Linaro Technical Forum

Attestation Verifier

Joakim Bech - Distinguished Engineer - Linaro

2024-05-08

What is the problem we're trying to solve?

High-level

- Ensure that we have an ecosystem ready when our CCA enabled device are readily available.

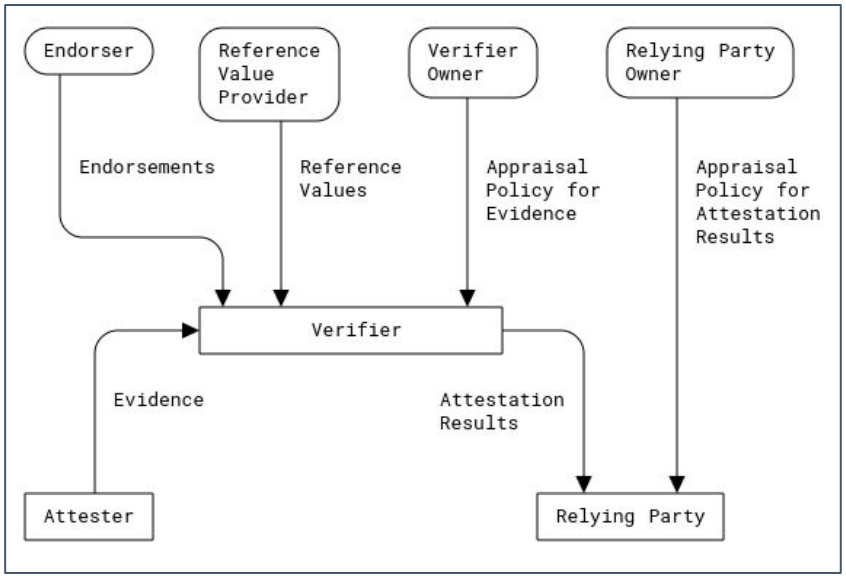
Secondary goals

- Answer the question, who is the attestation verifier?
- Solve fragmentation, lots of these solutions are proprietary.
- What characteristics should a verifier have to be trusted?
- Ease of use.

Why do we need it?

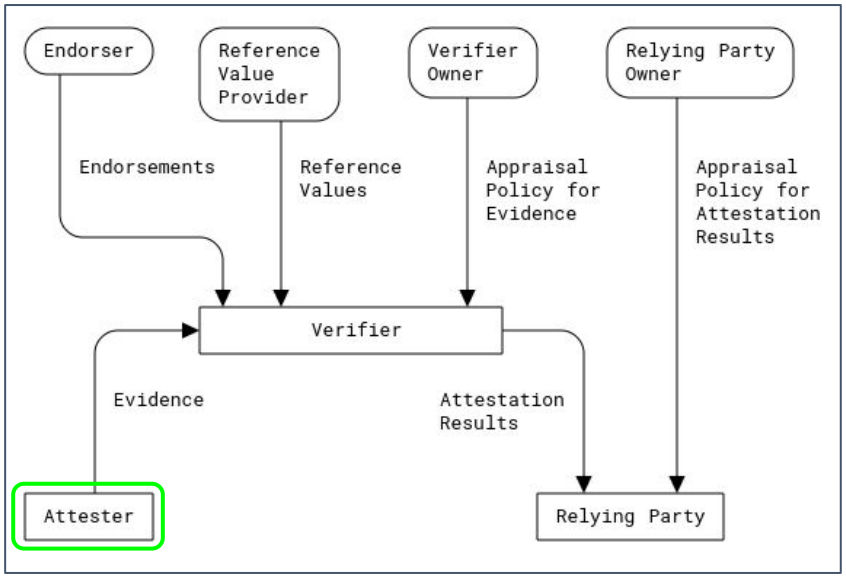
- Establishment of trust between mutually distrusting entities.
- Ensure that the devices we're communicating with are in the expected state and have the features enabled that they claim to offer.

IETF Remote ATtestation ProcedureS (RATS)



IETF Remote ATtestation ProcedureS (RATS)

Armv8-A, Armv9-A
AMD Xilinx, NXP, ST, ... and so on

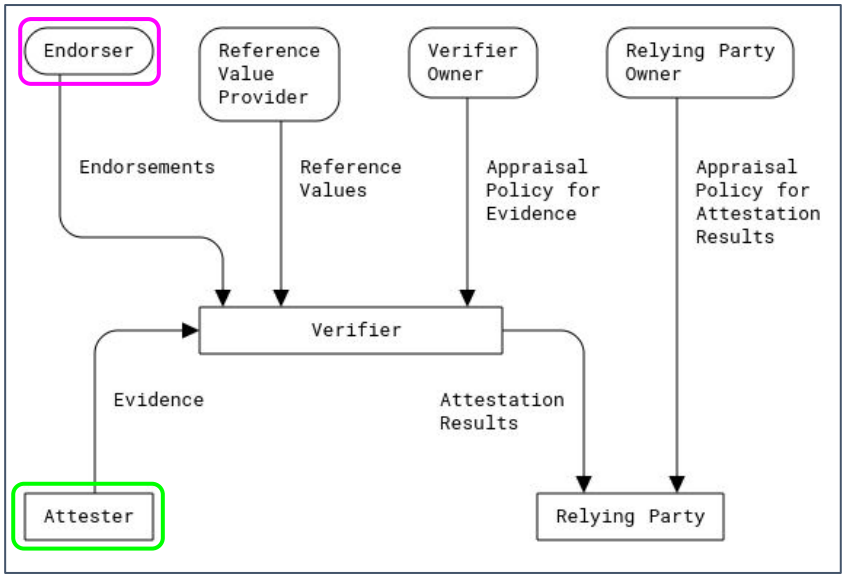


Linaro

IETF Remote ATtestation ProcedureS (RATS)

Armv8-A, Armv9-A
AMD Xilinx, NXP, ST, ... and so on

Device manufacturer, ... OEMs:
AMD Xilinx, NXP, ST, Intel, ...



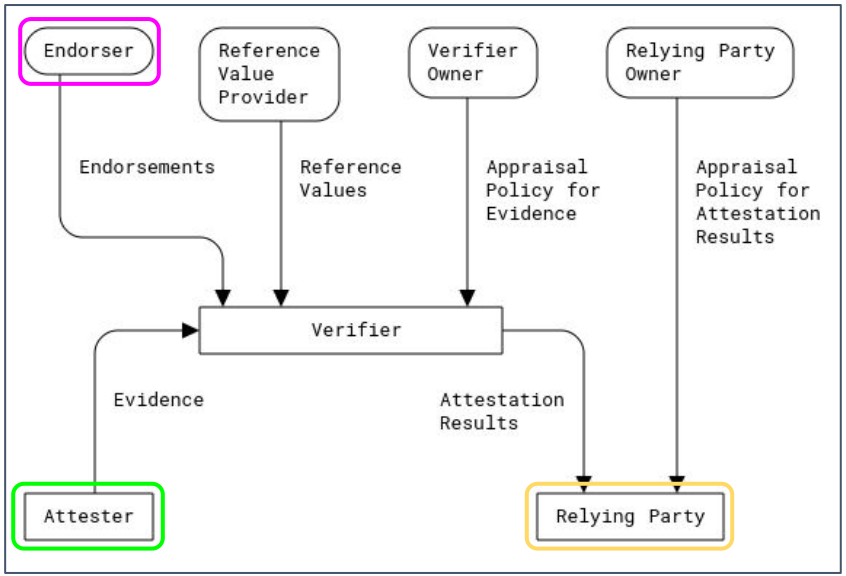
Linaro

IETF Remote ATtestation ProcedureS (RATS)

Armv8-A, Armv9-A
AMD Xilinx, NXP, ST, ... and so on

Device manufacturer, ... OEMs:
AMD Xilinx, NXP, ST, Intel, ...

HSBC, Barclays, Wells Fargo, ...



Linaro

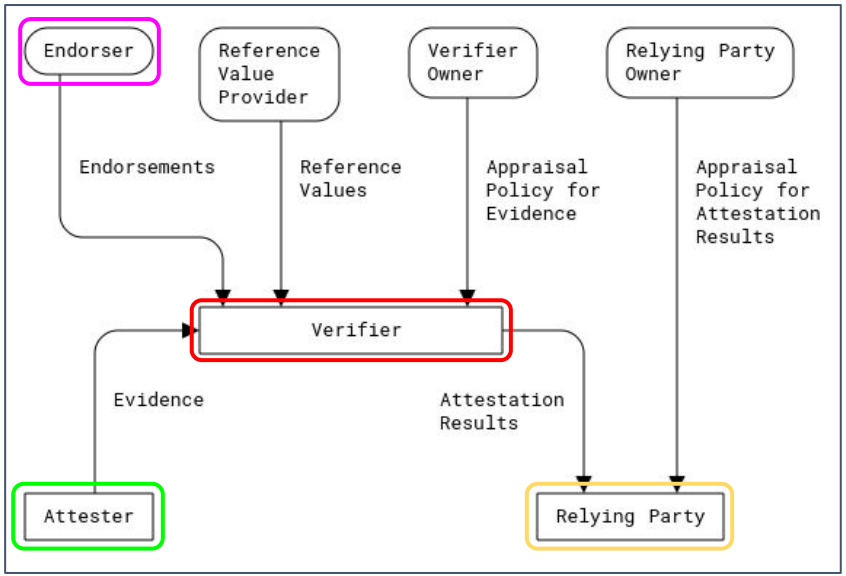
IETF Remote ATtestation ProcedureS (RATS)

Armv8-A, Armv9-A
AMD Xilinx, NXP, ST, ... and so on

Device manufacturer, ... OEMs:
AMD Xilinx, NXP, ST, Intel, ...

HSBC, Barclays, Wells Fargo, ...

Who is this?



Linaro

IETF Remote ATtestation ProcedureS (RATS)

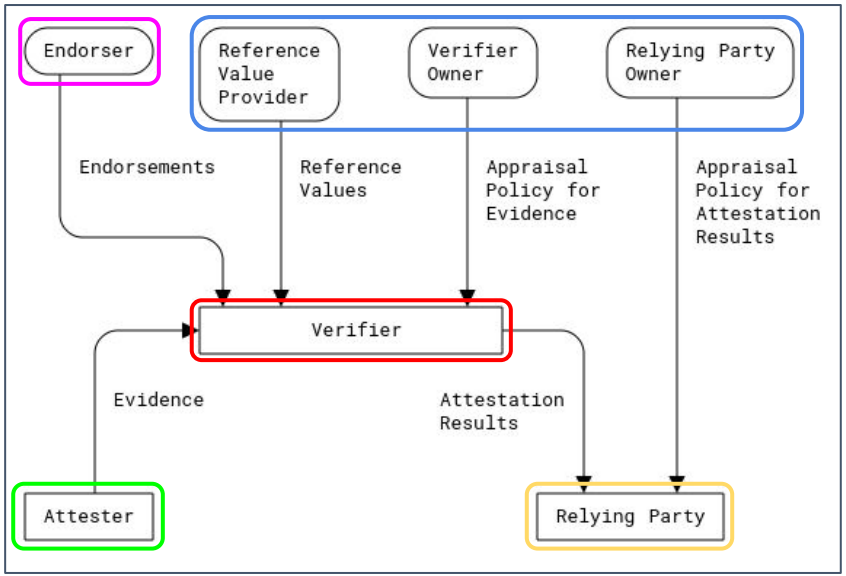
Armv8-A, Armv9-A
AMD Xilinx, NXP, ST, ... and so on

Device manufacturer, ... OEMs:
AMD Xilinx, NXP, ST, Intel, ...

HSBC, Barclays, Wells Fargo, ...

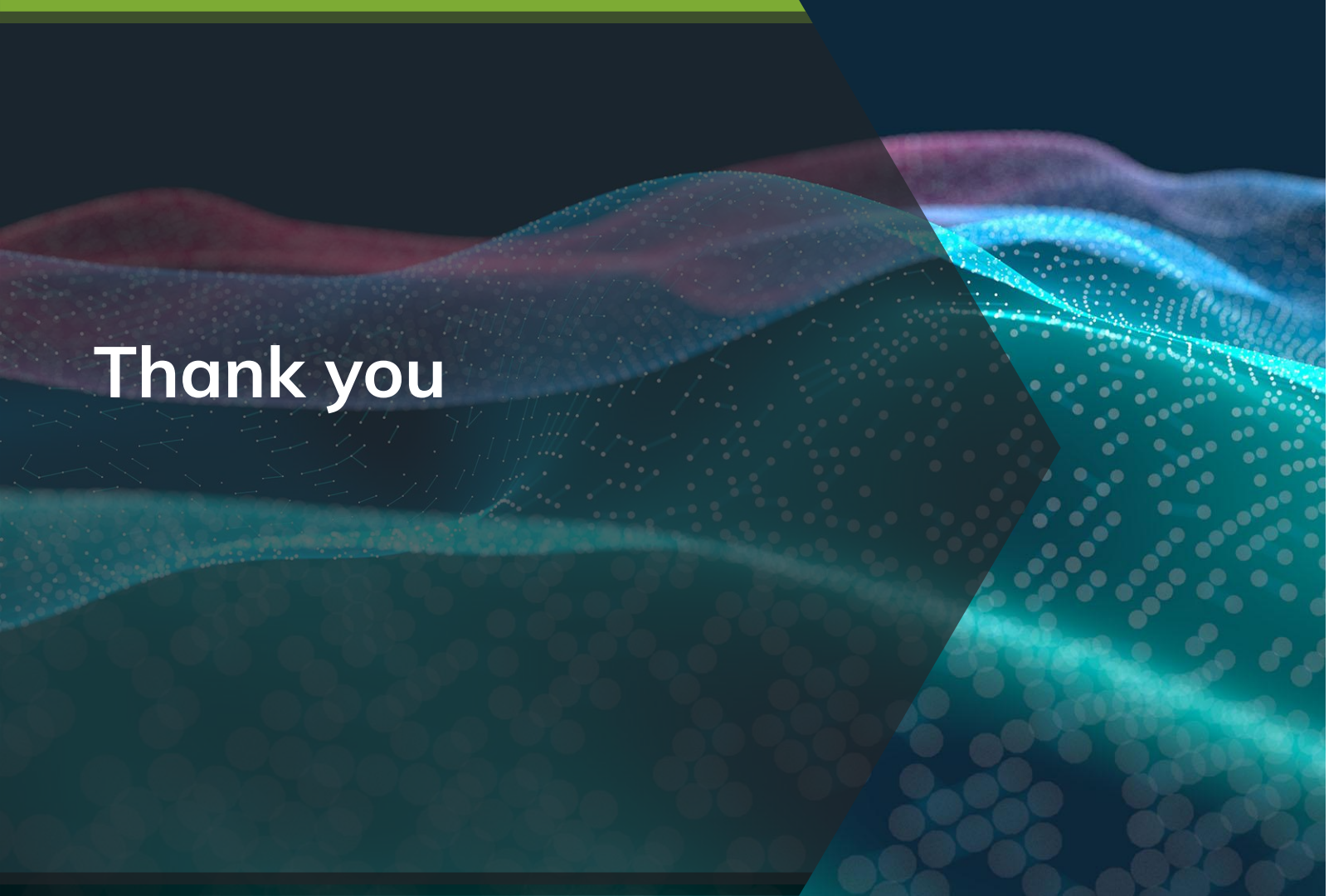
Who is this?

Also of interest, often the same players as the others



Work in progress

- DCAP - Deploy CCA on Arm Platforms
  - Data Center Group @ Linaro (Leonardo, Mathieu, Thomas, Kevin)
  - CoCo integration (CNCF)
  - CCA enablement in TRS
  - Documentation
  - FVP, QEMU (PoC/Reference build here), ... and other environments
- Project VERAISON
- IETF - RATS



Linaro

Terminology

Roles

- **Attester**: Produces **evidences**
- **Verifier**: Receives **evidences** and produces **attestation results**
- **Relying Party**: Receives **attestation results**, use that and **policies** to make decisions

Other roles

- **Endorser**: Produces **endorsements,** typically a manufacturer, trusted by verifier.
- **Reference Value Provider**: Produces “known good values”, typically a manufacturer.
- **Verifier Owner**: Entity authorized to configure an Appraisal Policy for Evidence in a Verifier
- **Relying Party Owner**: Entity authorized to configure an Appraisal Policy