Veraison

An open-source toolbox for verification of attestation evidence

https://github.com/veraison

Trivia

- VERAISON 
- Winemaking term
- IPA: veʁɛzɔ̃
- Backronym for "VERificAtIon of atteStatiON"
- Arm ATG ➡ Confidential Computing Consortium (LF)
- open-source, open-governance

Useful Pointers

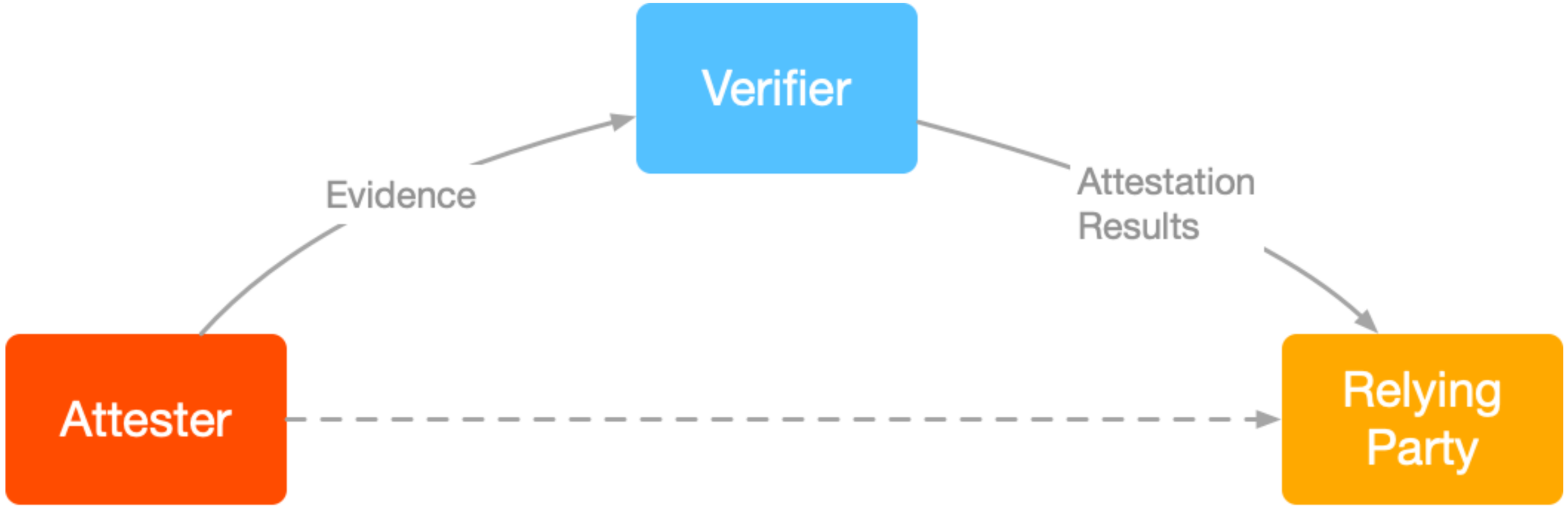
- https://github.com/veraison
- https://veraison.zulipchat.org/veraison
- https://lists.confidentialcomputing.io/g/veraison
- https://armltd.zoom.us/j/93024860563?pwd=dVpVcFRtSVFmV29HV3dHWENrZk5WQT09

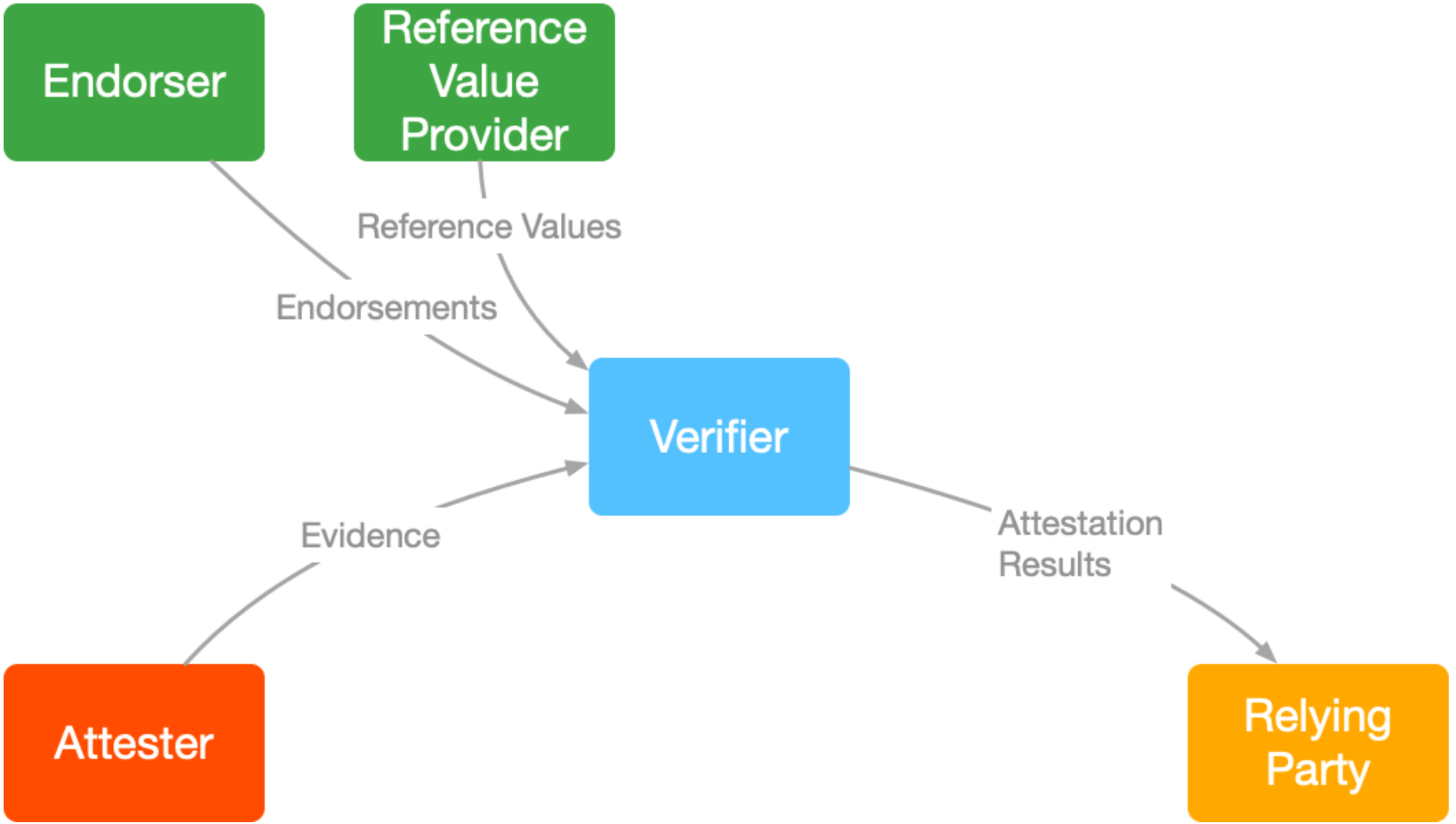
Remote Attestation Recap

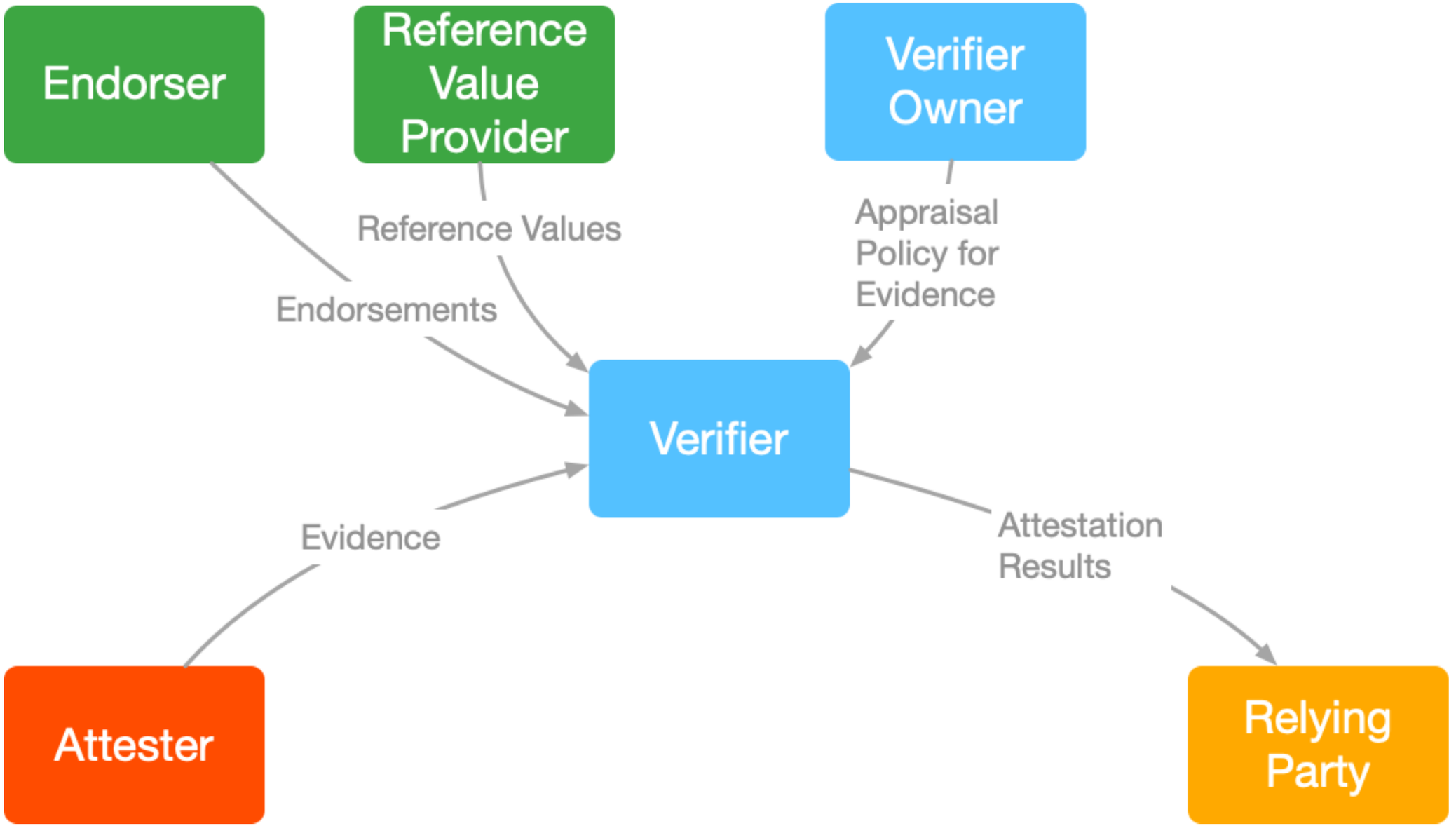

Attester
Relying Party

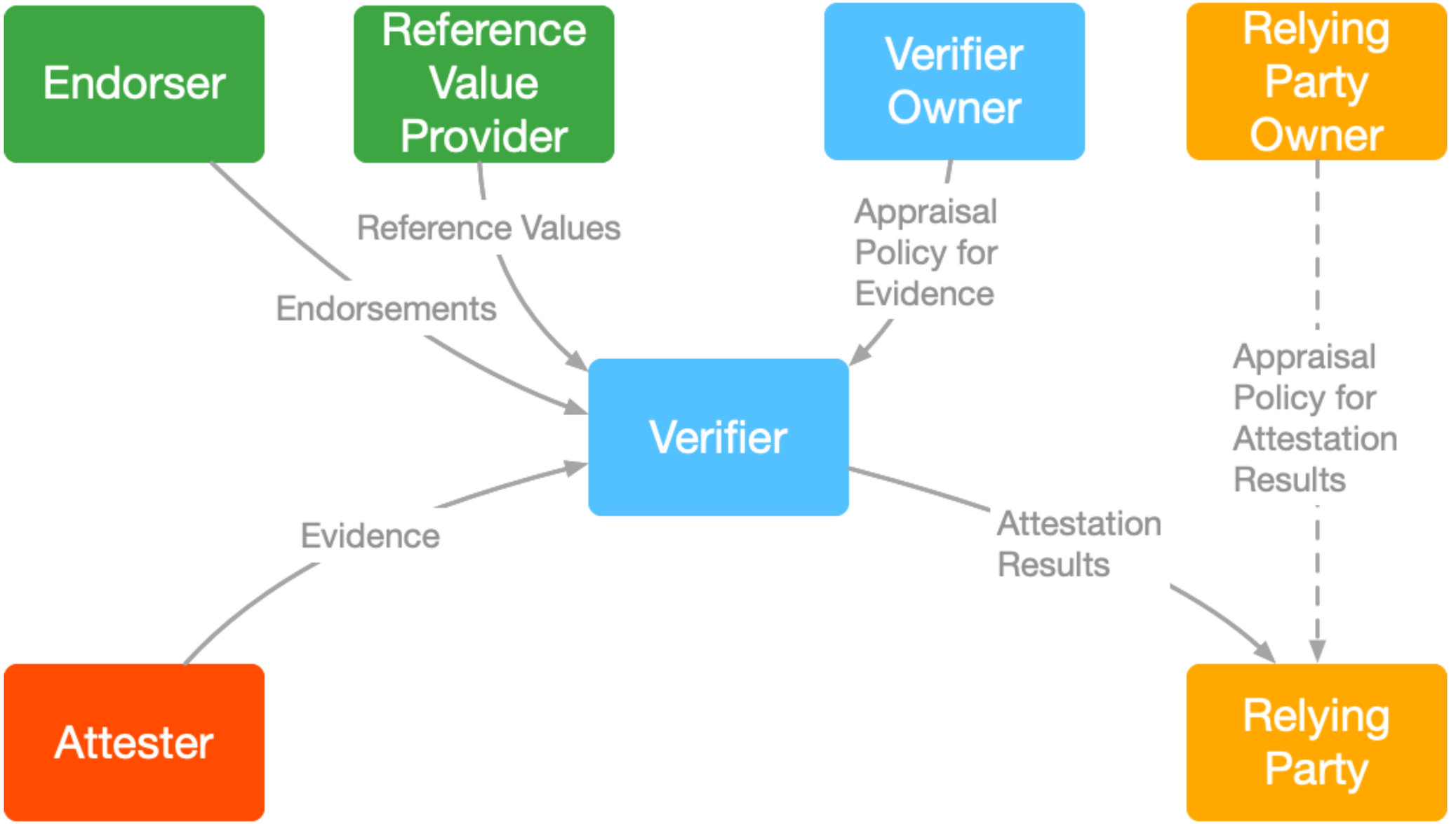

Attester
Relying Party


Attester
Evidence
Relying Party

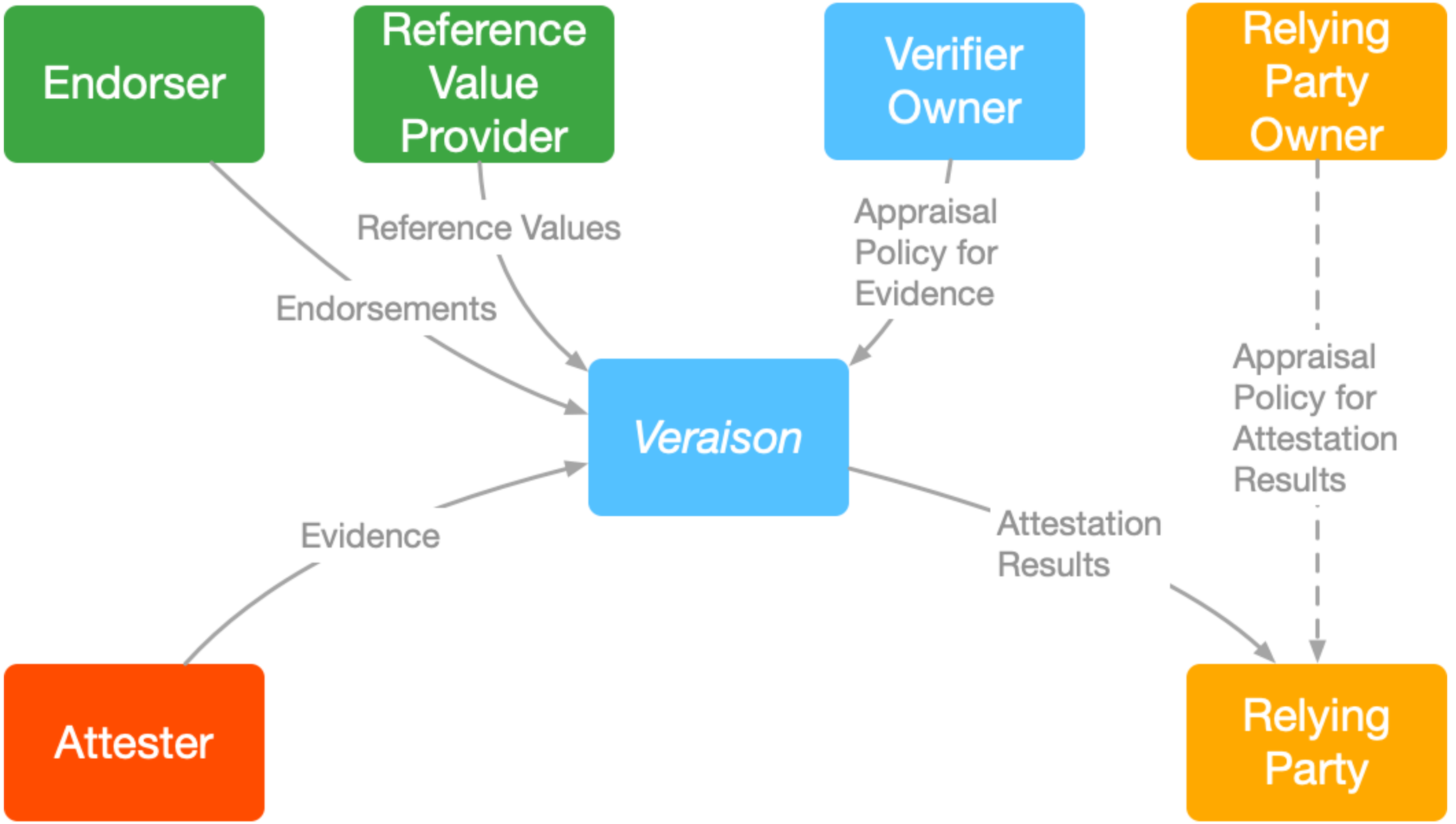

Verifier
Evidence
Attestation
Results
Attester
Relying
Party

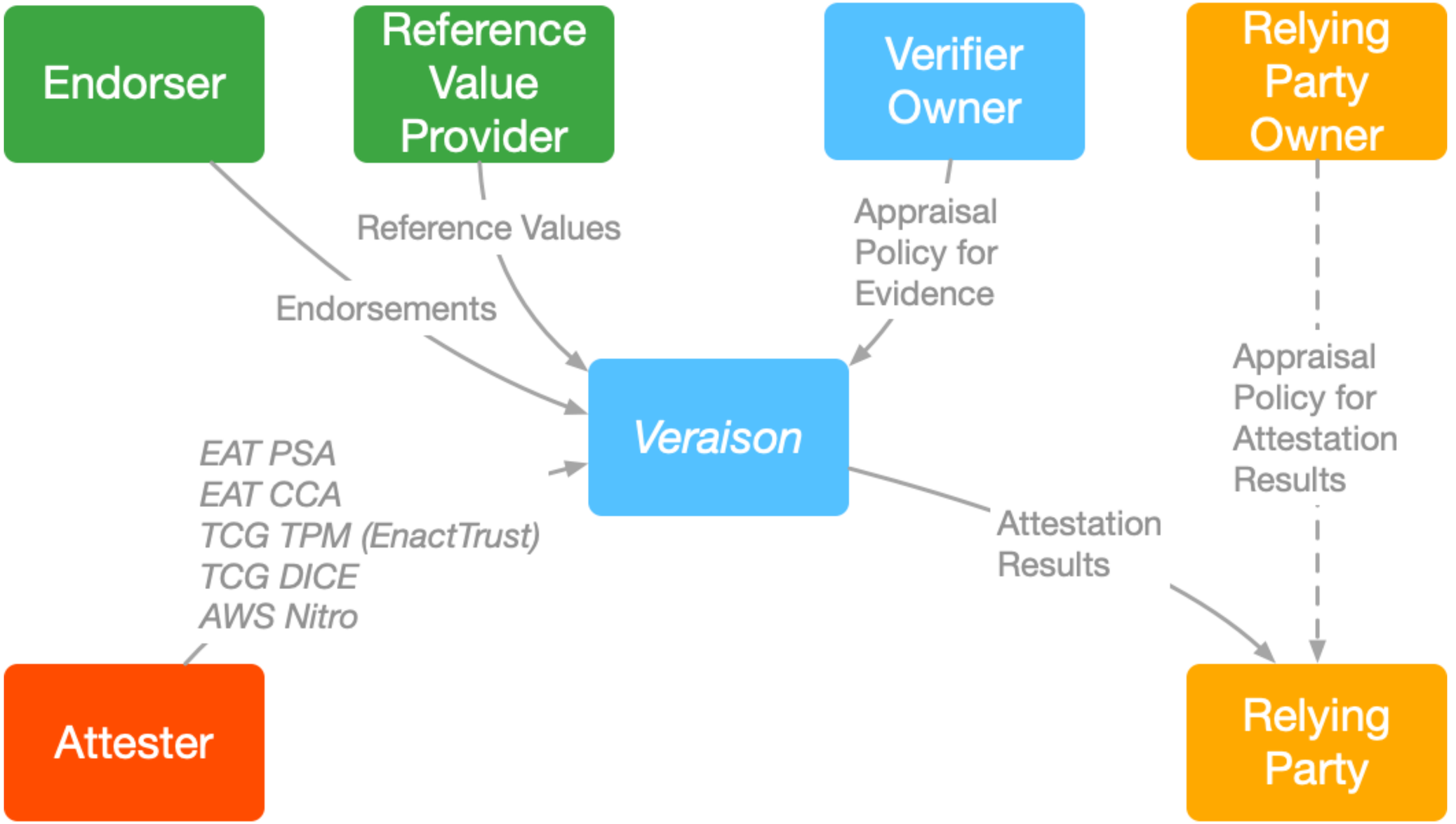

Endorser
Reference Value Provider
Reference Values
Endorsements
Verifier
Evidence
Attestation Results
Attester
Relying Party

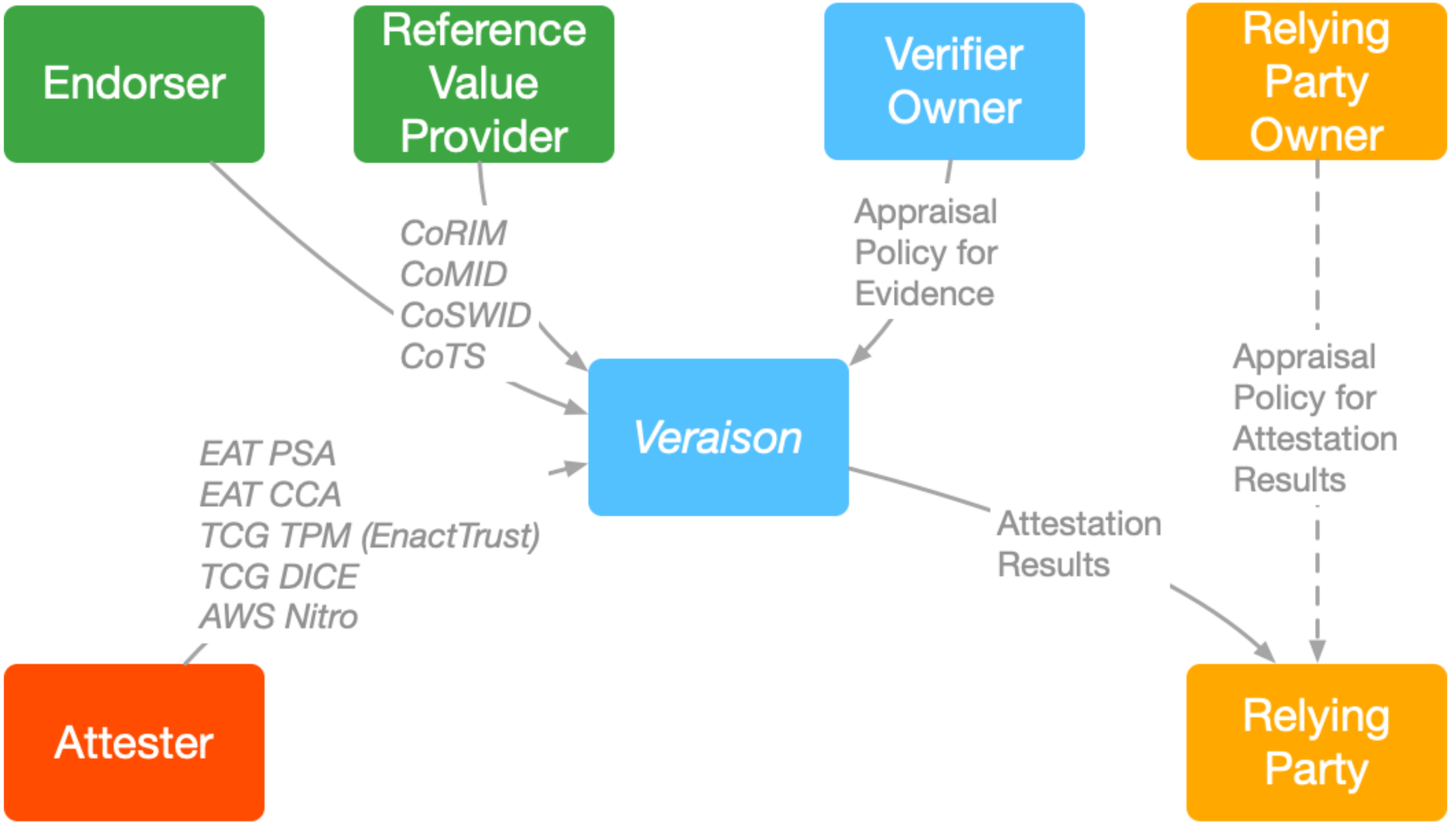

Endorser
Reference Value Provider
Verifier Owner
Reference Values
Appraisal Policy for Evidence
Endorsements
Verifier
Evidence
Attestation Results
Attester
Relying Party

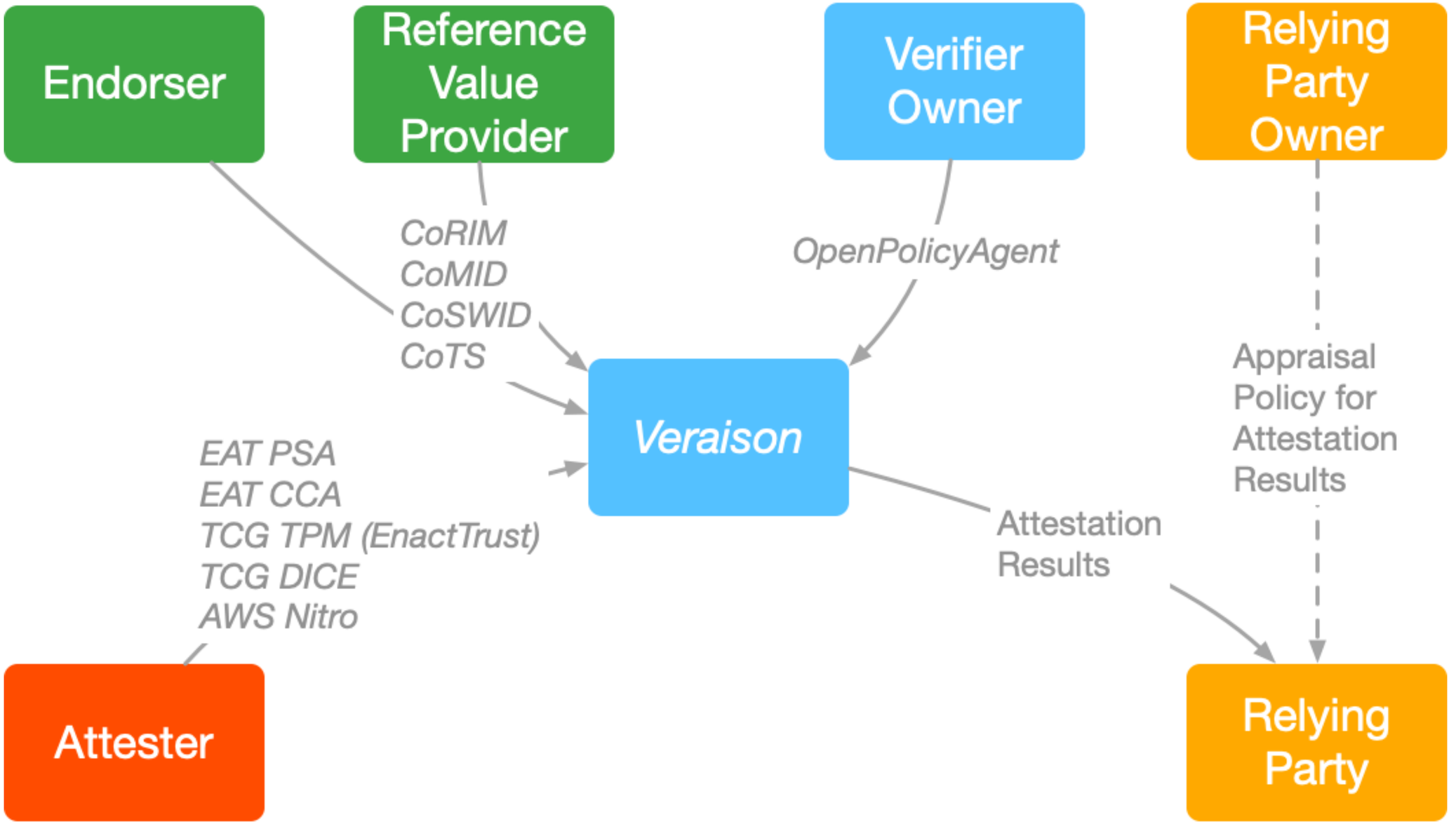

Endorser
Reference Value Provider
Verifier Owner
Relying Party Owner
Reference Values
Appraisal Policy for Evidence
Endorsements
Verifier
Appraisal Policy for Attestation Results
Evidence
Attestation Results
Attester
Relying Party

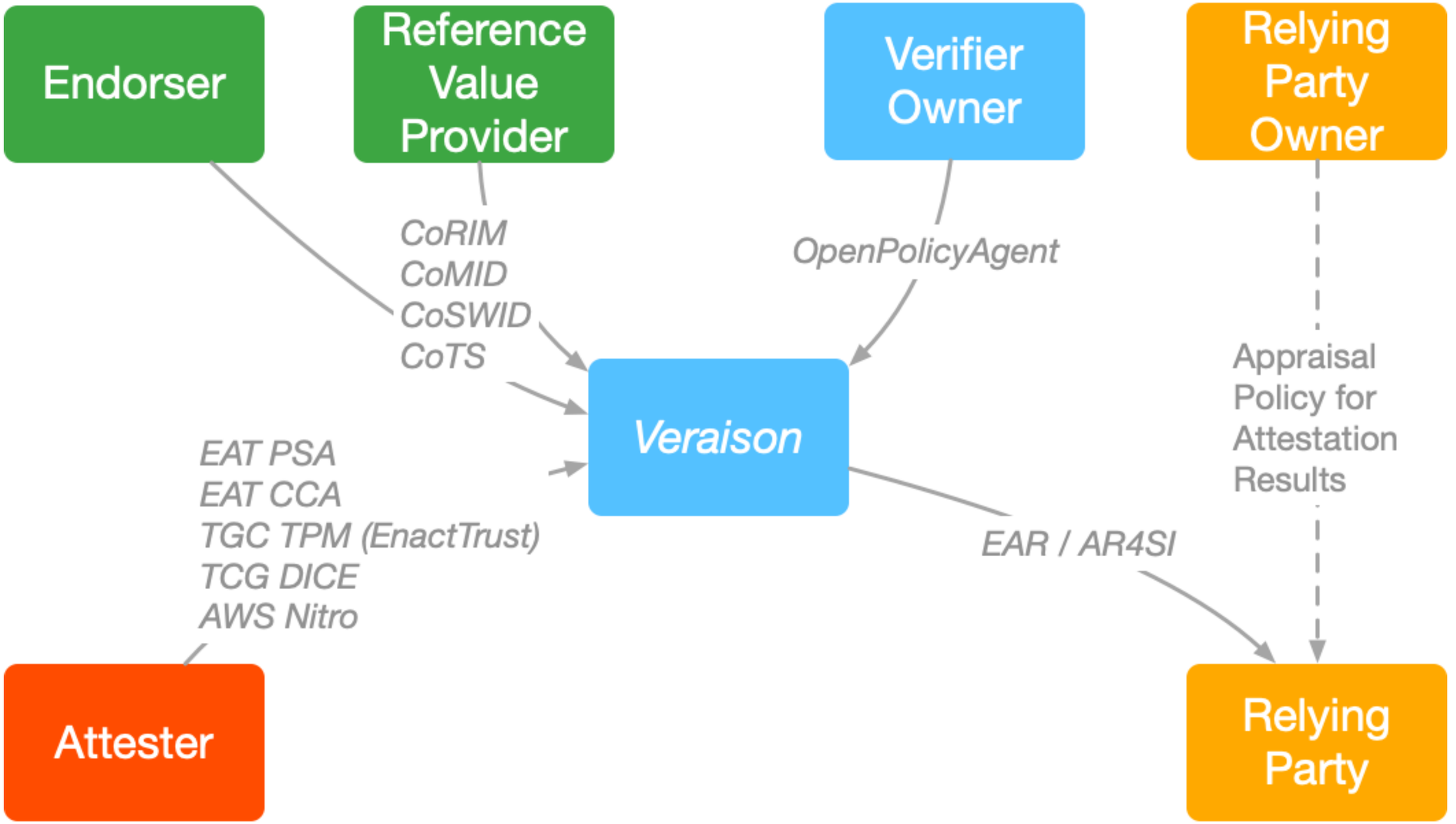
What is Veraison

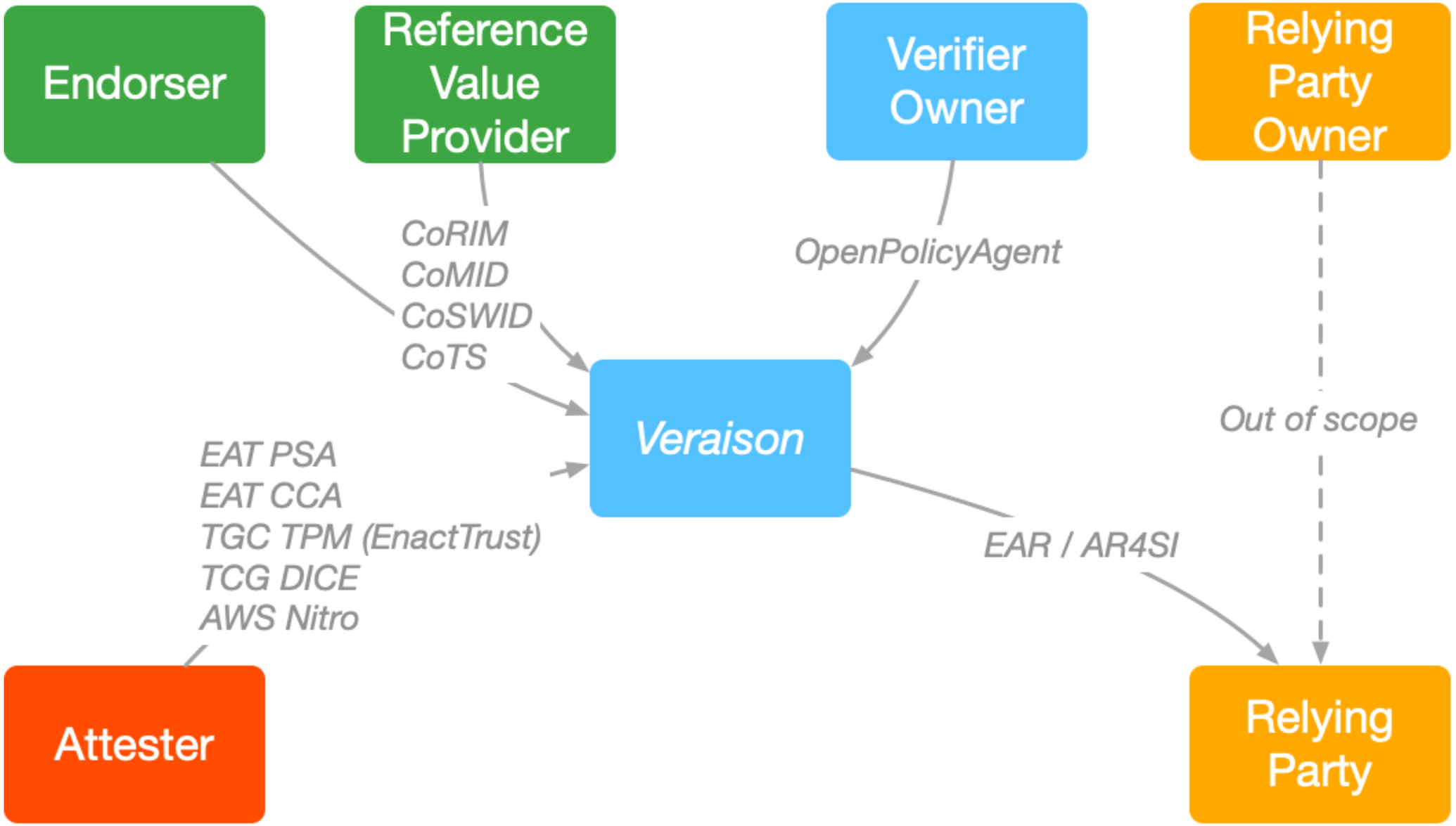

Endorser
Reference Value Provider
Verifier Owner
Relying Party Owner
Reference Values
Appraisal Policy for Evidence
Endorsements
Appraisal Policy for Attestation Results
Veraison
Evidence
Attestation Results
Attester
Relying Party


Endorser
Reference Value Provider
Verifier Owner
Relying Party Owner
Reference Values
Endorsements
Appraisal Policy for Evidence
Appraisal Policy for Attestation Results
Veraison
EAT PSA
EAT CCA
TCG TPM (EnactTrust)
TCG DICE
AWS Nitro
Attestation Results
Attester
Relying Party


Endorser
Reference Value Provider
Verifier Owner
Relying Party Owner
CoRIM
CoMID
CoSWID
CoTS
Appraisal Policy for Evidence
Appraisal Policy for Attestation Results
Veraison
EAT PSA
EAT CCA
TCG TPM (EnactTrust)
TCG DICE
AWS Nitro
Attestation Results
Attester
Relying Party

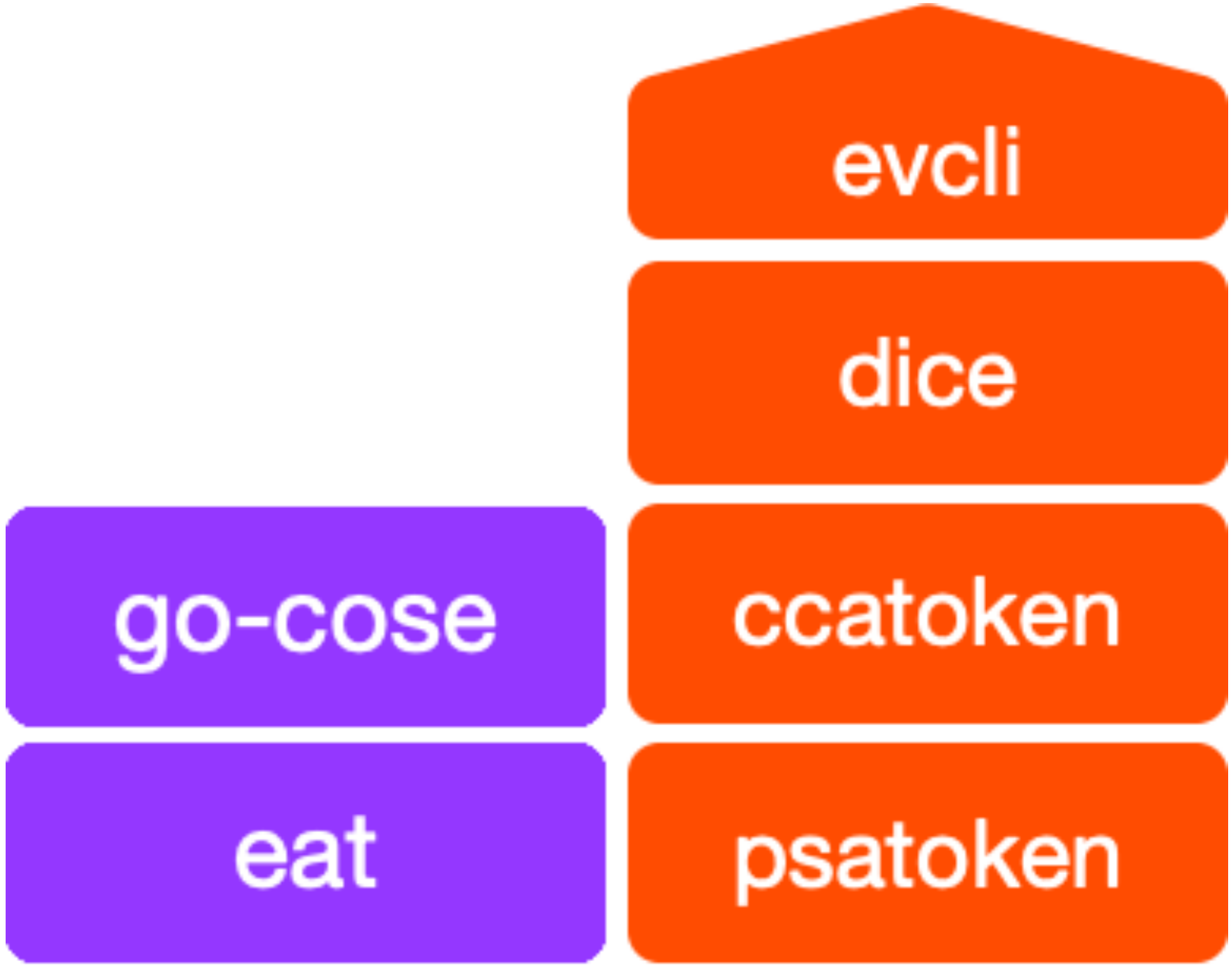

Endorser
Reference Value Provider
Verifier Owner
Relying Party Owner
CoRIM
CoMID
CoSWID
CoTS
OpenPolicyAgent
Appraisal Policy for Attestation Results
Veraison
EAT PSA
EAT CCA
TCG TPM (EnactTrust)
TCG DICE
AWS Nitro
Attestation Results
Attester
Relying Party

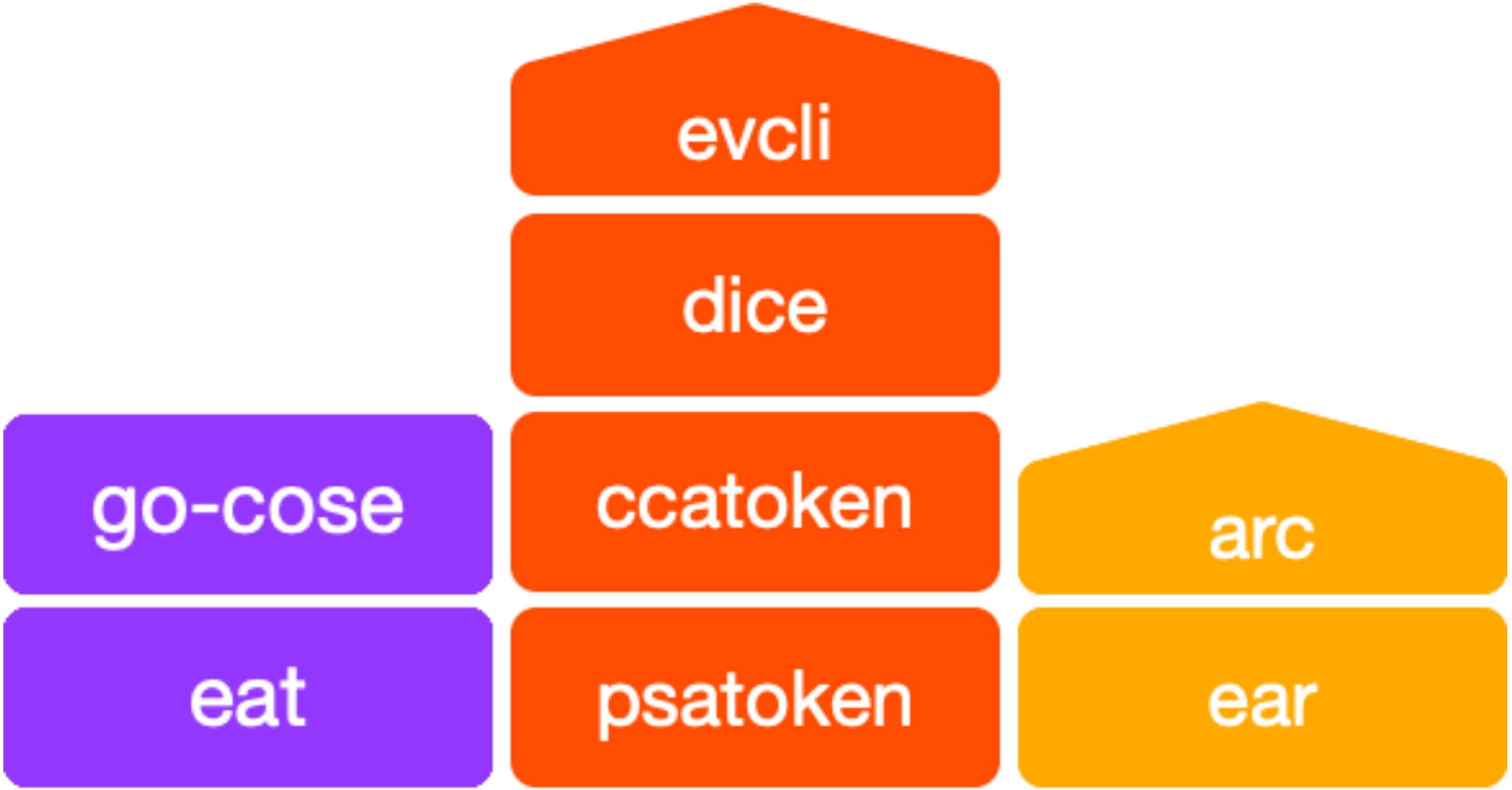

Endorser
Reference Value Provider
Verifier Owner
Relying Party Owner
CoRIM
CoMID
CoSWID
CoTS
OpenPolicyAgent
Appraisal Policy for Attestation Results
Veraison
EAT PSA
EAT CCA
TGC TPM (EnactTrust)
TCG DICE
AWS Nitro
EAR / AR4SI
Attester
Relying Party

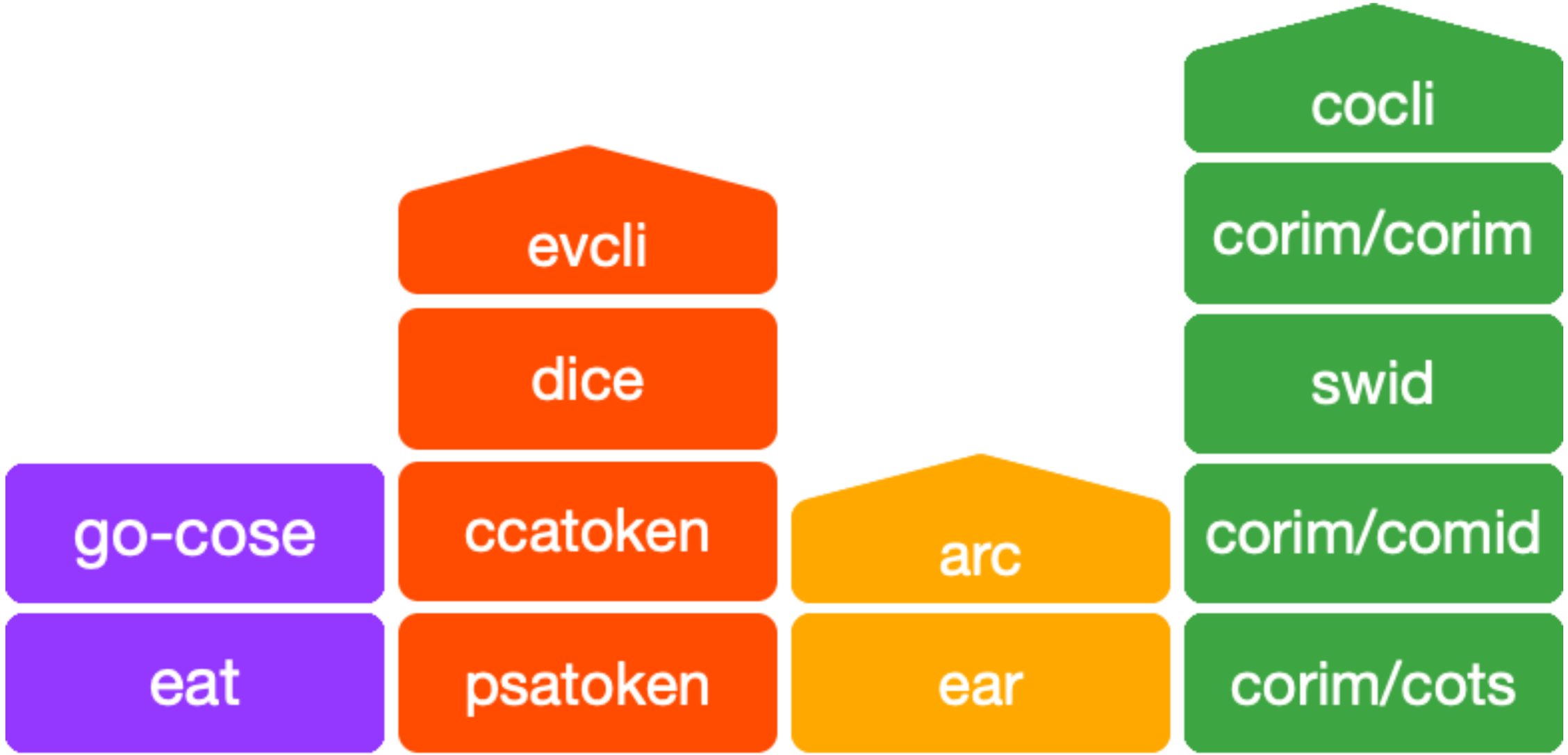

Endorser
Reference Value Provider
Verifier Owner
Relying Party Owner
CoRIM
CoMID
CoSWID
CoTS
OpenPolicyAgent
Veraison
Out of scope
EAT PSA
EAT CCA
TGC TPM (EnactTrust)
TCG DICE
AWS Nitro
EAR / AR4SI
Attester
Relying Party

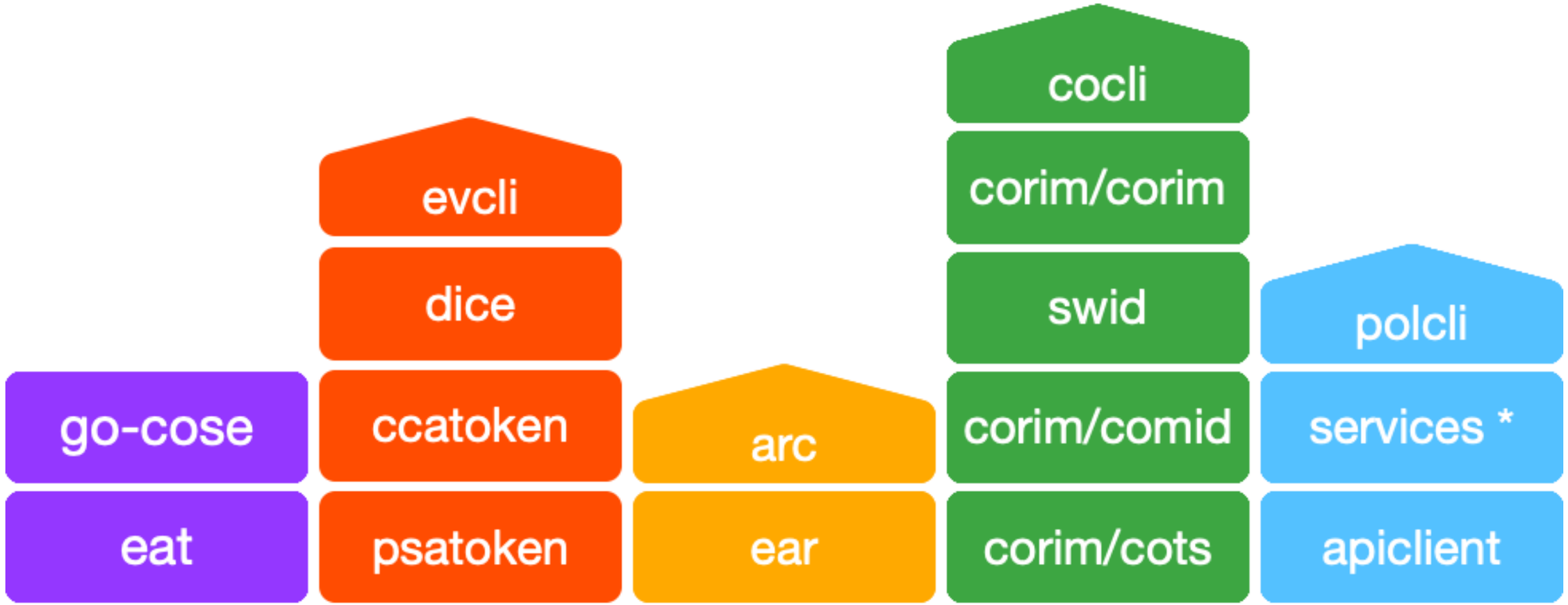
Packages Atlas


go-cose
eat

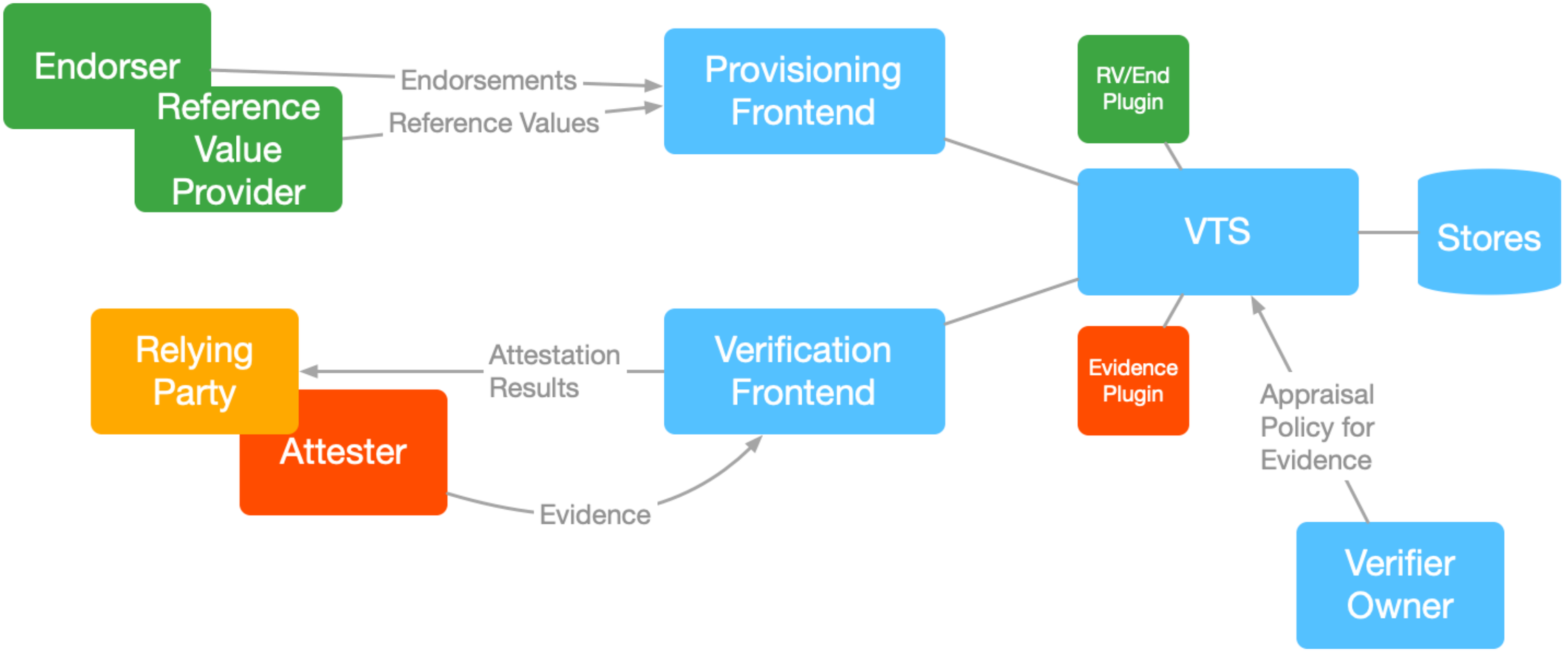

evcli
dice
go-cose
ccatoken
eat
psatoken


evcli
dice
go-cose
ccatoken
arc
eat
psatoken
ear


cocli
evcli
corim/corim
dice
swid
go-cose
ccatoken
arc
corim/comid
eat
psatoken
ear
corim/cots


cocli
evcli
corim/corim
dice
swid
polcli
go-cose
ccatoken
arc
corim/comid
services *
eat
psatoken
ear
corim/cots
apiclient

Services (current) Architecture


Endorser
Reference Value Provider
Endorsements
Reference Values
Provisioning Frontend
RV/End Plugin
VTS
Stores
Relying Party
Attester
Attestation Results
Verification Frontend
Evidence Plugin
Appraisal Policy for Evidence
Evidence
Verifier Owner

Next steps

- add new formats
- improve documentation
- work on IAM to support a multi-tenant service
- allow static ("plugin-less") build

Questions