

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?

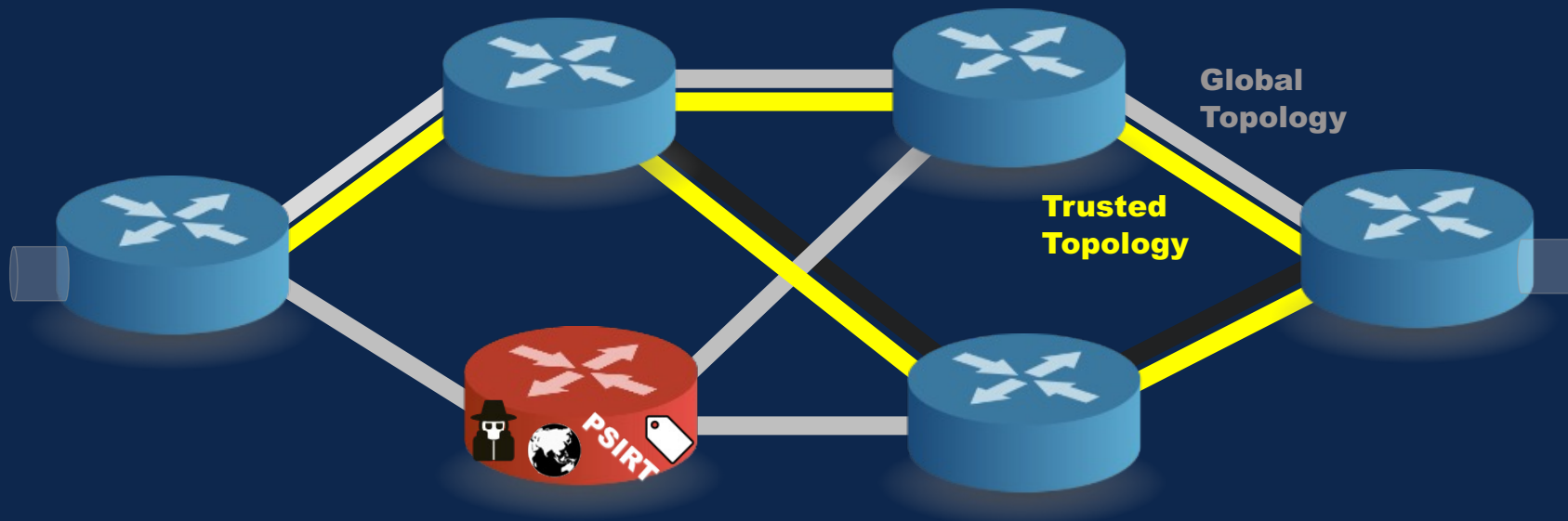
Bypass less Trustworthy Routers

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



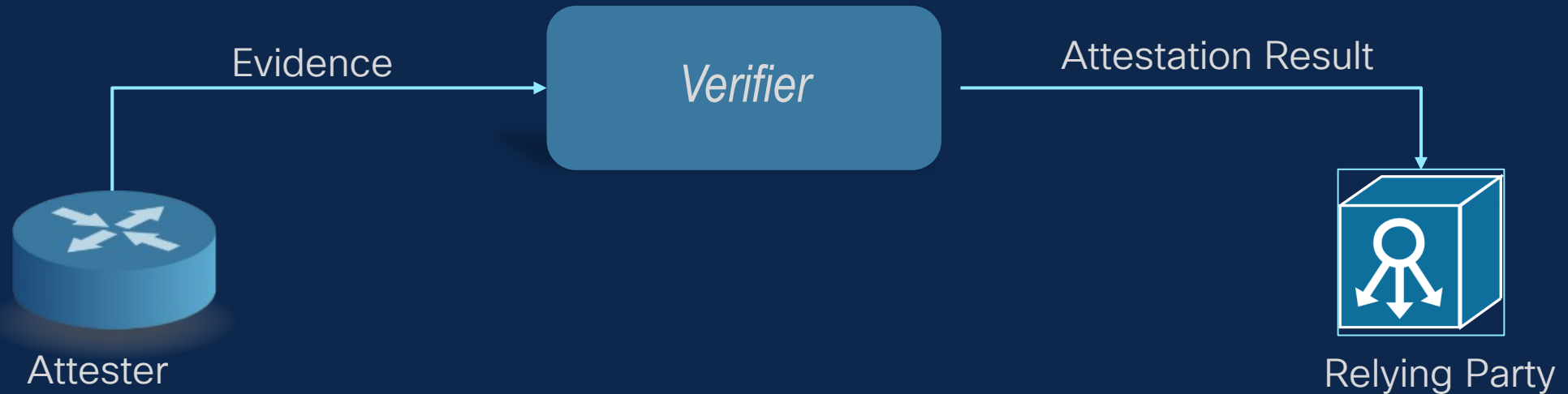
Trusted Path Routing

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



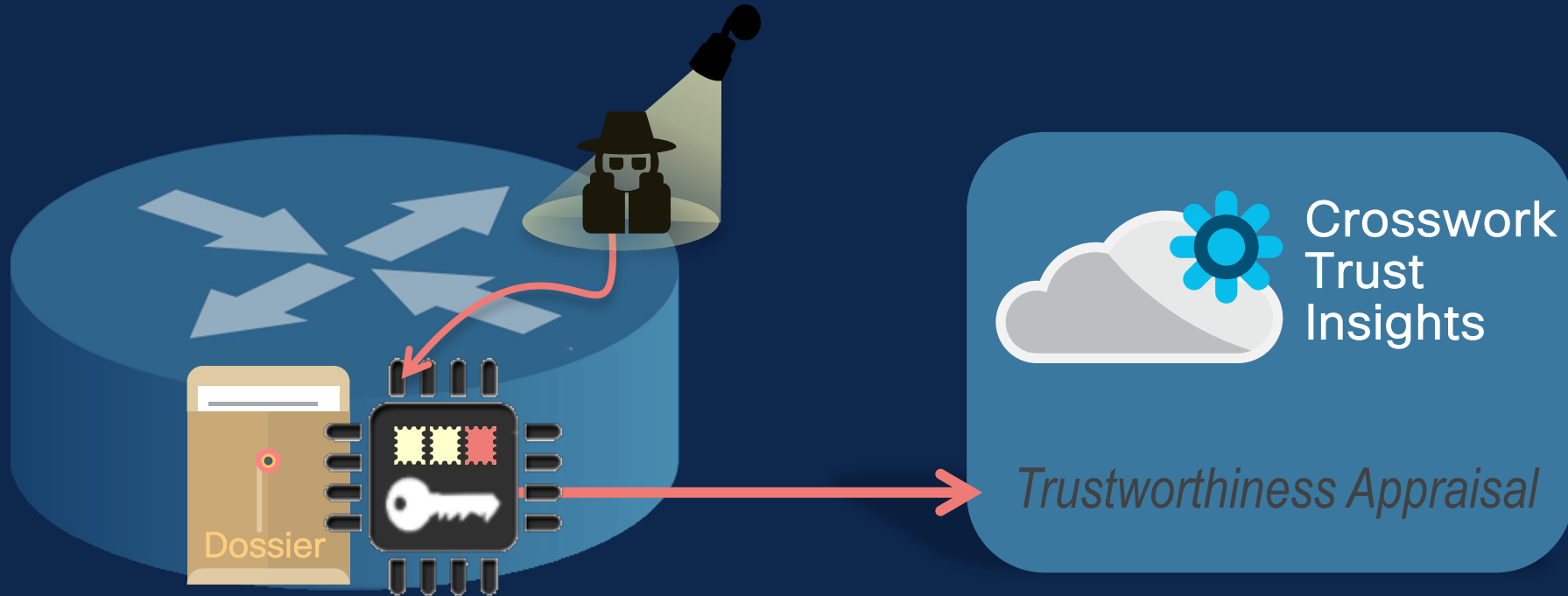
- Critically private flows don't transit less secure devices

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

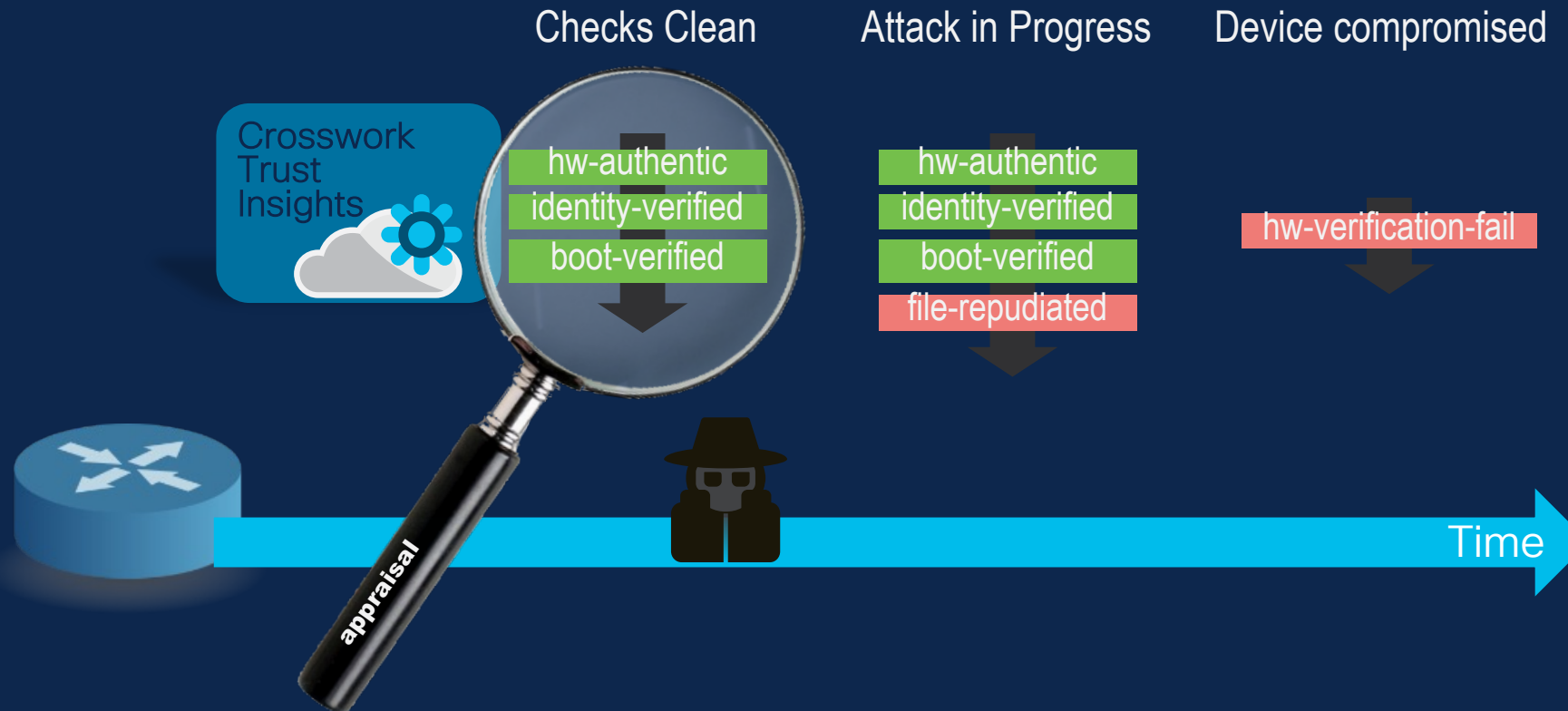
Trustworthiness Level

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

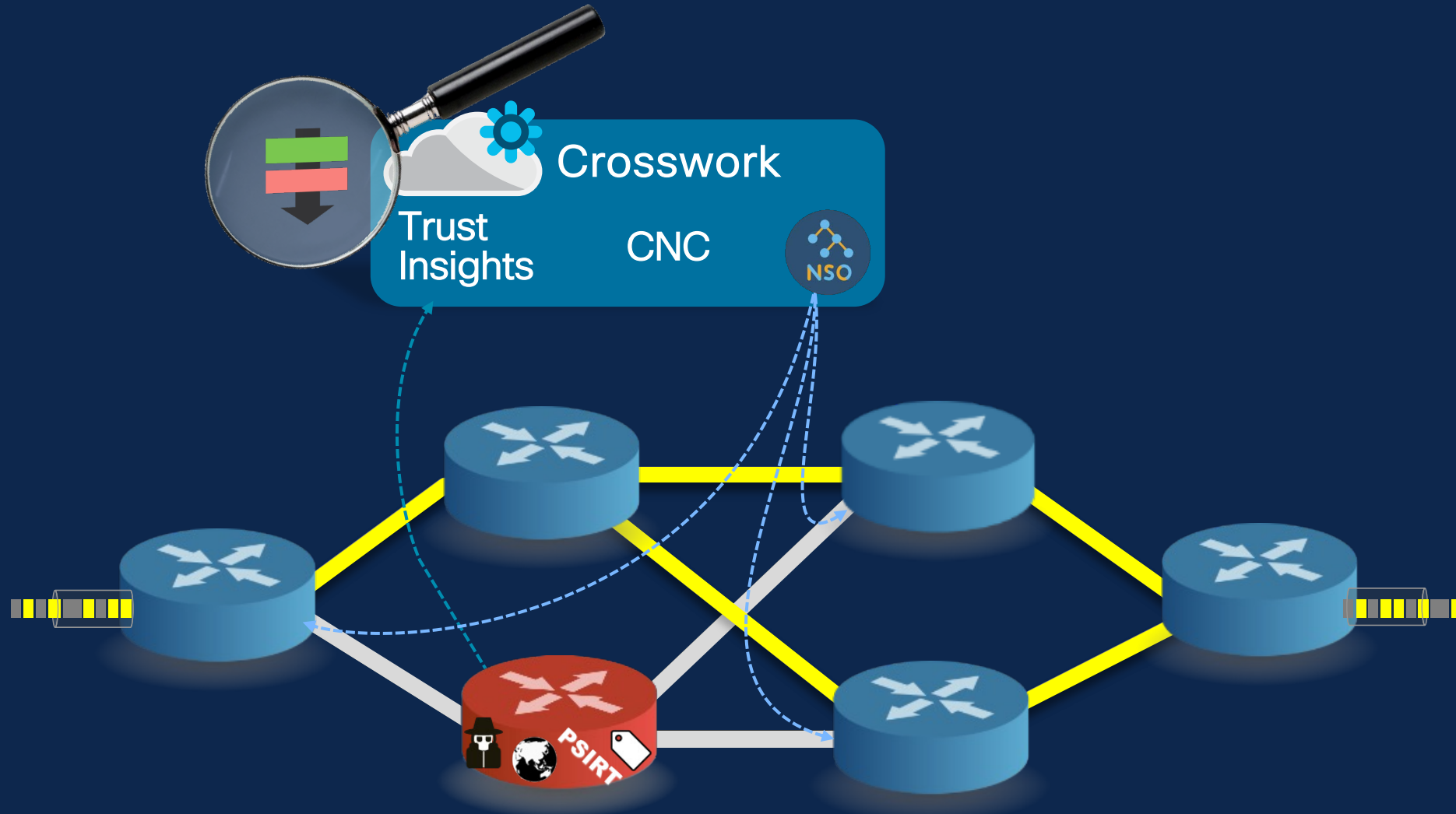
HW Integrity	hw-authentic	Device has authentic hardware
	fw-authentic	Device has authentic firmware
	hw-verification-fail	Device has failed its hardware or firmware verification
Unique Identity (SUDI)	identity-verified	Device has a verified unique identity
	identity-fail	Can't verify a Device's unique identity
Boot Integrity	boot-verified	Device is Boot Integrity Verified
	boot-verification-fail	Device has failed its Boot Integrity verification
Filesystem Integrity	files-verified	All relevant files in file system recognized
	file-repudiated	File(s) exist which should not be present

Trustworthiness Appraisal

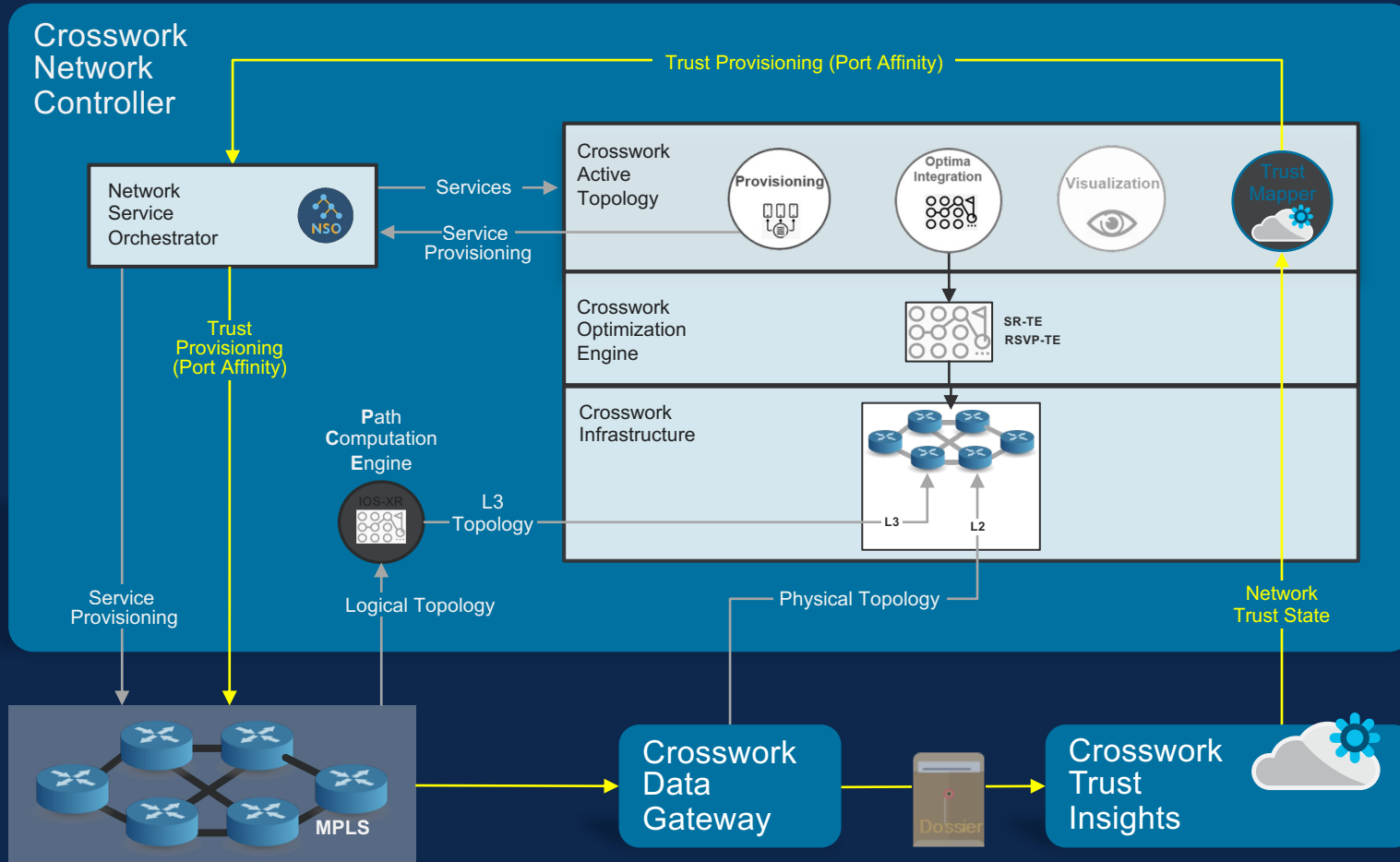
- One to Many Trustworthiness Levels assigned during an appraisal cycle.



Centralized Trusted Path Routing

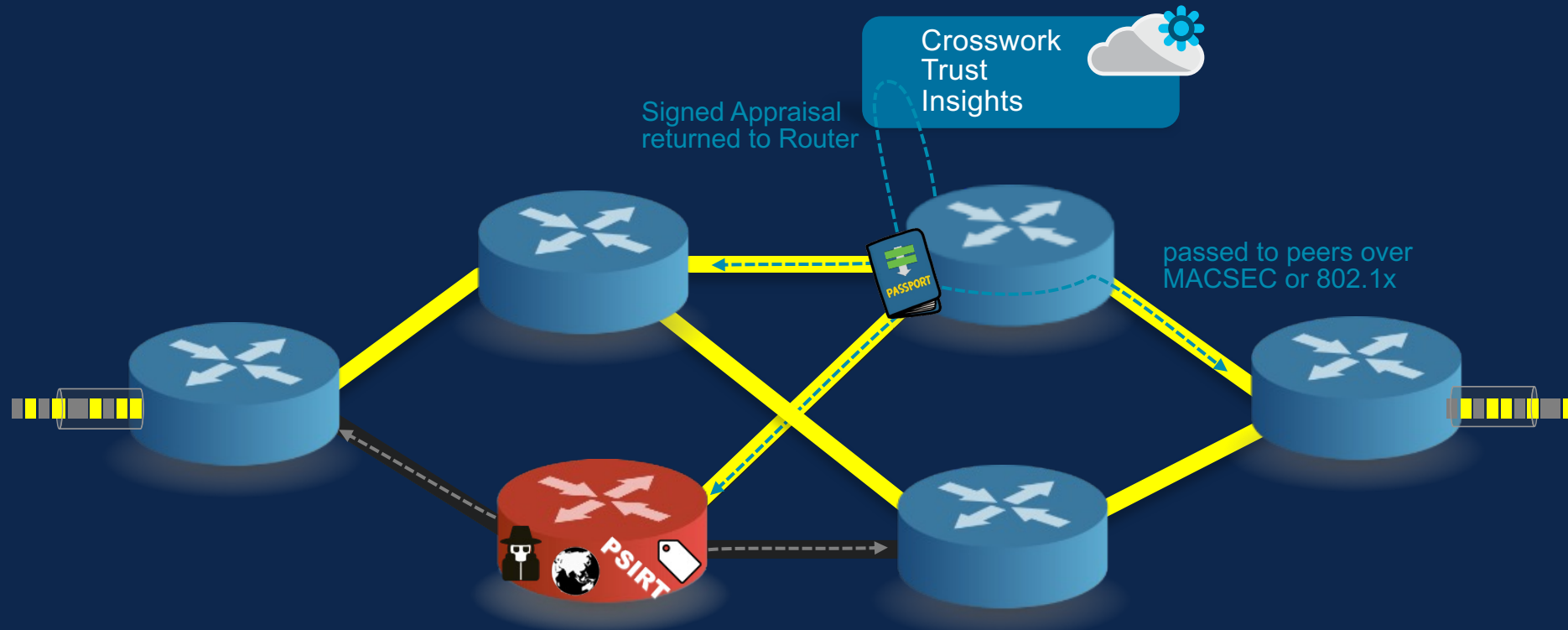


Centralized Trusted Path Routing



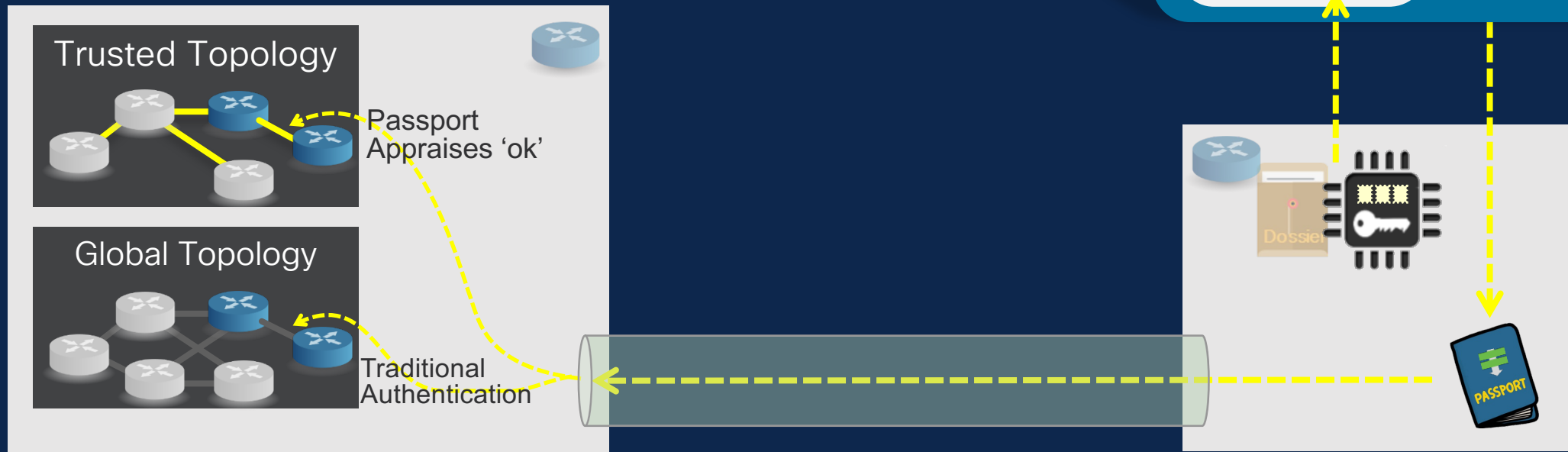
Distributed Trusted Path Routing

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

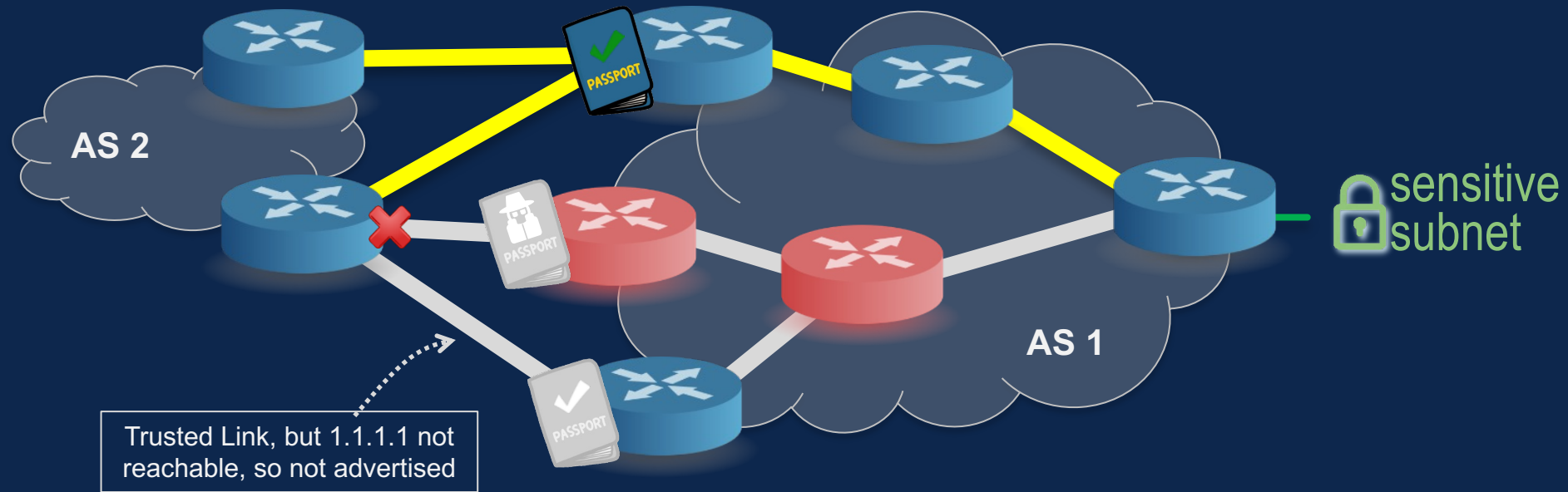


Passport

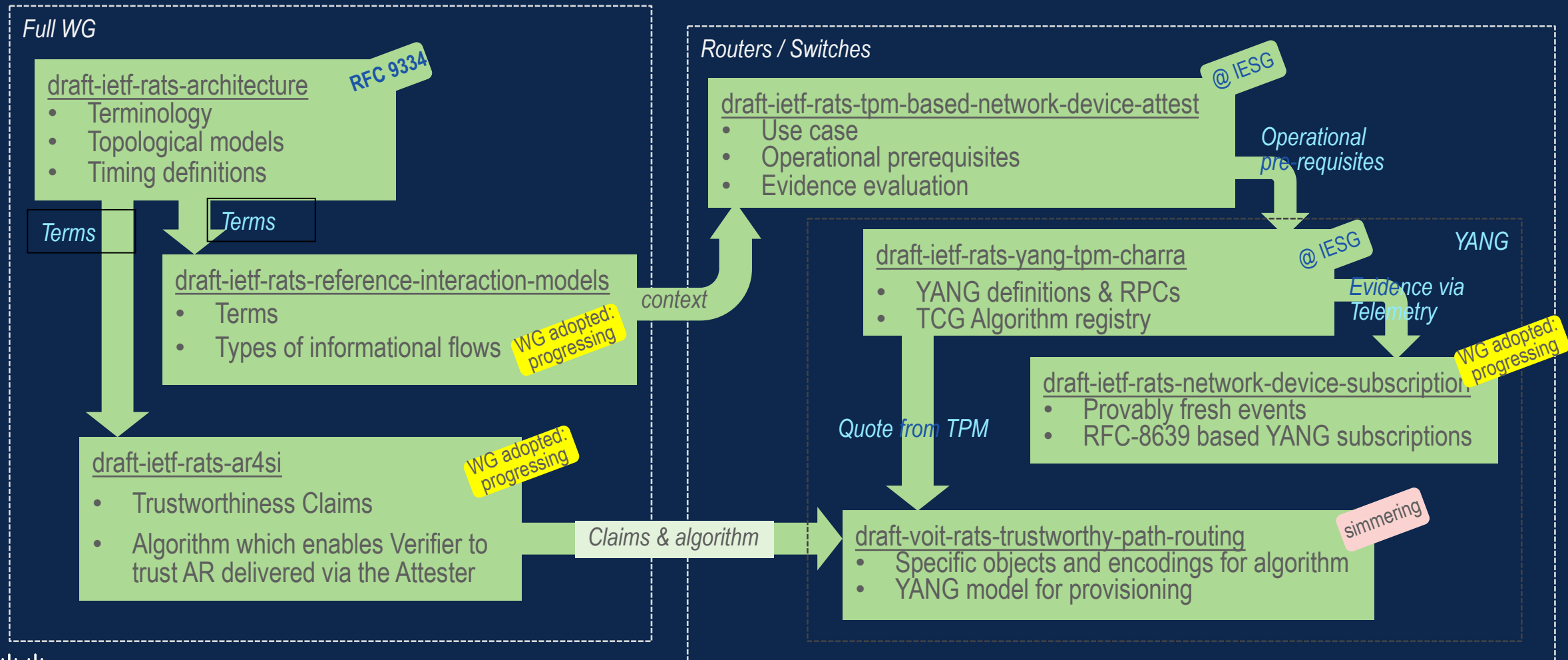
Trustworthiness becomes a Routing Metric



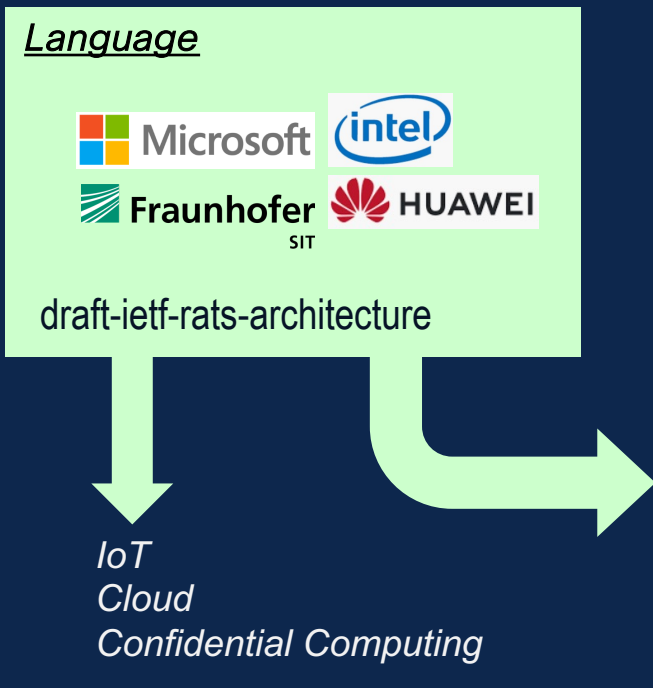
Trusted Path Routing Inter-AS Advertisement



IETF Standardization: Remote Attestation and Procedures (RATs)



Vendor Leveraging IETF Standardization



Router/Switch

Cryptoprocessors in Routers



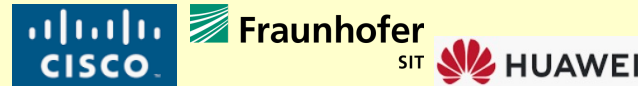
draft-ietf-rats-tpm-based-network-device-attest

YANG Device Model



draft-ietf-rats-yang-tpm-charra

Attestation Telemetry



draft-birkholz-rats-network-device-subscription

Trusted Path Routing



draft-voit-rats-trustworthy-path-routing

Legend:

WG Adopted

Individual

Acknowledgements

This is work that was led by my Cisco Colleagues

Eric Voit

Chennakesava Reddy Gaddam



CISCO **SECURE**