Relying Party)

Network Operator

Customer B

Customer (Relying Party)

Customer A

Network Operator

Customer B

i2rs

Evidence

rats-yang-tpm-charra

Customer facing API: TBD

Path Evidence (PE)

Intra-ISP API: TBD

Network Operator 2

Update PE With RE/PoT

Update PE With RE/PoT

Update PE With RE/PoT

Update PE With RE/PoT

PR/A (path request/answer)
Gap Analysis

Inside and between the operators

- Router <-> Orchestrator
  - “I2rs”, YANG
  - Draft-ietf-rats-tpm-charra
  - Other options

- Orchestrator <-> Orchestrator
  - Keys for Proof of Transit
  - Multiple Exit
  - Descriminator/transition

- Operators and Routing platform vendors
  - Probably background check model

Between Operators and End Customers

- Initiator customer and operator
- Ending customer and operator
Questions/Discussion