Attestation and Verification

The elephant in the confidential computing room

sameo@rivosinc.com - LPC 2022

Rivos

Protecting Data in Use

Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment. (CCC whitepaper)

Protecting Data in Use

Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment. (CCC whitepaper)

Protecting data in use is of limited value if you can't trust who generates and uses it

Protecting Data in Use

Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment. (CCC whitepaper)

Protecting data in use is of limited value if you can't trust who generates and uses it

Can you trust your guest SW stack?

Can you trust your Confidential Compute hardware?

Protecting Data in Use

Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment. (CCC whitepaper)

Protecting data in use is of limited value if you can't trust who generates and uses it

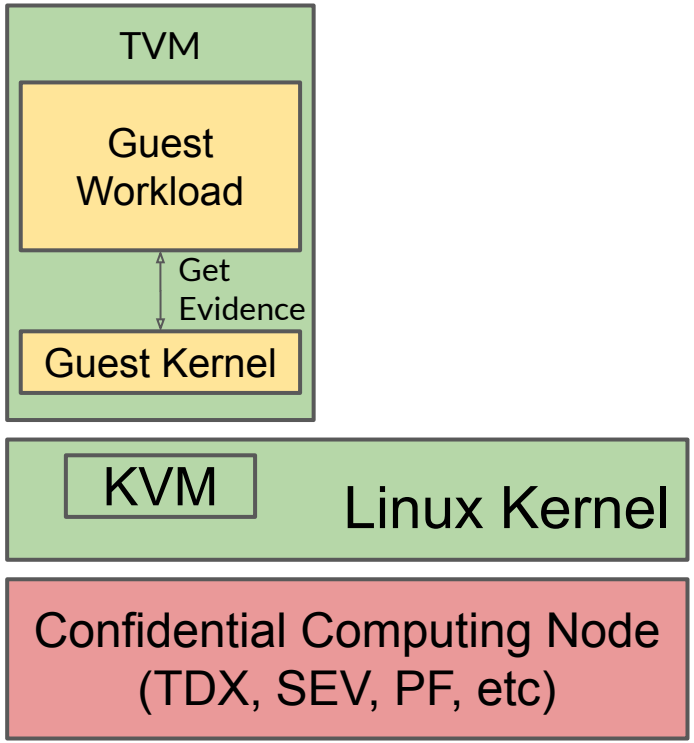
Can you trust your guest SW stack?

Can you trust your Confidential Compute hardware?

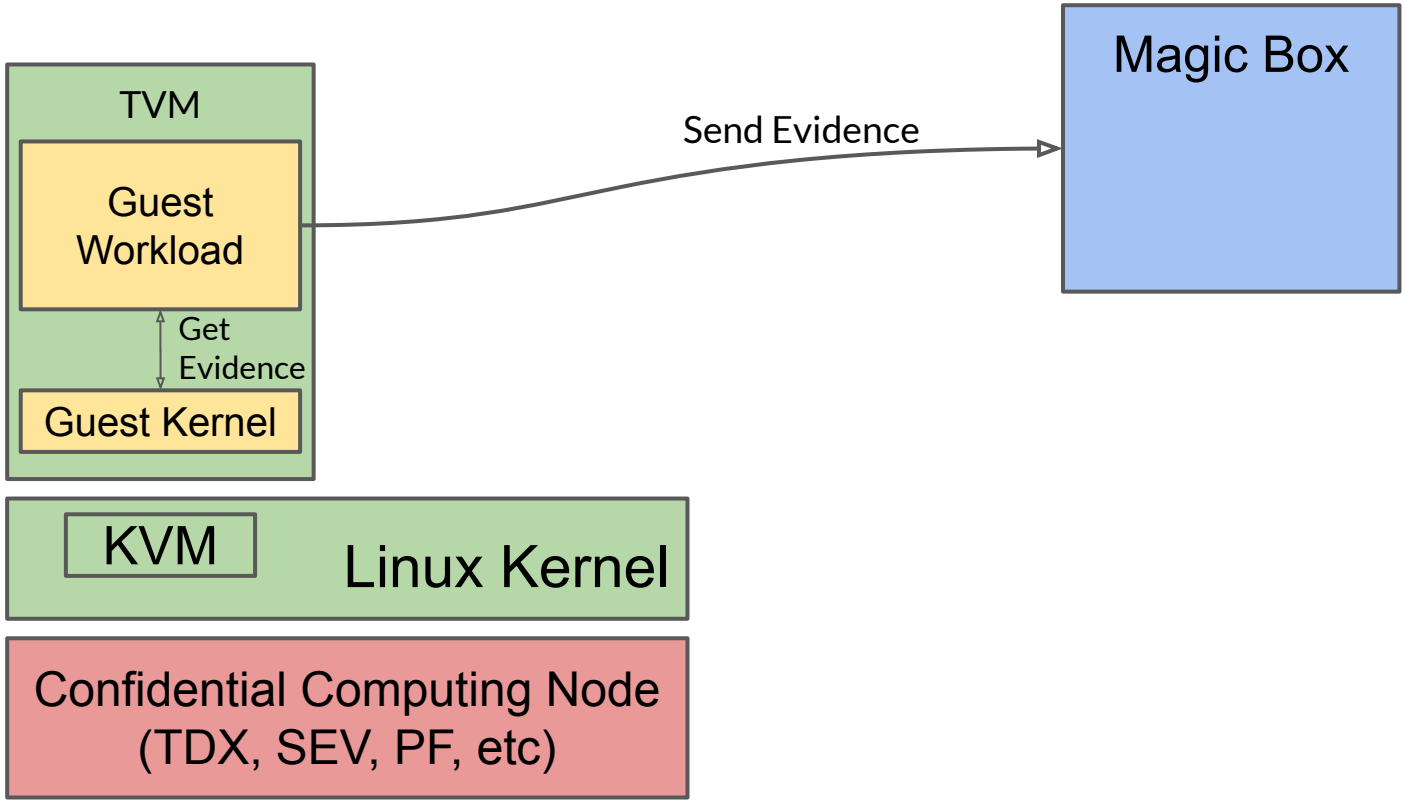
Attest and Verify

Confidential Computing without attestation and verification is not confidential

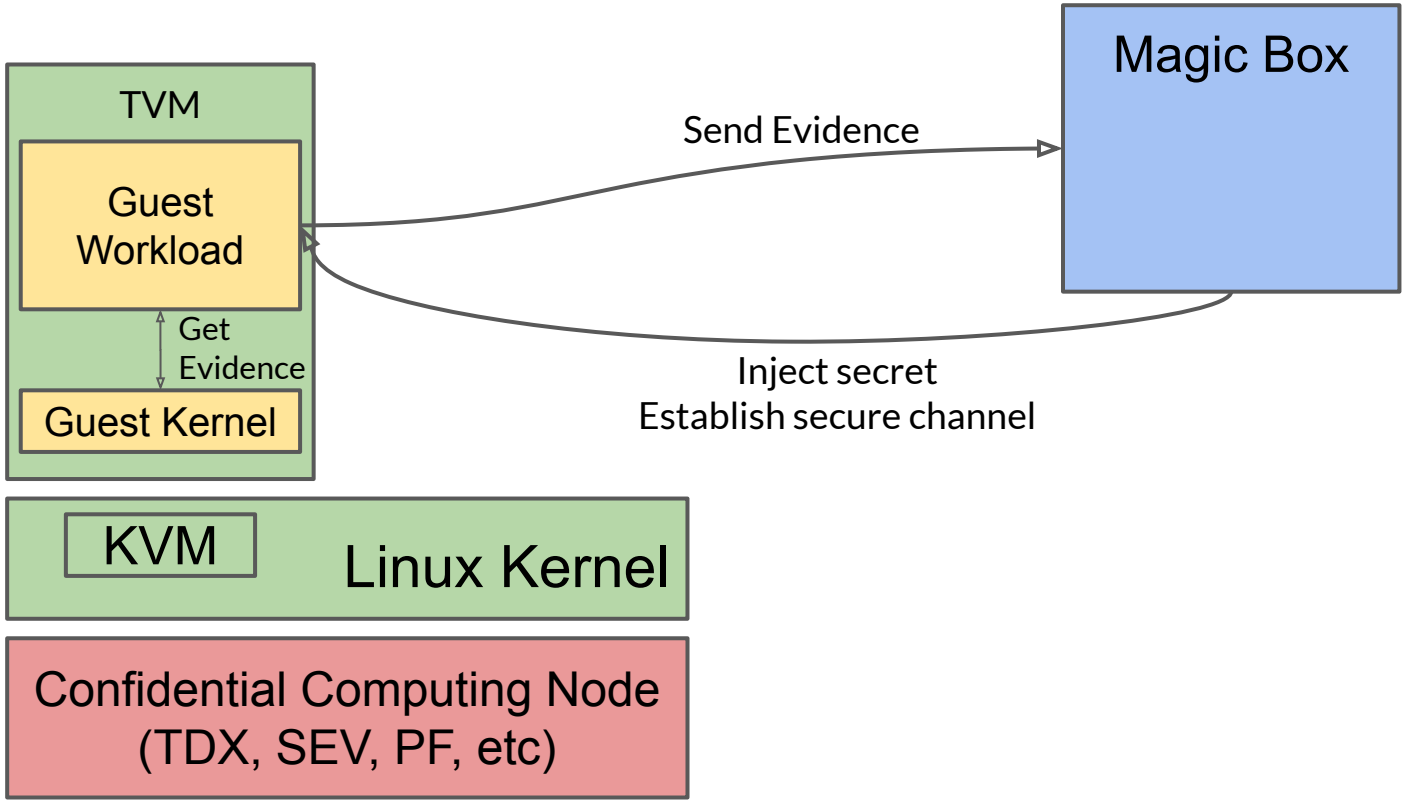
Our Main Focus



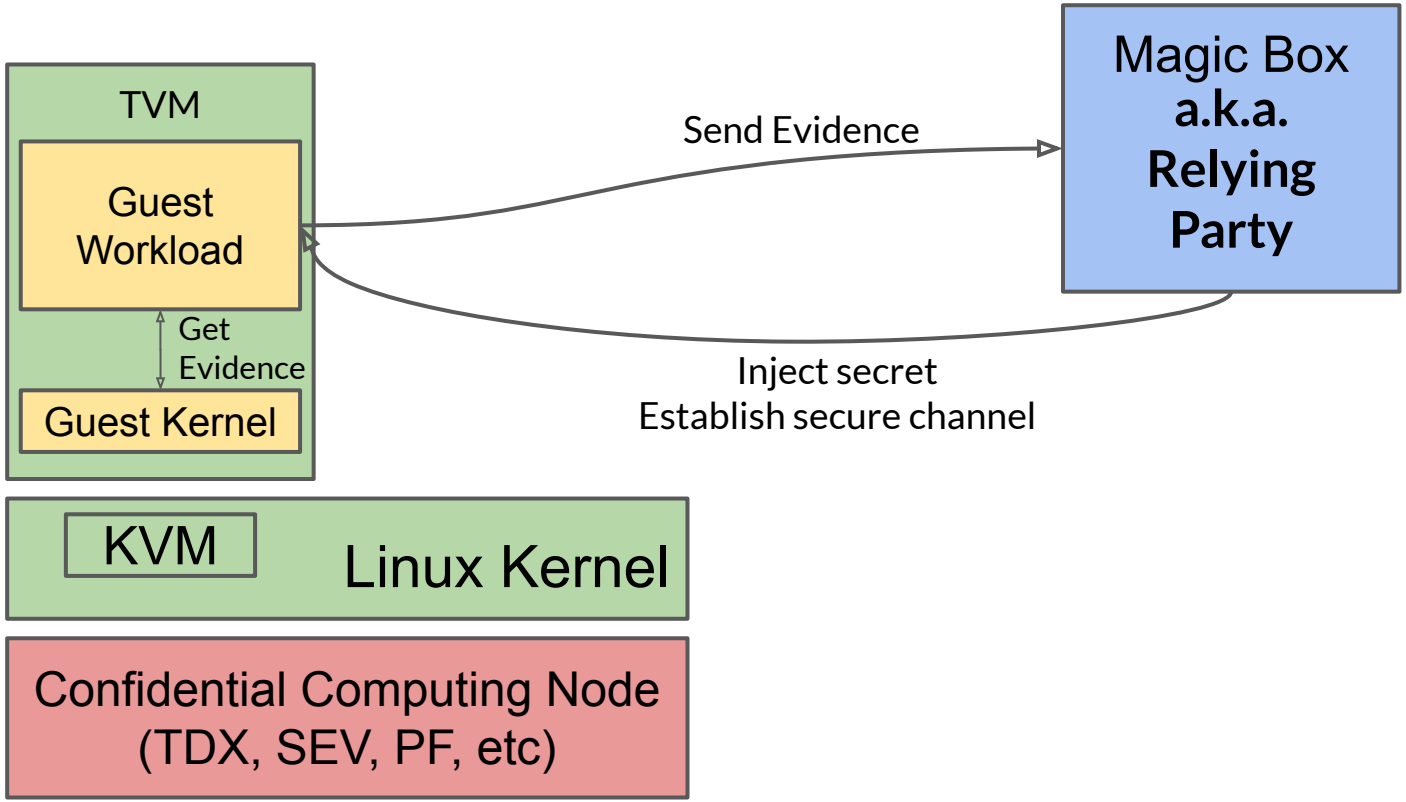
What We Tend to Forget



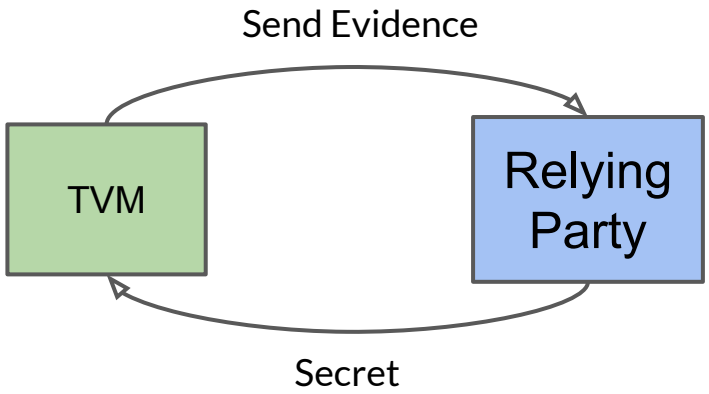
What We Tend to Forget



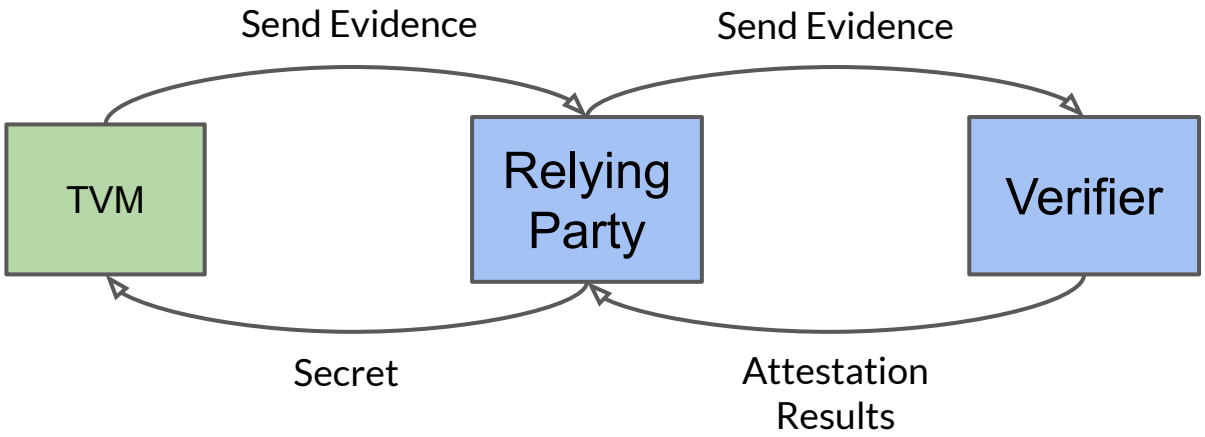
What We Tend to Forget



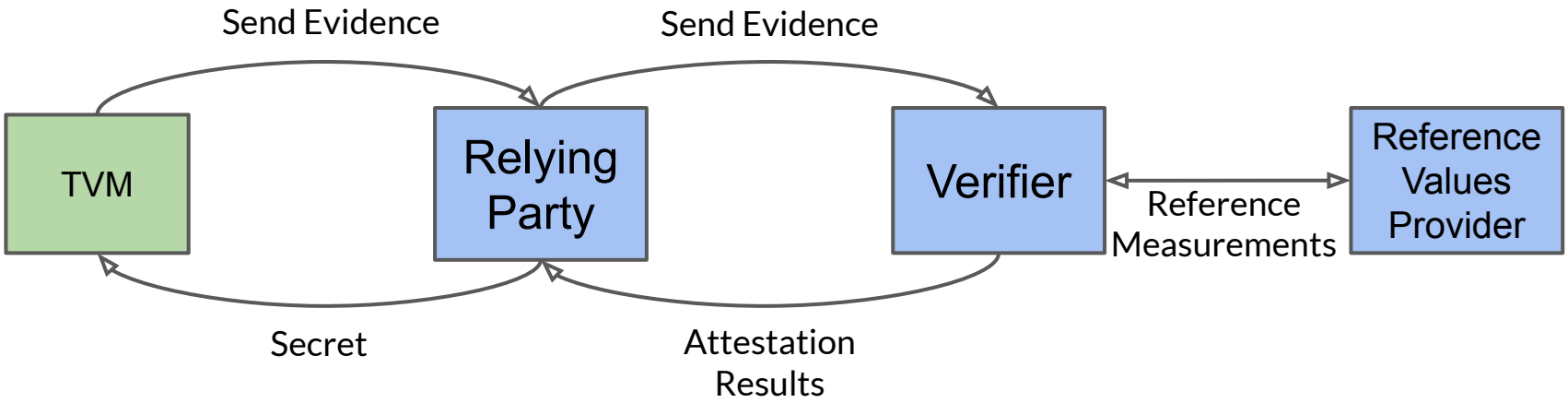
The IETF RATS Magic Box



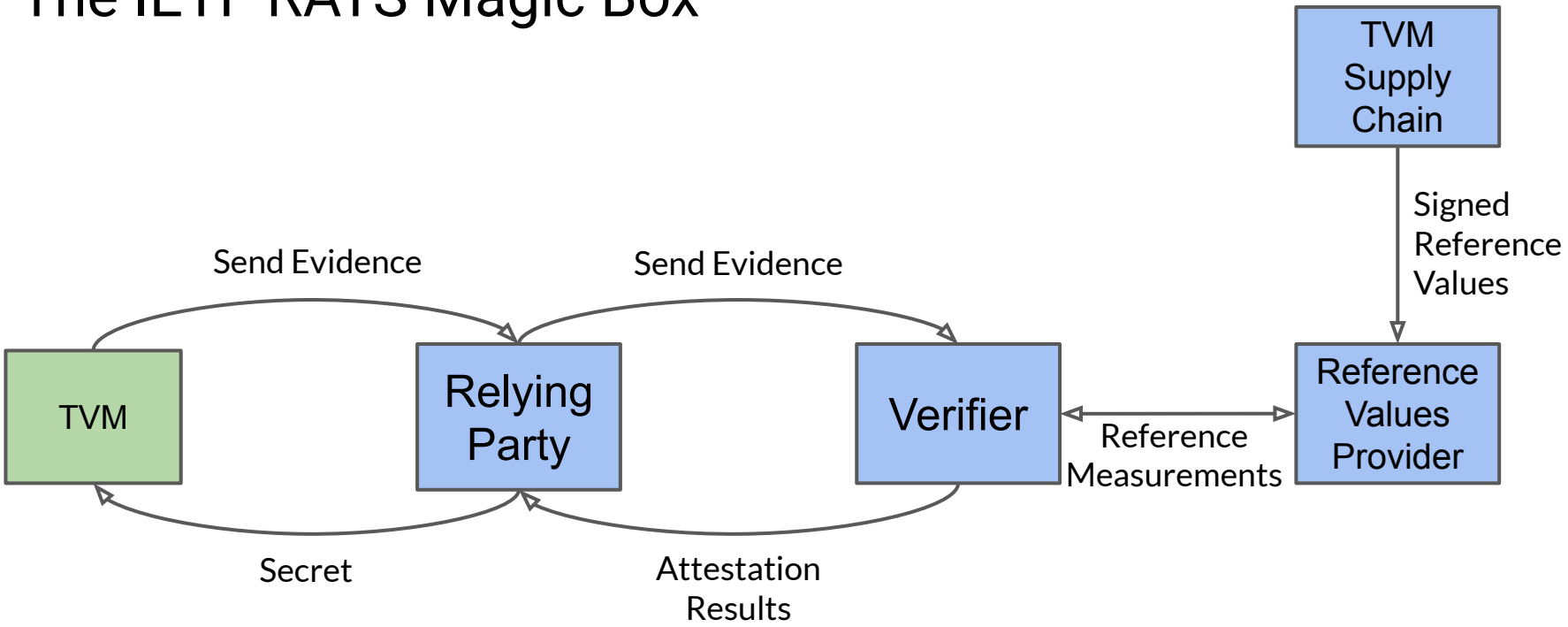
The IETF RATS Magic Box



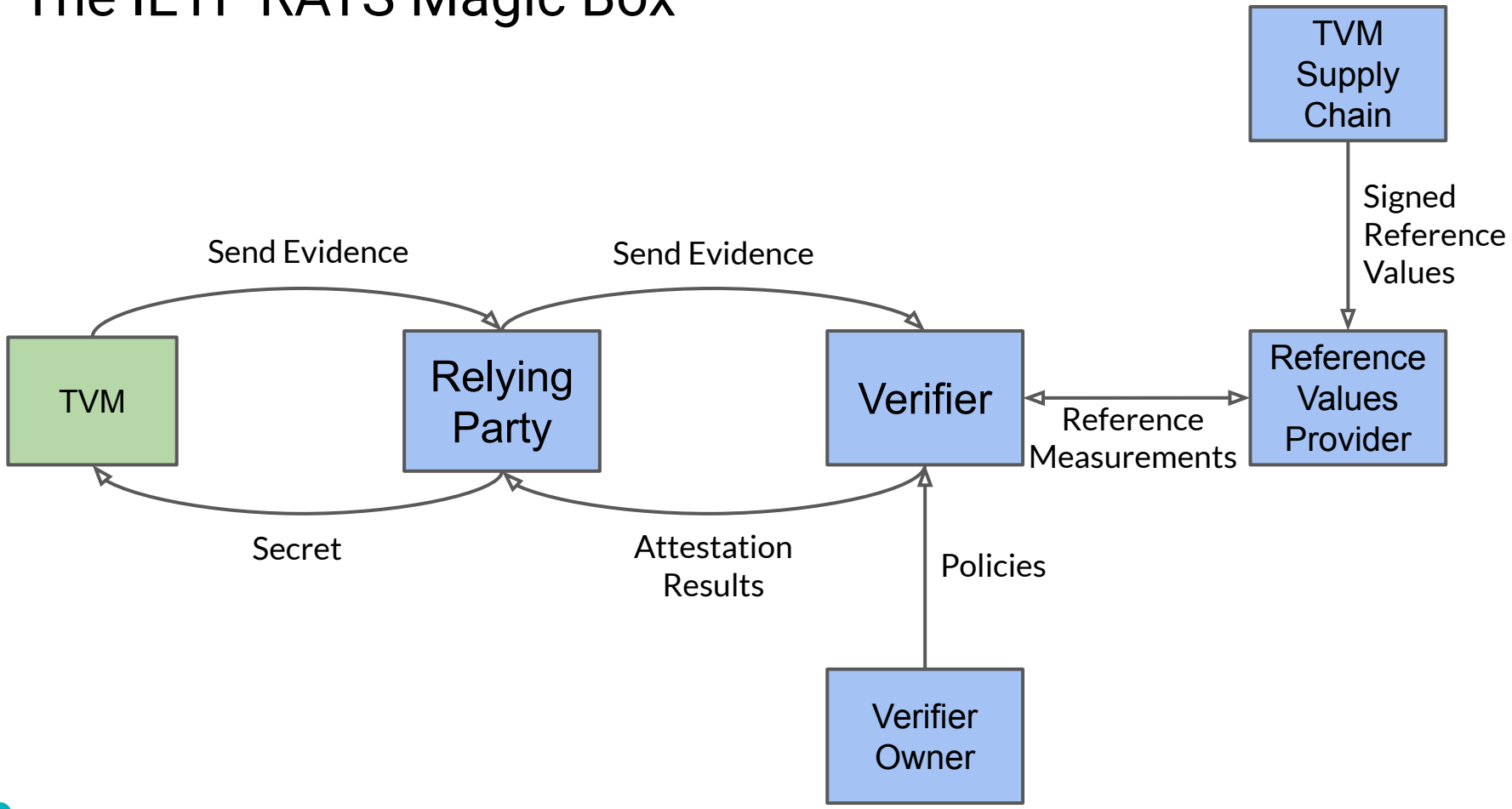
The IETF RATS Magic Box



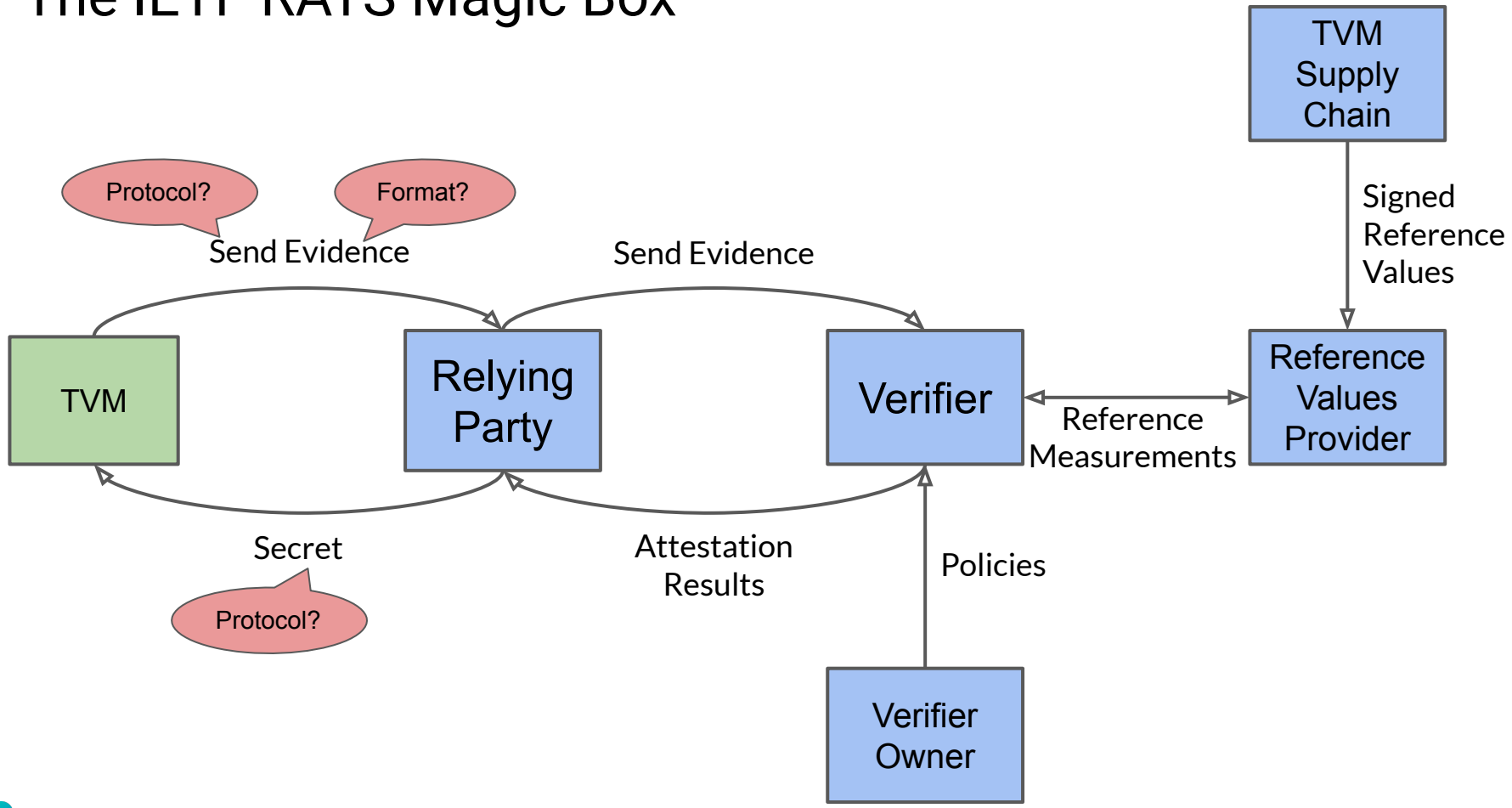
The IETF RATS Magic Box



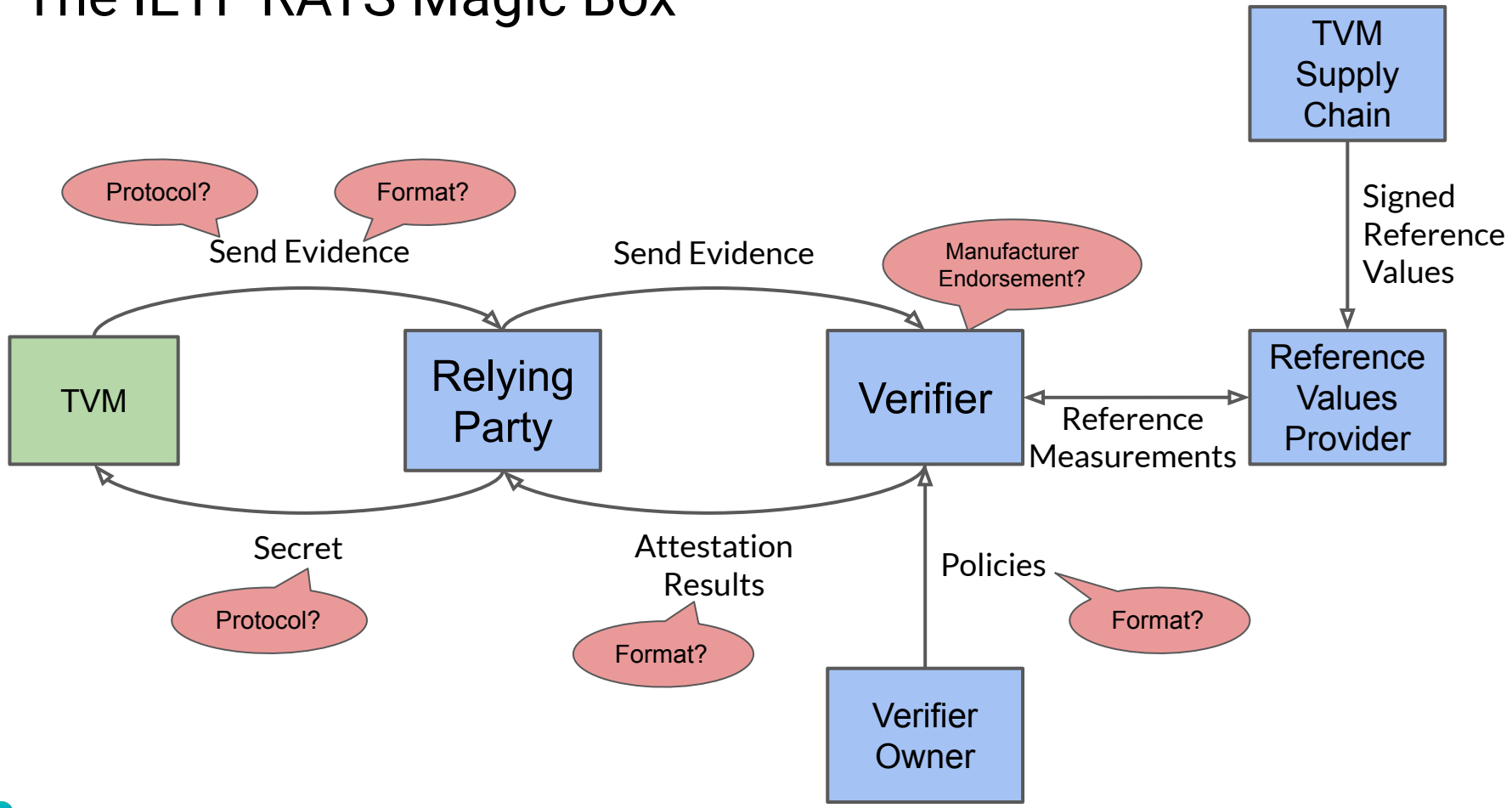
The IETF RATS Magic Box



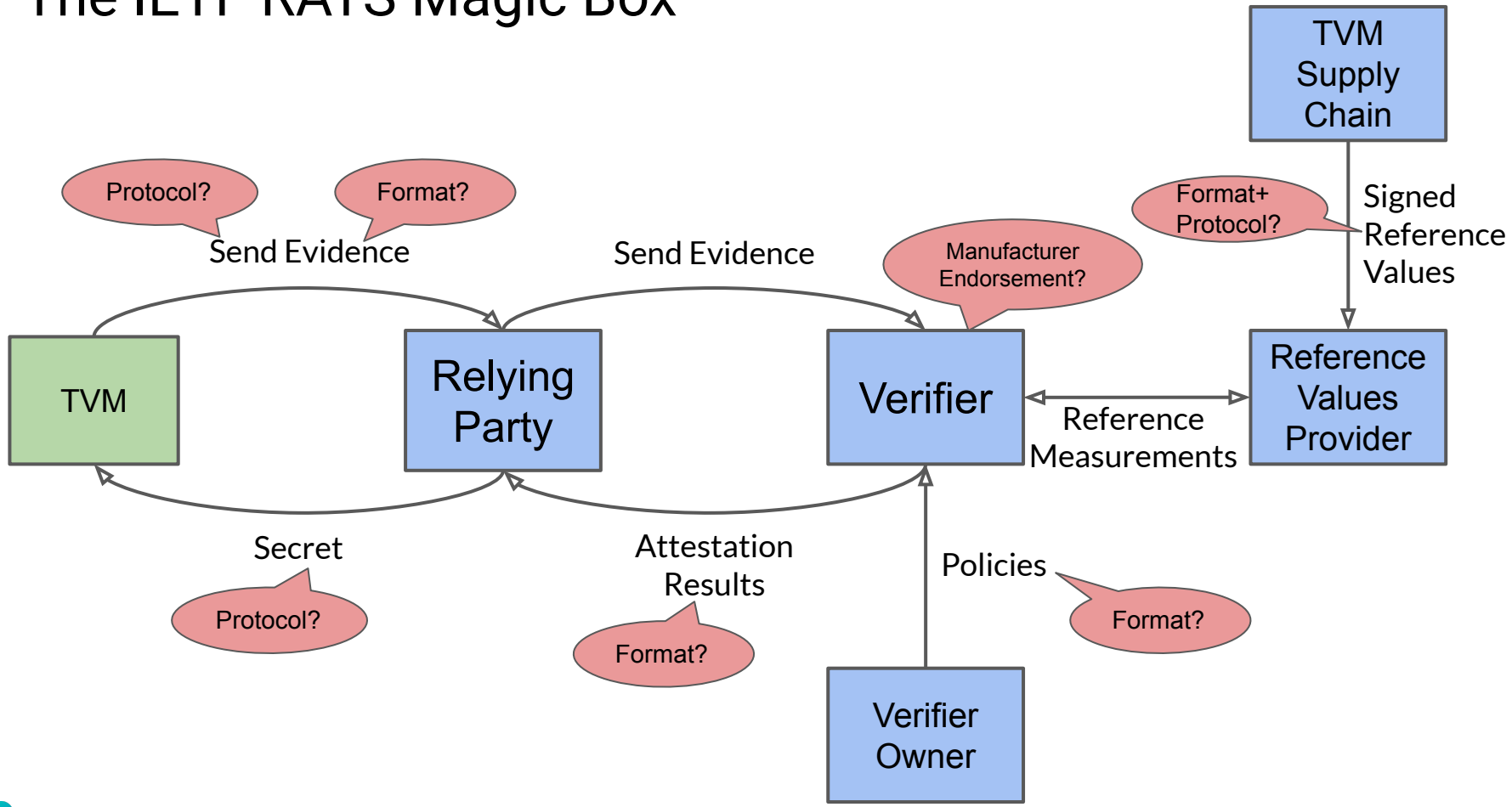
The IETF RATS Magic Box



The IETF RATS Magic Box



The IETF RATS Magic Box



End-to-End Confidential Computing

Platform enabling is only one part of the confidential computing chain…

- The rest is *“only”* about deploying and interacting with attestation services

Interfaces, protocols, formats, and manufacturer interactions are very fragmented

- Usually manufacturer or/and cloud provider specific
- Multiple IETF initiatives to clear the mess (RATS)

Plumbing an evidence into an attestation service is very challenging

The Confidential Containers Approach

Generic and open Interfaces, plugin architecture for existing manufacturer solutions

The Confidential Containers Approach

Generic and open Interfaces, plugin architecture for existing manufacturer solutions

Generic Relying Party protocol - KBS protocol (HTTPS & JSON Web Encryption)

Hardware agnostic Evidence format - TCG DICE or RATS EAT

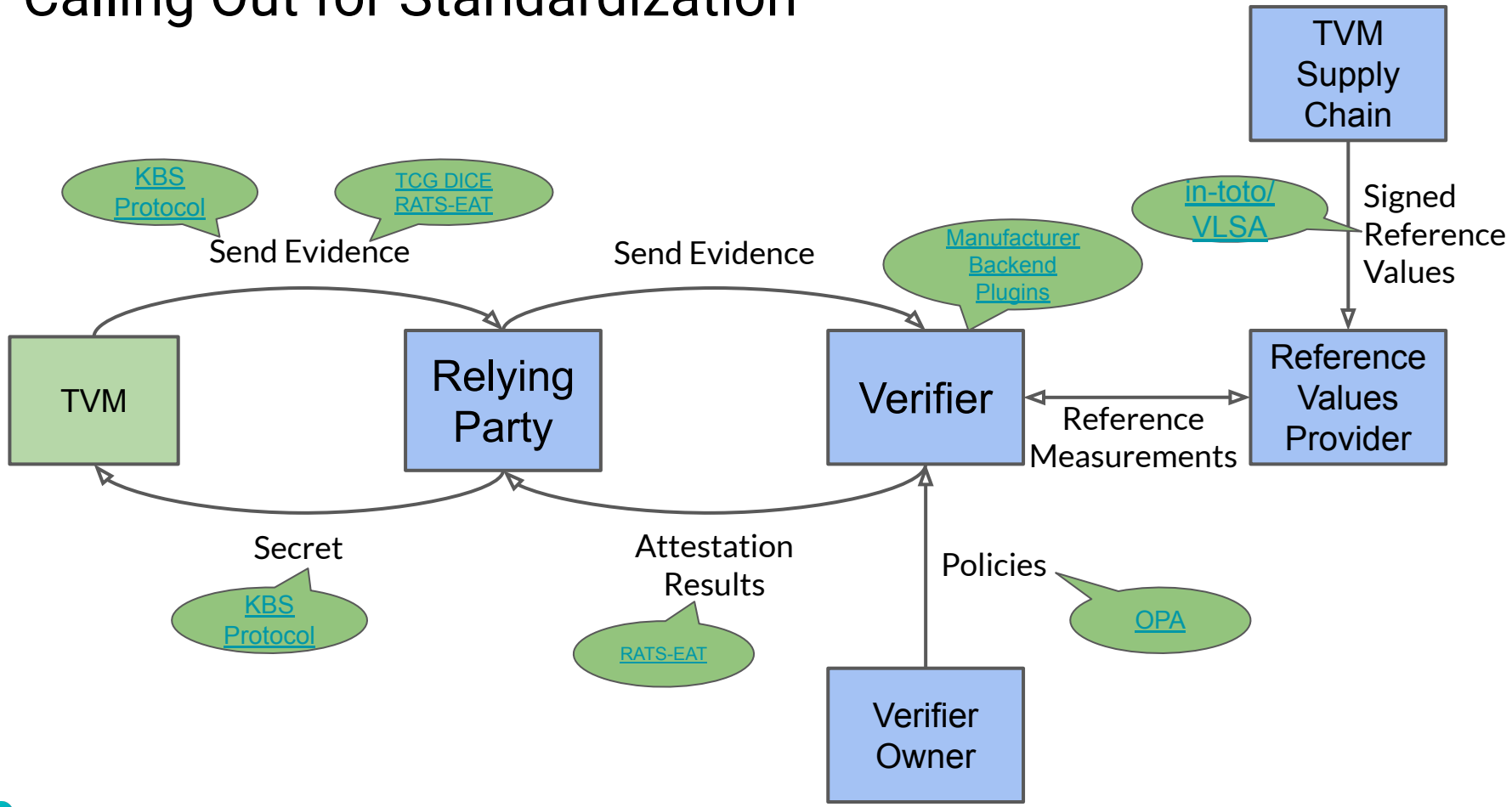
Manufacturer-pluggable Verifier architecture - Attestation Service framework

Manufacturer agnostic Reference Value Provider Service - The RVPS crate

With Support for modern and open source supply chain architectures - In-toto+SLSA

Open, cloud native format for Policies - Open Policy Agent

Calling Out for Standardization



Calling Out for Standardization

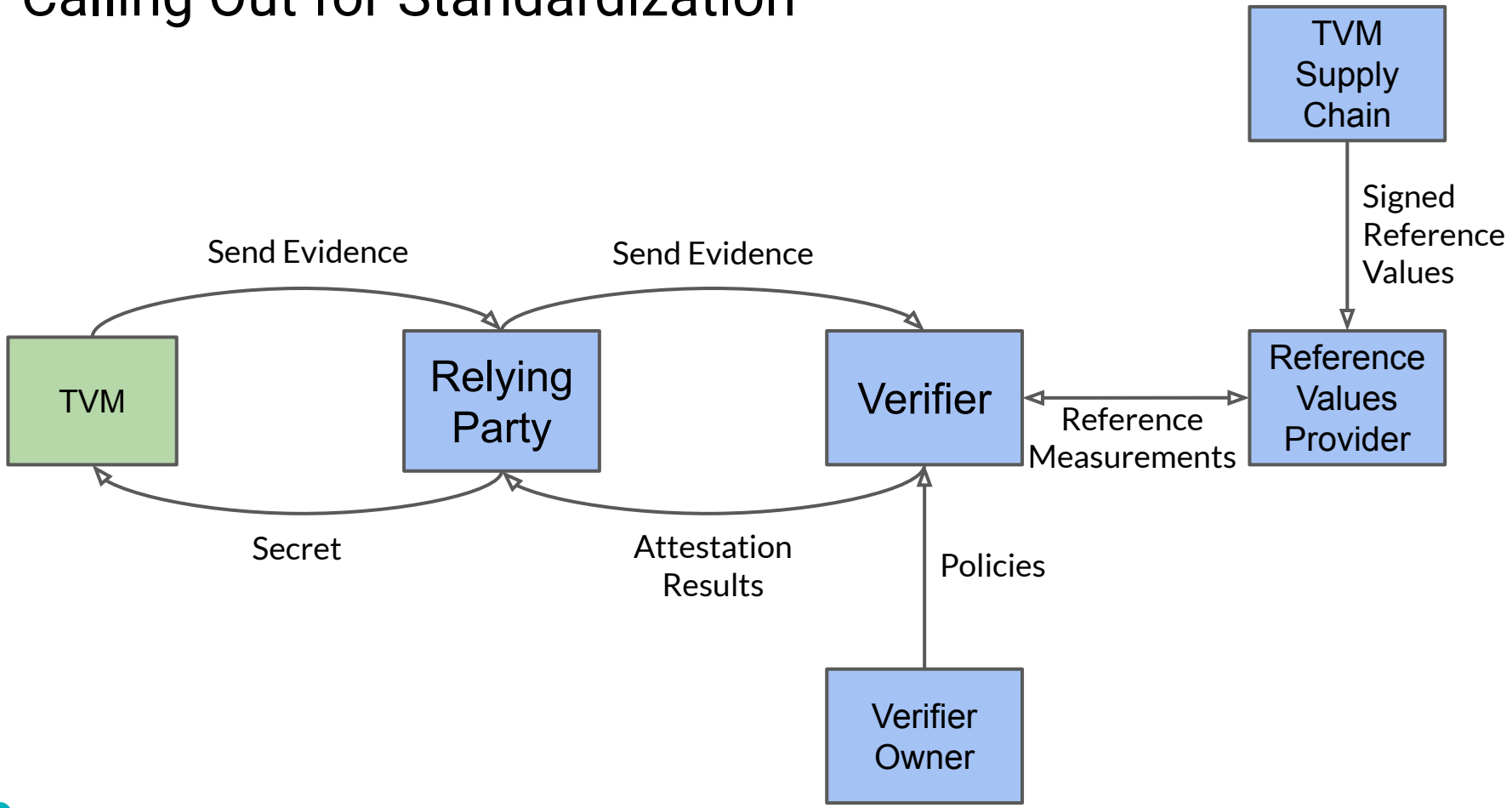
Let’s make the next confidential computing software stack simpler…

Simplify the interfaces between the TVM and the Relying Party

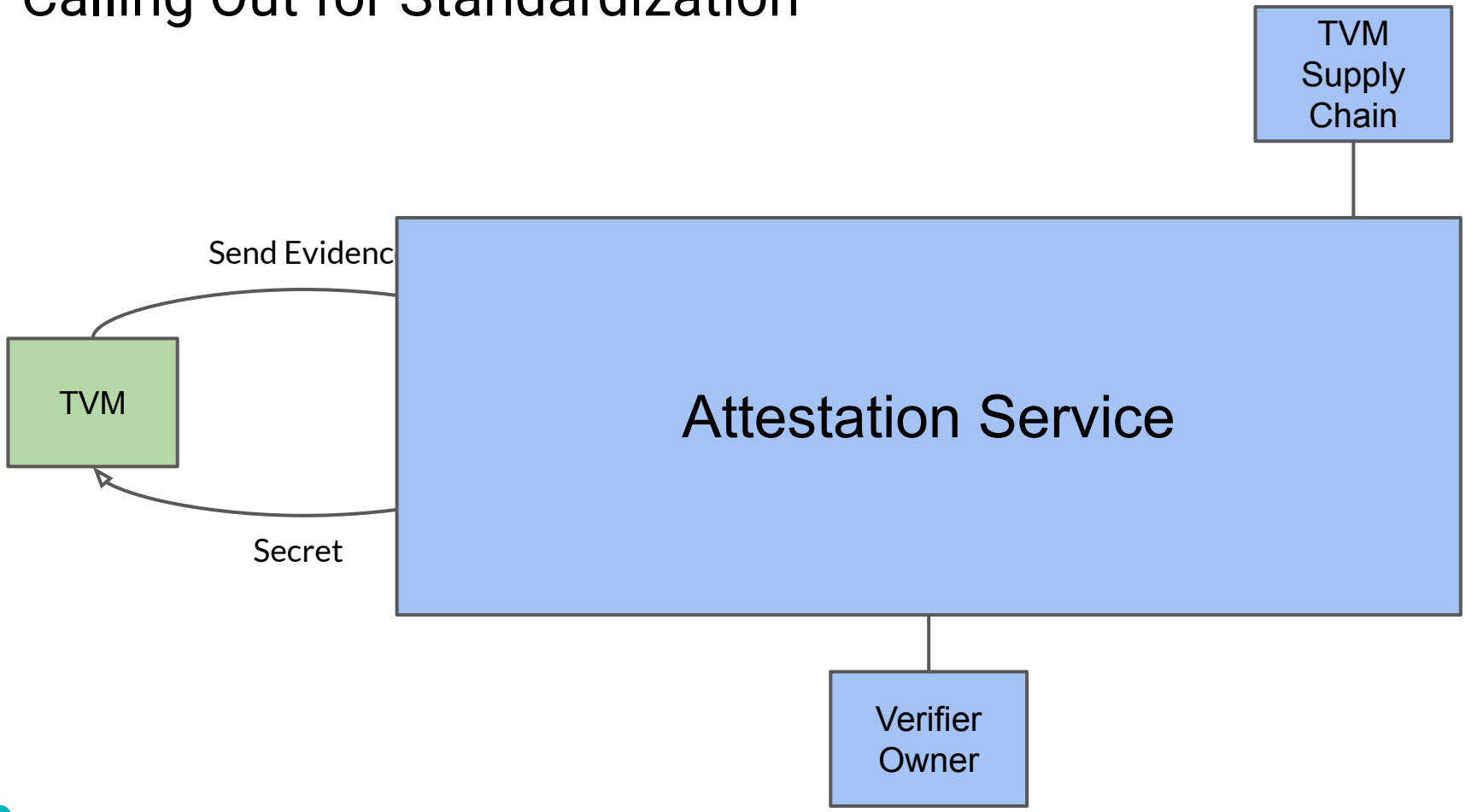
Simplify the interaction between the supply chain and the Relying Party

Simplify the verification policies description

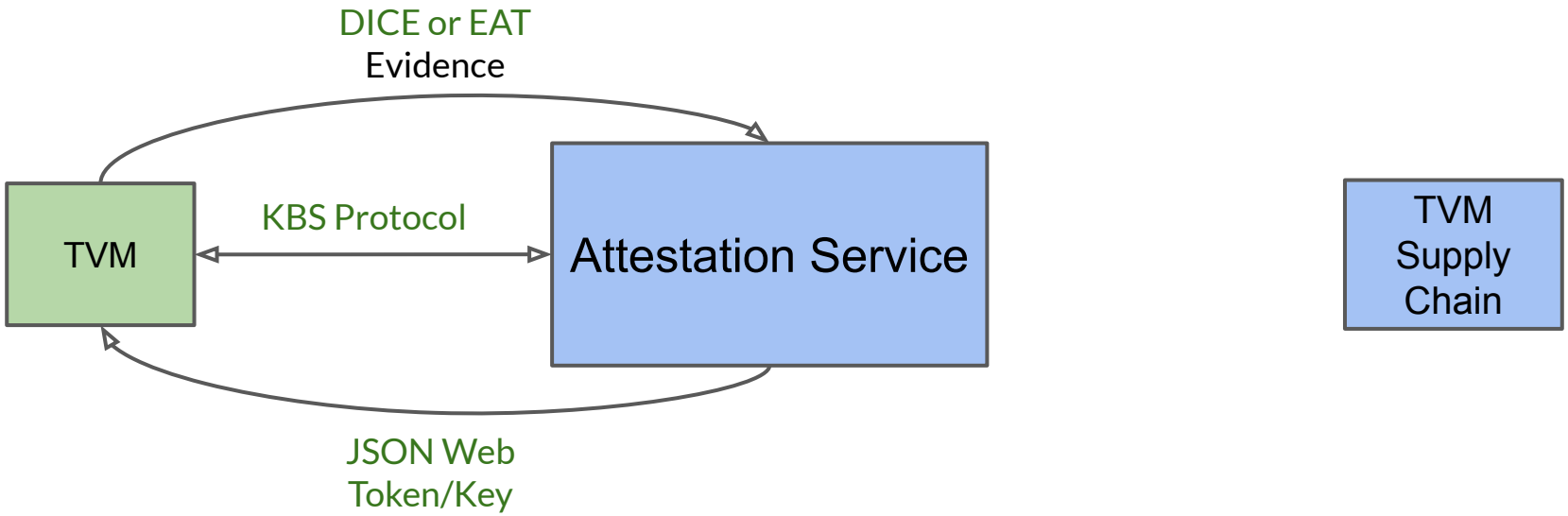
Calling Out for Standardization



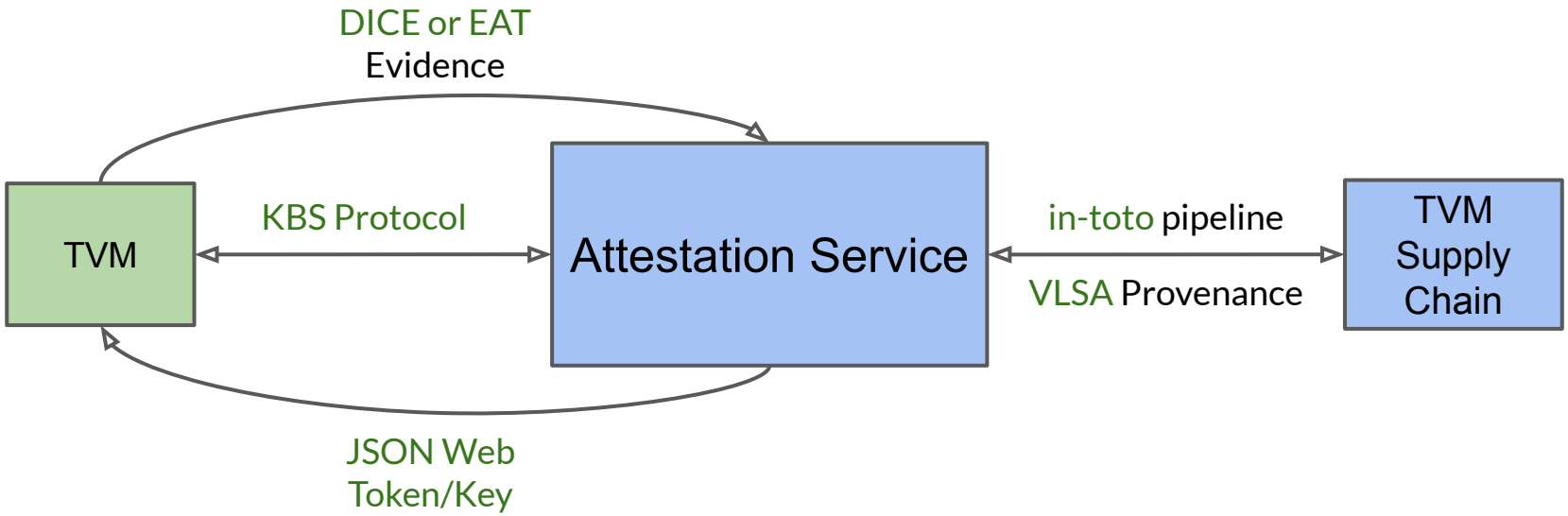
Calling Out for Standardization



Calling Out for Standardization



Calling Out for Standardization



Calling Out for Standardization