CISCO SECURE

The bridge to possible

Attestations for Trusted Path Routing

Nancy Cam-Winget, Cisco Fellow
Cisco Systems, Security Business Group Office of the CTO

November 14, 2023

Critically Private Customer IP Flows

Government

Finance

Military

Medical

Concerns

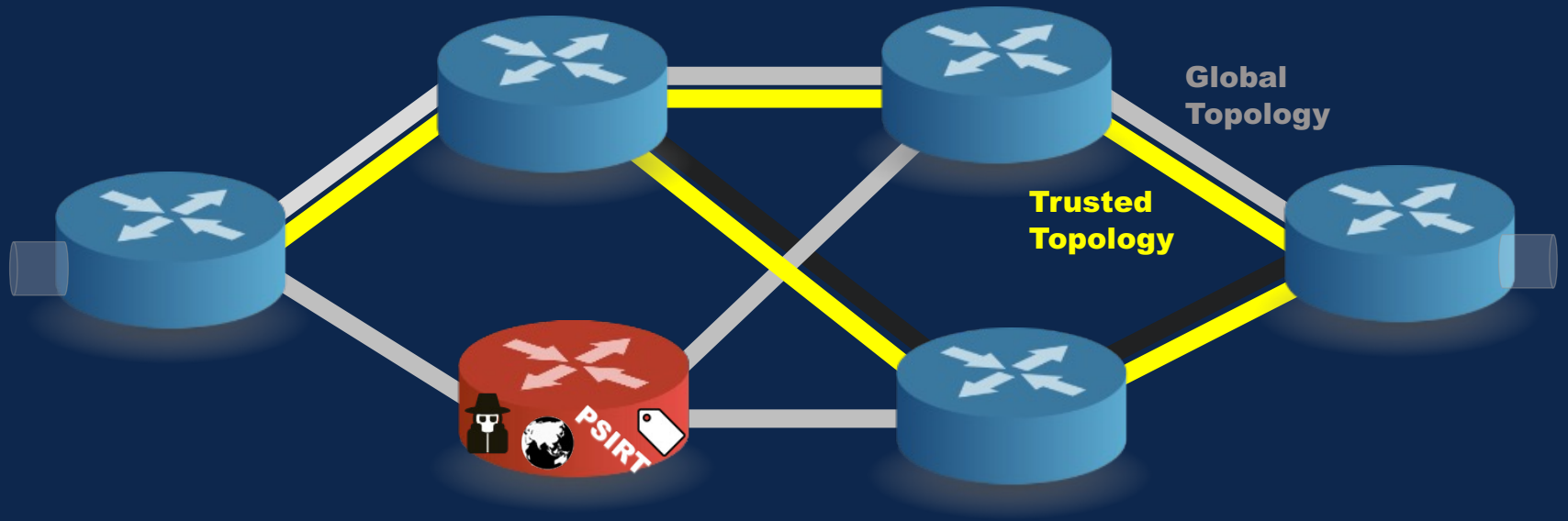
- Keys can be stolen/broken
- Source+destination visibility is info leakage
- Quantum Decryption?

Bypass less Trustworthy Routers

- Untrustworthy vendor
- Unpatched code
- Boot Integrity Fail
- Active compromise underway

Trusted Path Routing

- At edge, regular flows & critically private flows mixed
- Critically private flows forwarded into Trusted Topology

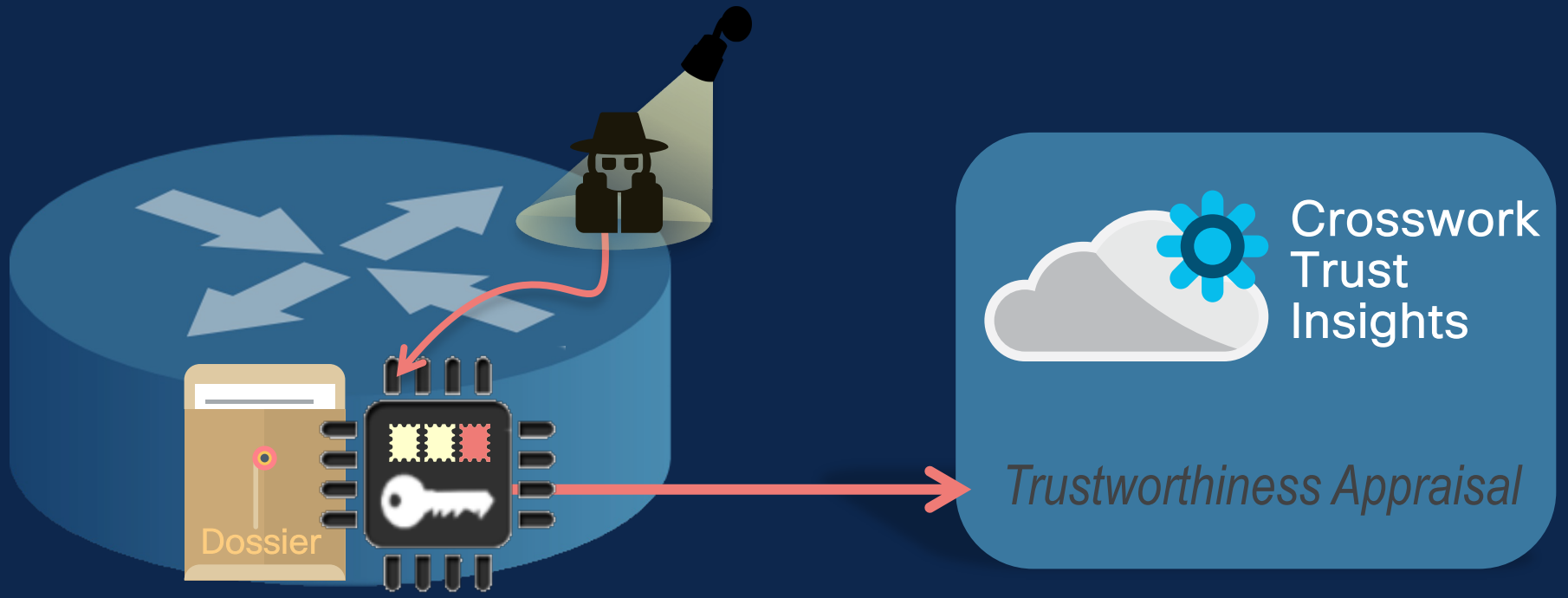


- Critically private flows don’t transit less secure devices

Remote Attestations: IETF RFC 9334

In Remote ATtestation procedureS (RATS), one peer (the "Attester") produces believable information about itself ("Evidence") to enable a remote peer (the "Relying Party") to decide whether or not to consider that Attester a trustworthy peer. Remote attestation procedures are facilitated by an additional vital party (the "Verifier").

Remote Attestation in Routers



Logs & Cryptoprocessor (TAm)
Secured Router Measurements

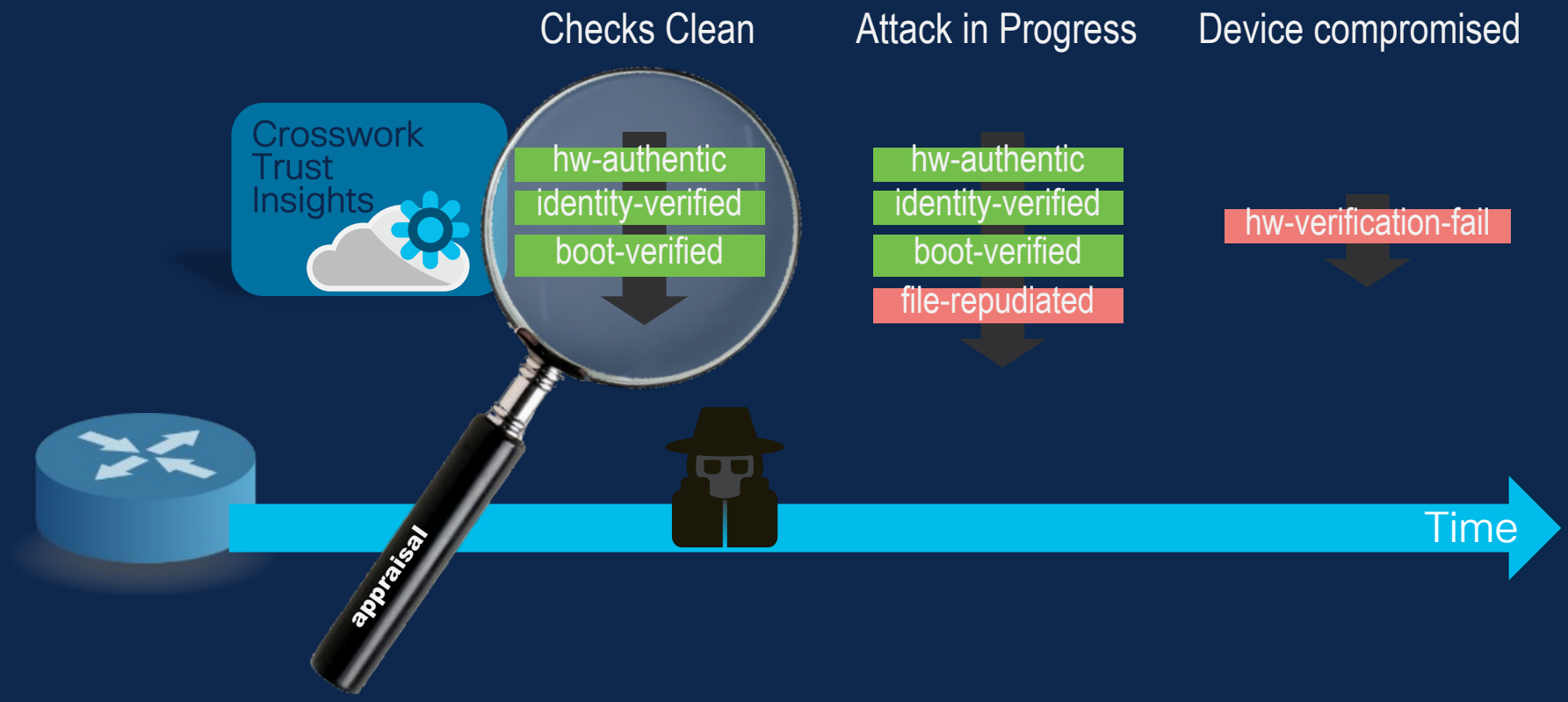
- Hardware Tampering
- BIOS/ROMmon Attacks
- Software Image Attacks
- Runtime Attacks

Trustworthiness Level

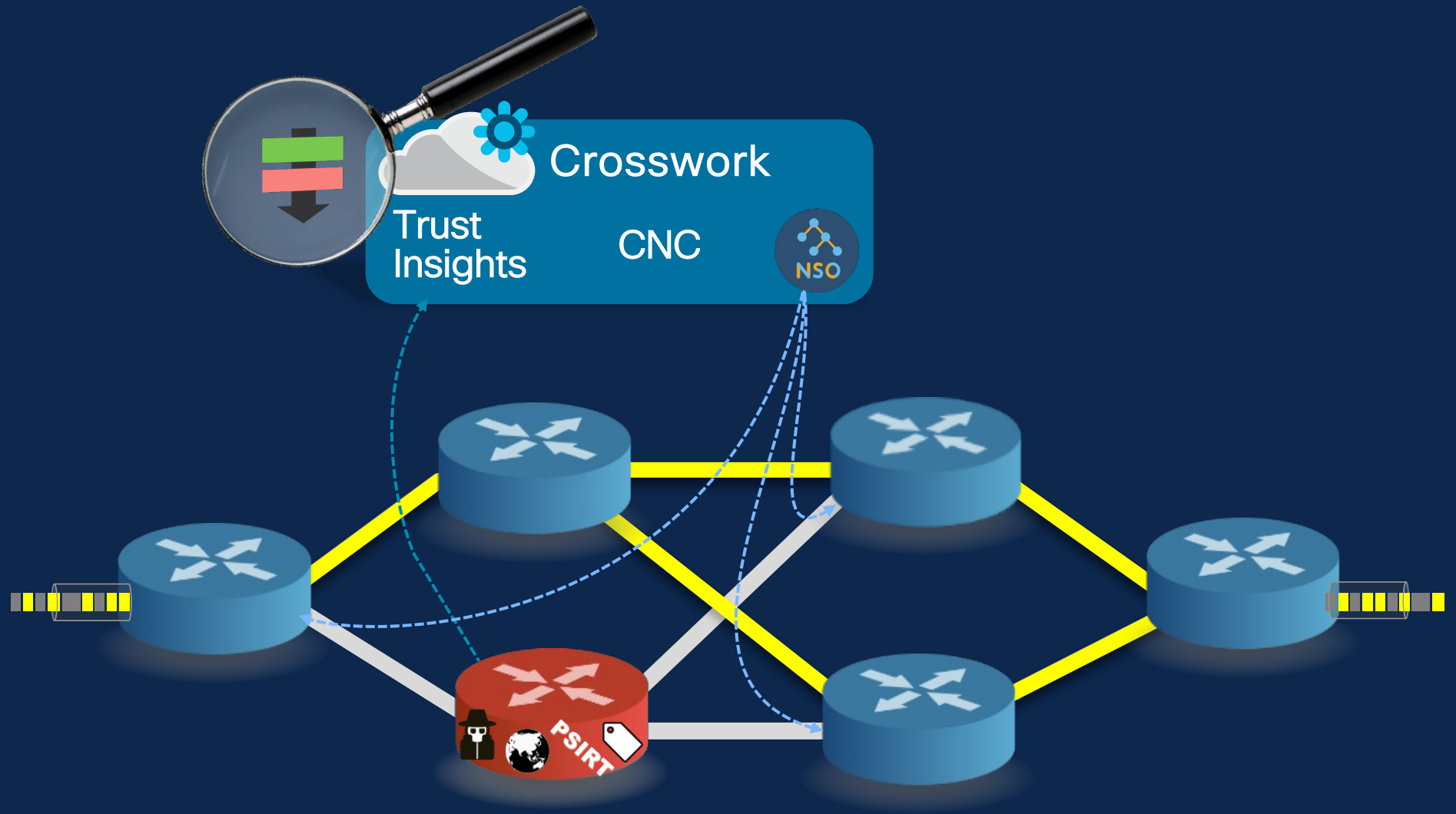
- Actionable assertion resulting from Dossier appraisal
- Dependent on capabilities of the appraised router

Trustworthiness Appraisal

- One to Many Trustworthiness Levels assigned during an appraisal cycle.

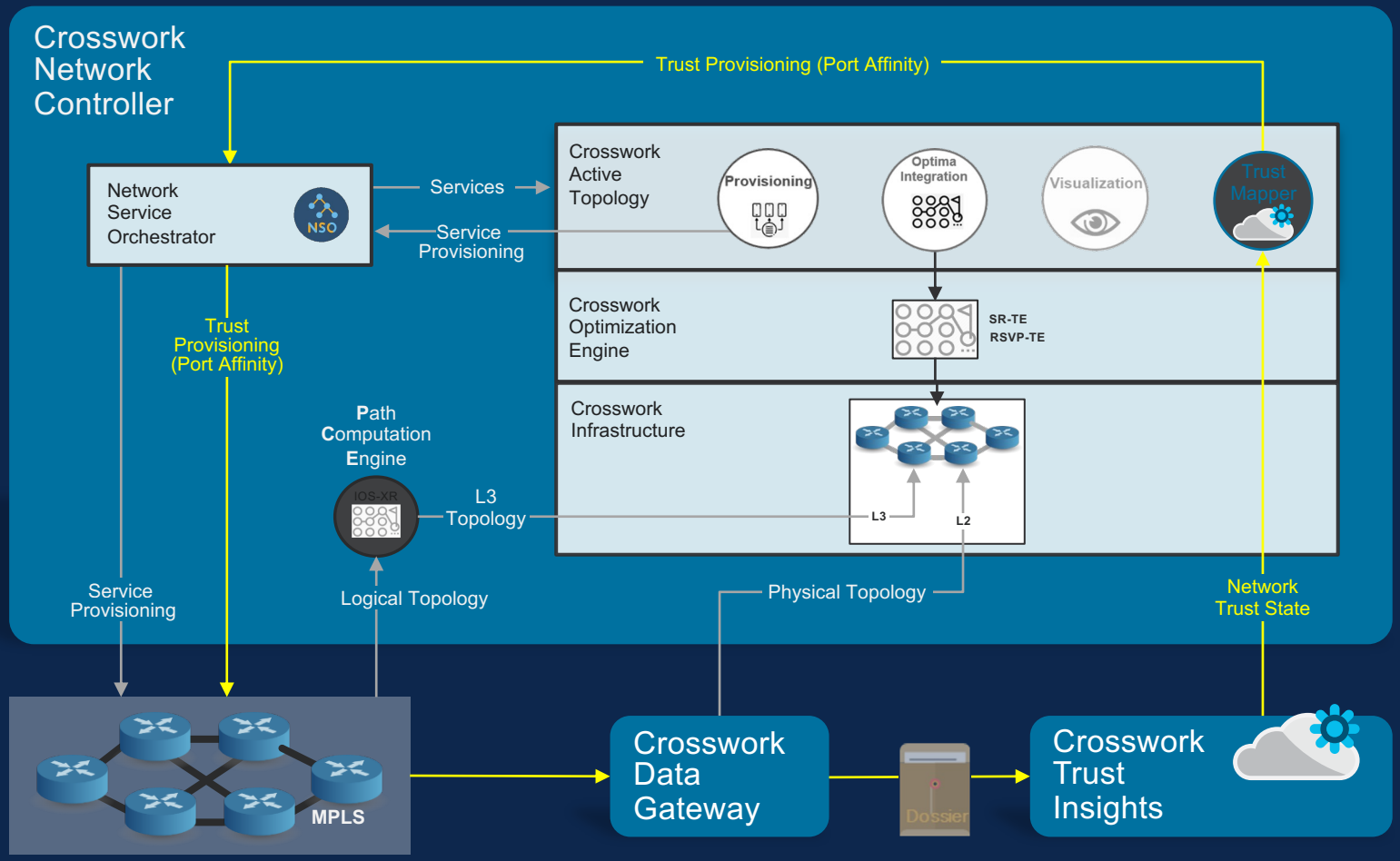


Centralized Trusted Path Routing



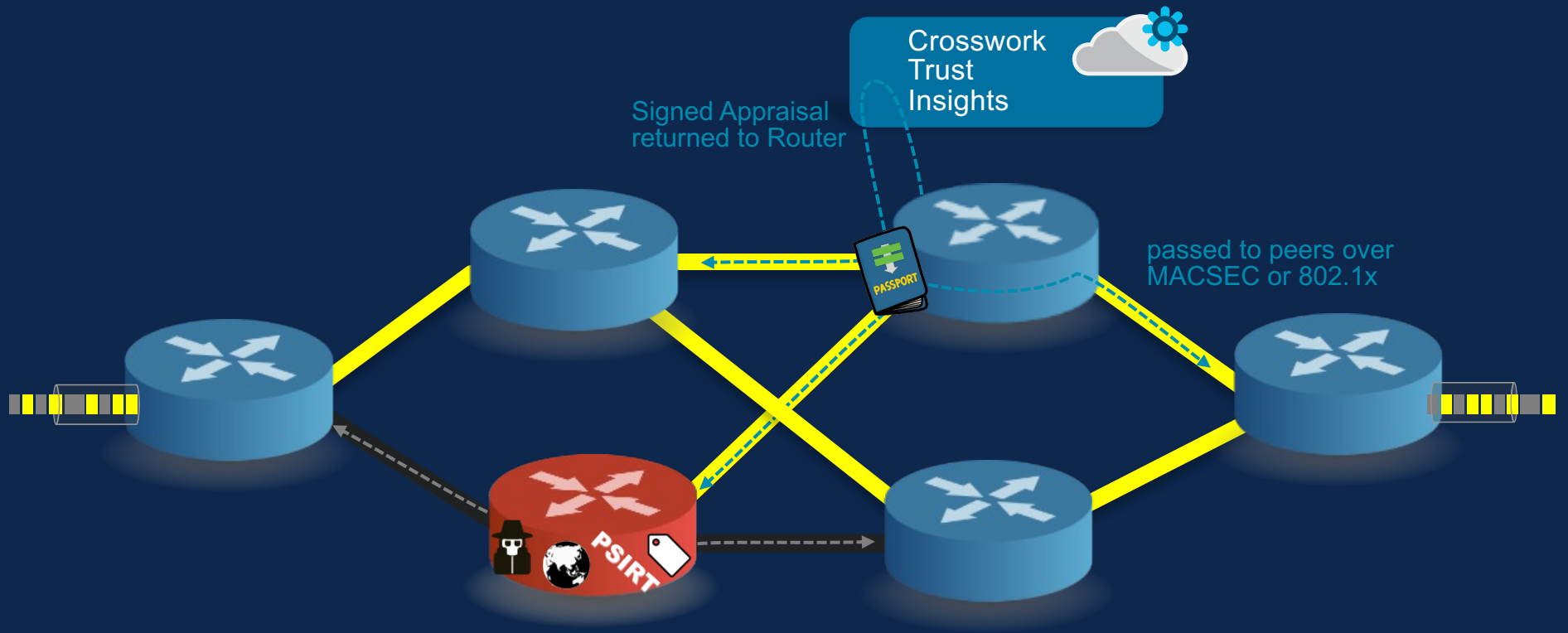
9

Centralized Trusted Path Routing



Distributed Trusted Path Routing

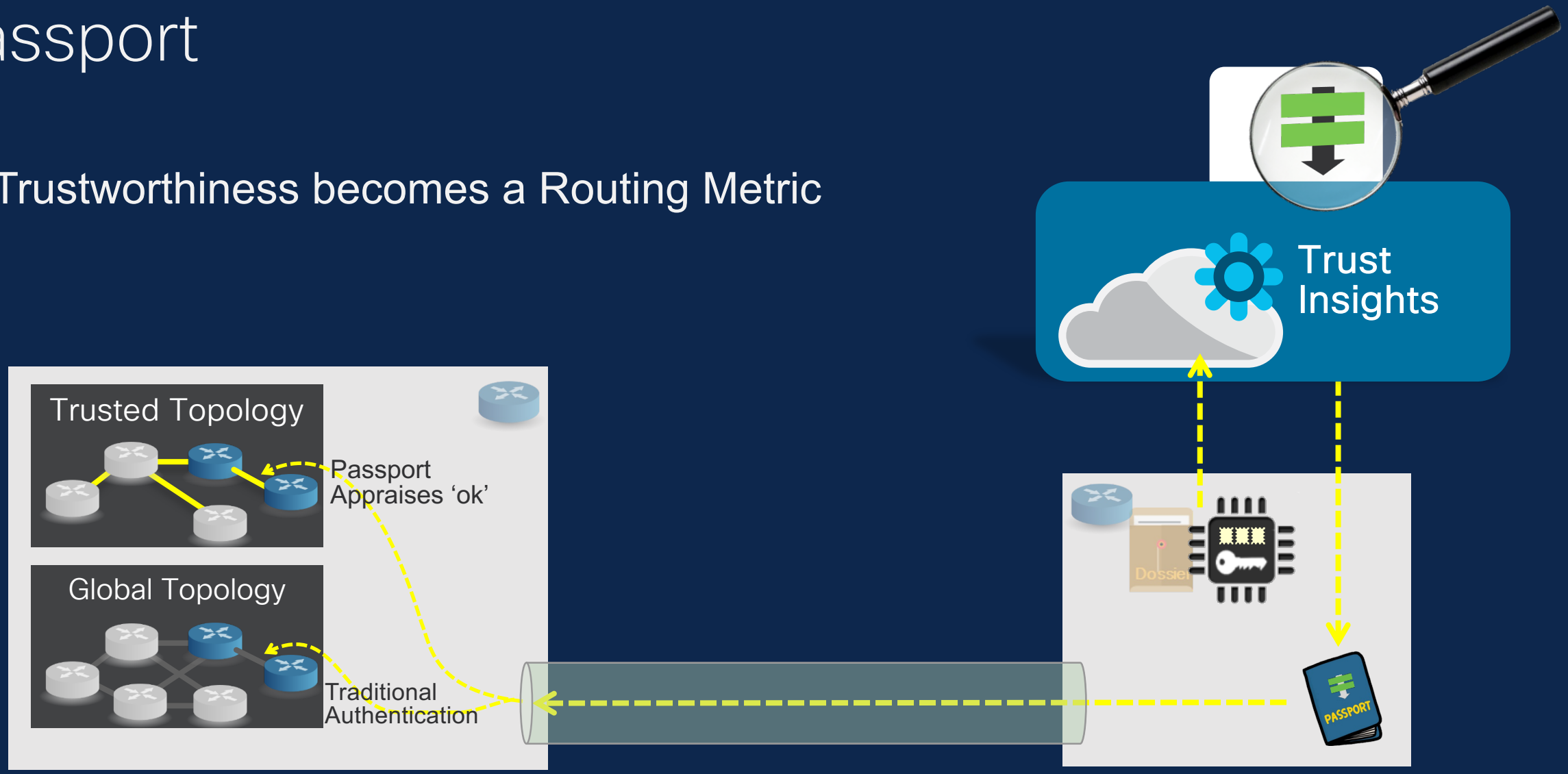
- *Required* at Routing boundaries, even with Centralized TPR deployments
- Peer's trust is established via Link Layer credentials



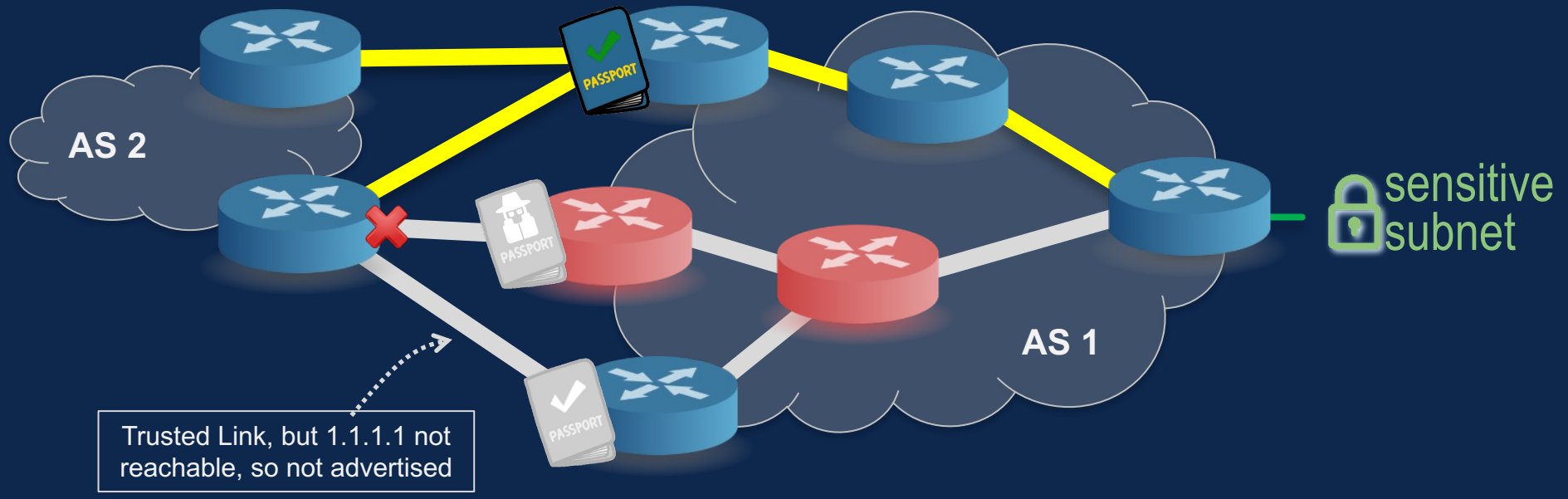
11

Passport

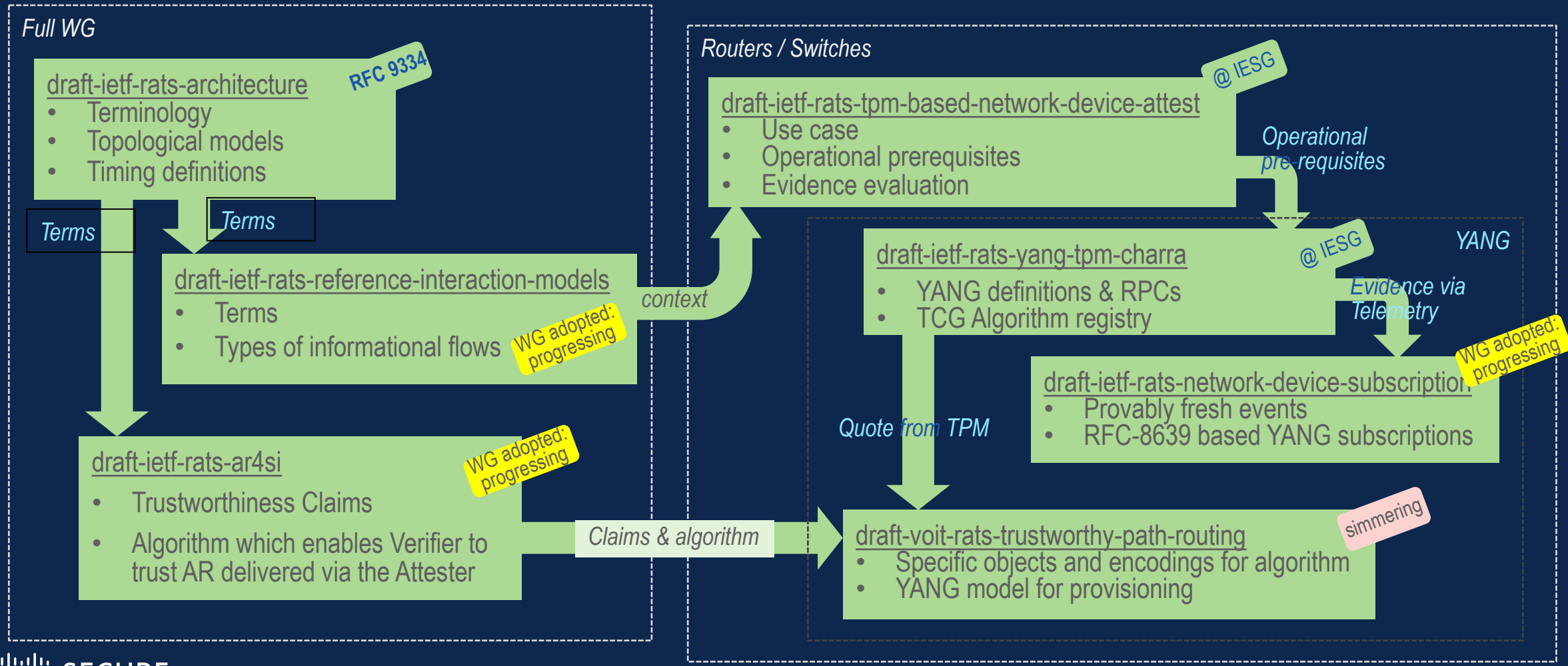
Trustworthiness becomes a Routing Metric



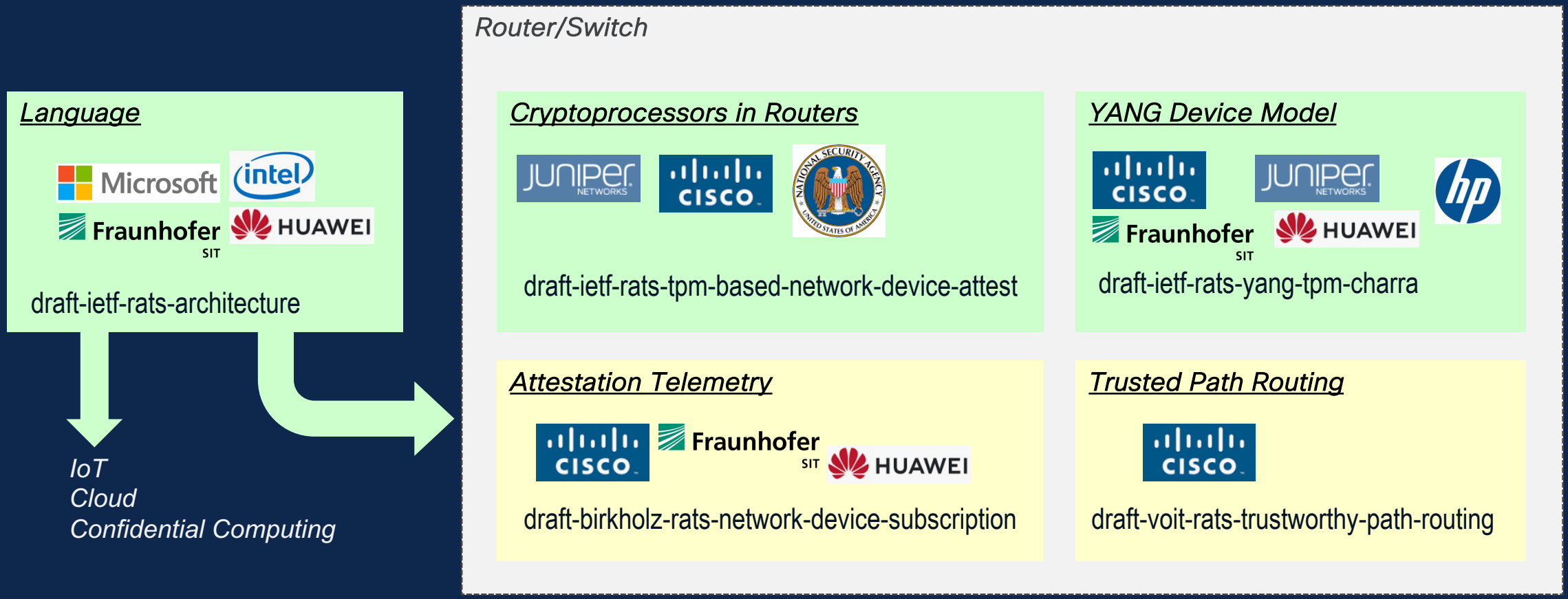
Trusted Path Routing
Inter-AS Advertisement



IETF Standardization: Remote ATtestation and Procedures (RATs)



Vendor Leveraging IETF Standardization



Legend: WG Adopted | Individual

Acknowledgements

This is work that was led by my Cisco Colleagues

Eric Voit

Chennakesava Reddy Gaddam


cisco SECURE