CISCO
The bridge to possible

Certificate Authority Browser Forum

Cisco Root Store Update

Eric Hampshire & Chad Dandar
Cisco Cryptographic Services
Security & Trust Organization
Oct 8, 2024

Update - Agenda

- TRS Today

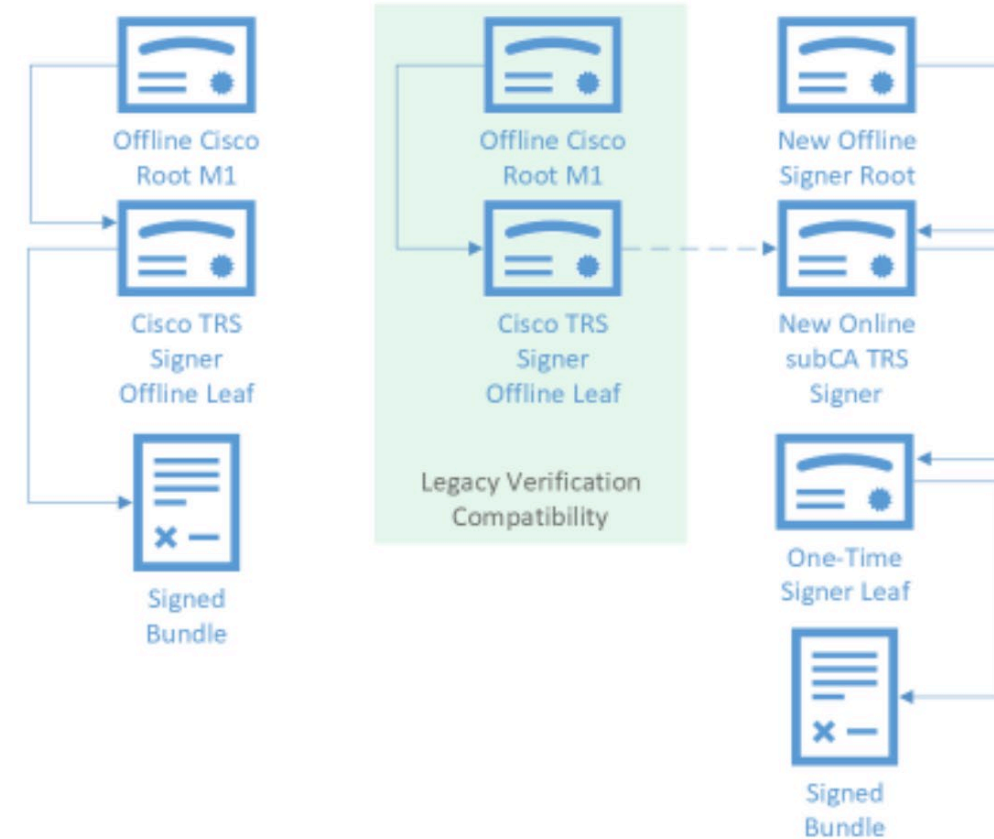- TRS Future (In Progress)

- TRS Statistics

TRS (Today)

- 5 bundles – Cisco Roots are in all bundle types
    - Intersect (125)– Must be in MS, Mozilla, Apple, and Google trust stores
    - Union – (236) Must be in any one of MS, Mozilla, Apple, and Google trust stores
    - Core – (34) Limited Root CAs, only used for authenticating TLS traffic to Cisco products + services
    - FedRAMP (97) - Used for US federal operations, this bundle consists of the Core bundle, the USA CAs from the Intersect bundle, and root CAs from the US DoD External PKI Trust Chains
    - Webex (6) - Set of root certificate authorities that are trusted to issue public TLS certificates to names used by CTG/Webex

TRS (Future – In Progress)

- Same five + A La Carte (product teams can create their own bundles)

- Revocation of TRS bundles: Each bundle release will be tied to an individual certificate.

- Automatic updates (yay automation!)

- Bundle history

- Bundle manifest + diffs

Trusted Root Store Signing Chain Update Proposal rev 2

Offline Cisco Root M1

Cisco TRS Signer Offline Leaf

Signed Bundle

Offline Cisco Root M1

Cisco TRS Signer Offline Leaf

Legacy Verification Compatibility

New Offline Signer Root

New Online subCA TRS Signer

One-Time Signer Leaf

Signed Bundle

Current TRS Signing Chain

Proposed TRS Signing Chain

TRS Signing Chain Risks:

	Current TRS	Proposed TRS
Long Lived Root	✗	✓
OCSP Available	✗	✓
Untrapped Signer Key	✗	✓
Good Root Signing Algo	✗	✓
Adequate PQ Key Size	✗	✓
Revoke Individual Bundles	✗	✓

TRS: Top Products

Cisco's Product Portfolio for TRS

20%

80%

- Yes
- No

Top Products having TRS

47%

53%

- Yes
- No

Cisco Confidential
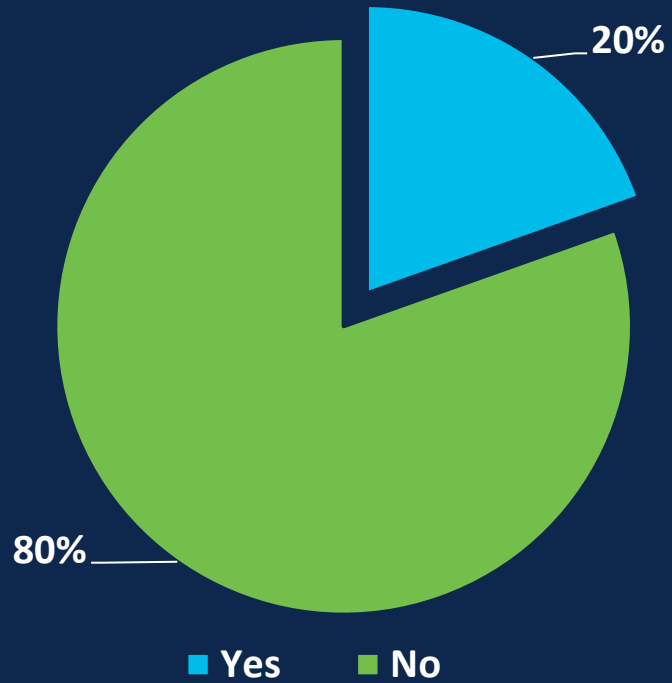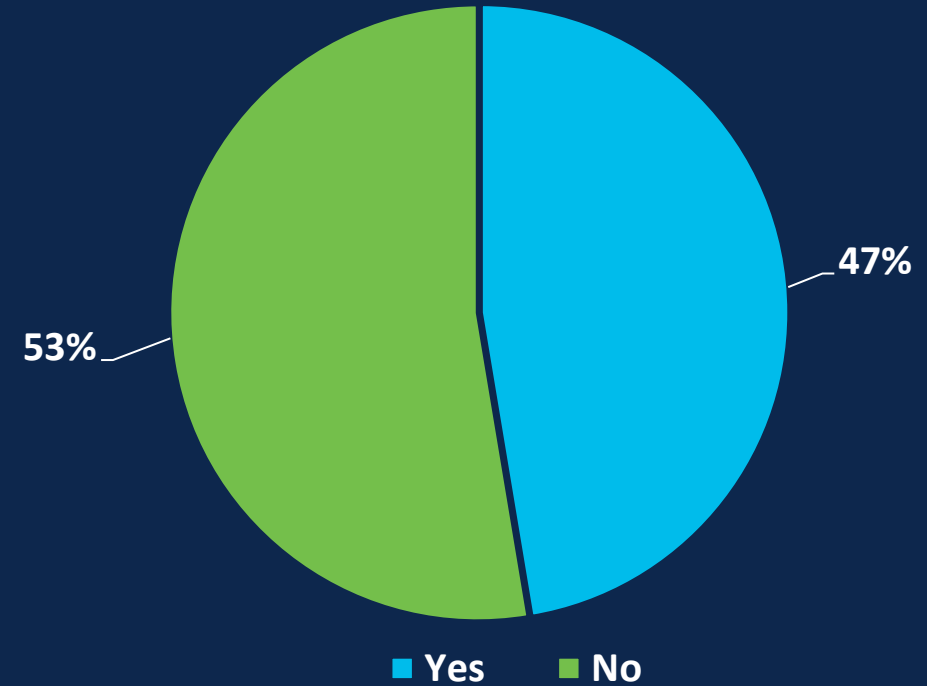
Download Trends – Trusted Root Store

Bundle Type		Q2 FY24	Q3 FY24	Q4 FY24	Q1 FY25
Core	External	18,173,484	30,856,335	21,309	67,449
	Internal	406	632	2	3
Intersect	External	326,097,496	102,445	60,458	159,089
	Internal	218,172	373,456	14	87
Union	External	41	192	109	112
	Internal	6	-	-	-
FedRamp	External	-	38	35	35
	Internal	-	-	-	-
Webex		-	1	-	-
	Total downloads	**344,489,605**	**31,333,099**	**81,927**	**226,775**

*Note: Cisco's FY runs Aug-Jul

CISCO

The bridge to possible