The Case for Binding and Embedding

Streamlining security certifications across a multi-module platform



Trish Wolff
Security Research Engineering Technical Leader

September 17, 2026

The 60-second version

The opportunity

Binding and embedding allows for flexibility in cryptographic module validation.

One validated crypto core can now serve an entire product line instead of being re-validated inside every product.

The catch

Continuous monitoring is essential to ensure all modules in the chain stay active.

If the reused module goes Historical – all other uses of that module go Historical, and you start the process over again.

The answer

Treat revalidation of the reused module as a planned, funded, recurring activity.

Cryptographic security is a program, not a project.

© 2026 Cisco and/or its affiliates. All rights reserved.

Agenda

01 The why

02 The standards

03 The business case

04 The “shift left” proposition

05 The challenges

06 The certification roadmap

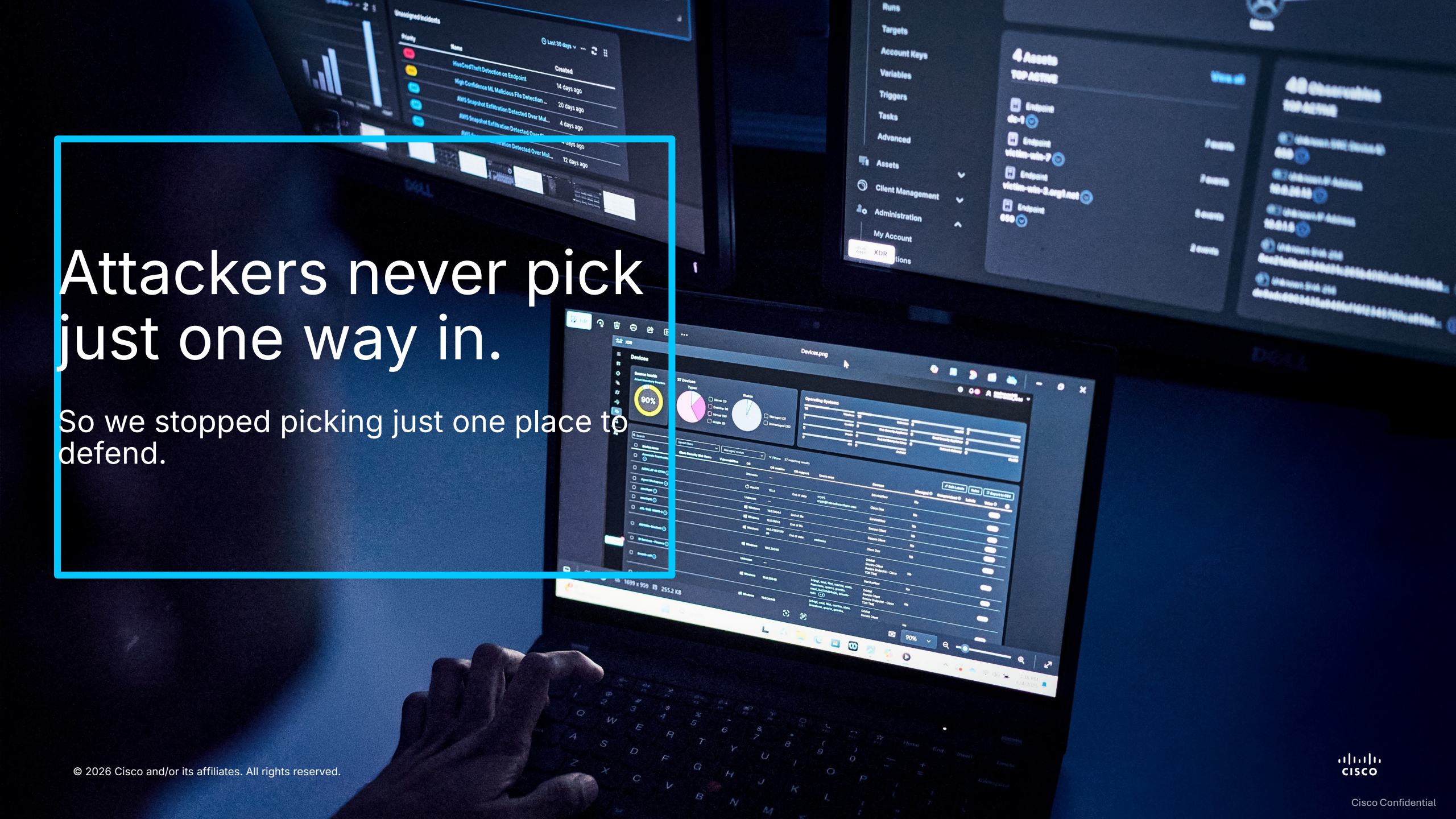
07 The sustaining loop

08 The take aways

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

The why

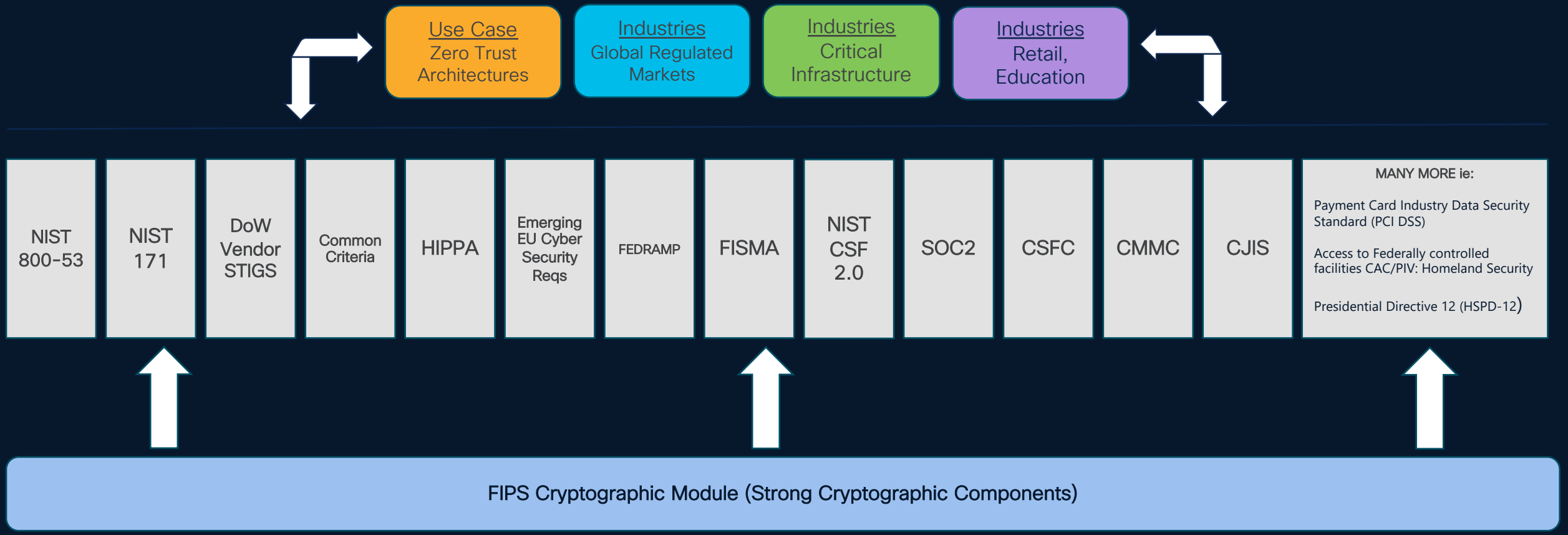


© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

FIPS – Bedrock of Certifications

Strong crypto is at the core



© 2026 Cisco and/or its affiliates. All rights reserved.

Time matters

- Align with evolving regulatory frameworks
- Accelerate time-to-market for advanced technology
- Close the “vulnerability gap”
- Drive strategic market differentiation

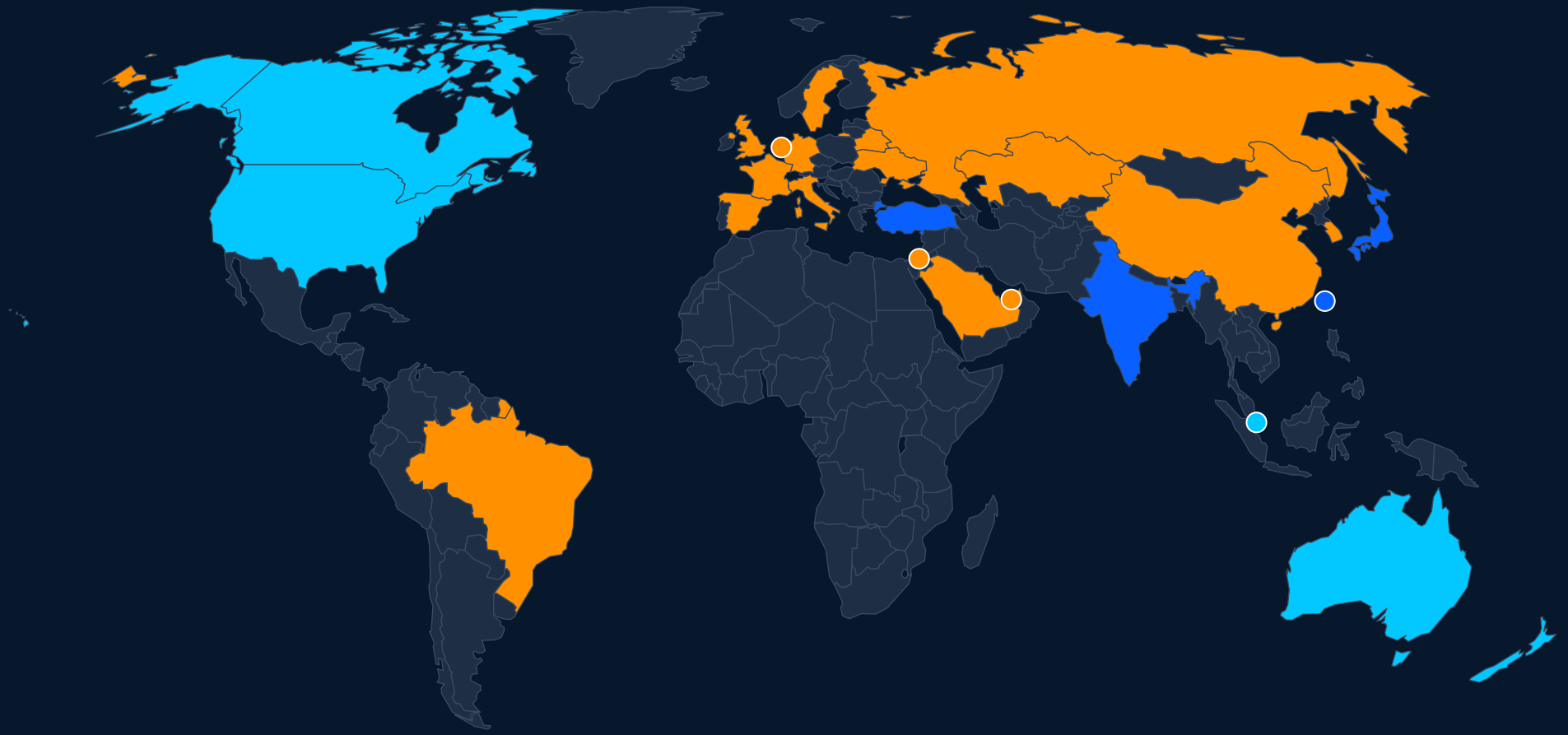


© 2026 Cisco and/or its affiliates. All rights reserved.

The standards

Standardizing what defines "strong cryptography"

26 countries with a mandated or de facto crypto validation regime, colored by the standard it is built on



FIPS 140-3 / CMVP accepted (5)

ISO/IEC 19790-based scheme (4)

Own national crypto standard (17)

No published requirement / not assessed

Categories reflect the primary basis of each regime. Several 'own standard' schemes (China GM/T 0028, Korea KCMVP) are structurally derived from ISO/IEC 19790 / FIPS 140 but mandate national algorithms. Dots mark countries too small to render at this scale (Singapore, UAE, Israel, Netherlands, Taiwan). Indicative assessment - verify against current national requirements before external use.

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

The standards stack

FIPS 140-3	The US/Canadian federal requirement. Does not restate the requirements — it points to ISO.
ISO/IEC 19790:2012	The actual security requirements. Cryptographic boundary, module types, SSP management, zeroisation, self-tests.
ISO/IEC 24759:2017	The test requirements. Source of the AS / VE / TE assertion numbers your lab works to.
SP 800-140A – 140F	NIST modifications to the ISO annexes. SP 800-140B governs the Security Policy format.
FIPS 140-3 Implementation Guidance	Where IG 1.A lives. Binding, embedding, entropy caveats, SSP classification, CVE management.
CMVP Management Manual v2.7	Programme mechanics: submission scenarios, sunset dates, Historical and Revoked lists, queue handling.

© 2026 Cisco and/or its affiliates. All rights reserved.

The alphabet soup

EVM – **E**xisting **V**alidated **M**odule

IUT – **I**mplementation **U**nder **T**est

OEUPT – **O**perational **E**nvironment Update

ESV – **E**ntropy **S**ource **V**alidation

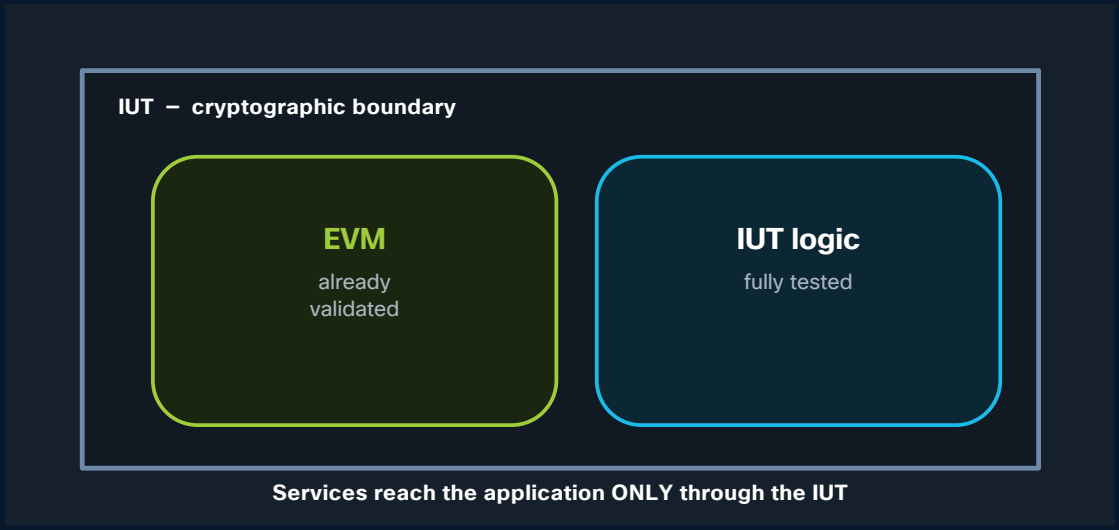
ESVUP – **E**ntropy **S**ource **V**alidation Update



© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Embedded



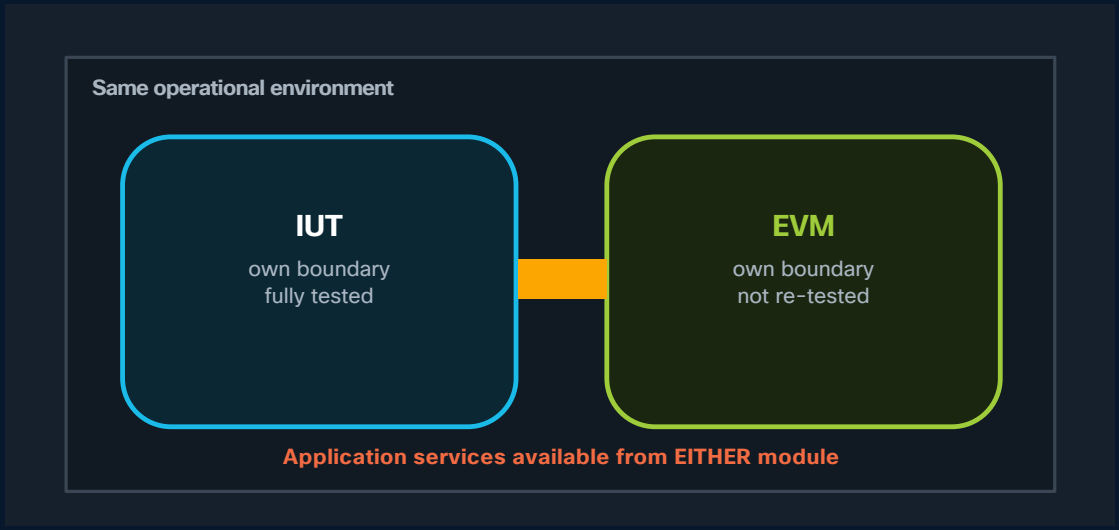
> *"An embedded cryptographic module is a module that is wholly contained within the module boundary of an IUT and whose services are provided solely to the IUT."*
>
> **– IG 1.A, Resolution 2**

- **EVM security level may be LOWER than the IUT**
  - Provided the lab shows the EVM already meets the higher requirement, or the IUT meets it on the EVM's behalf (IG 1.A 4.b)
- **SSPs crossing into the EVM are not "entry/output"**
  - IG 9.5.A Table 1 classifies this as N/A – the SSP never leaves the cryptographic boundary
- **Zeroisation relief applies below Level 4**
  - ISO/IEC 19790:2012 §7.9.7 – covered in Part 4

> **USE EMBEDDED WHEN**
>
> You own or fully control the EVM, and you want a single external interface and one certificate story for the customer.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bound



> *"A binding cryptographic module is a module with a separate, disjoint cryptographic boundary (IUT) that depends on an EVM. Application services are available from either cryptographic module."*
>
> **– IG 1.A, Resolution 3**

- **EVM must be the SAME or HIGHER security level**
  - All sections except Mitigation of Other Attacks (IG 1.A 4.b). The reverse of the embedded rule.
- **Tested OEs must match, or one inside the other**
  - IG 1.A 3.a – this is what couples your OE roadmap to the EVM vendor's
- **SSPs between IUT and EVM ARE entry/output**
  - ISO 19790 §7.9.4 and §7.9.5 apply. Classified MD/EE in IG 9.5.A.

USE BOUND WHEN

The EVM is a shared platform service other products also call directly, or it is a third-party module you do not control.

© 2026 Cisco and/or its affiliates. All rights reserved.

The business case

The business case

What reuse removes

No re-testing of the EVM (IG 1.A 4.a)

The EVM is already tested. Removes the source code review and operational testing for all future use.

One crypto core serves multiple customer use cases

Validate the core once; every downstream product references it rather than rebuilding it.

What you still pay for

Full validation of the IUT (IG 1.A 4.a)

You do not inherit the EVM's certificate. Your module is tested front to back.

OE Updates to EVMs (IG 1.A Additional Comments)

OE of the IUT must also be listed on the EVM. However, putting the OE on the EVM may be enough to meet customer needs

Dependency management, forever

The EVM's sunset, OEs and CVEs are now your problem too. This is the real ongoing cost.

Where the saving concentrates

Entropy

ESV certificates never expire (MM §4.8). Validate once, cite from many modules.

Review effort

Fewer independent full submissions competing for the same CMVP queue.

© 2026 Cisco and/or its affiliates. All rights reserved.

The money matters

A full submission is roughly 3× an UPDT and 6× an OEUP

Lab fees vary greatly between a full submission and OEUP and UPDT scenarios

Scenario	What it covers	NIST CR fee	New sunset?
FS – Full Submission (Level 1)	A brand new validation	$16,000	Yes – 5 yr
FS – Full Submission (Level 2)	A brand new validation	$17,000	Yes – 5 yr
FS – Full Submission (Level 3)	A brand new validation	$17,500	Yes – 5 yr
UPDT – Update	<30% security change, or reset the clock	$5,500	Yes – 5 yr
OEUP – Operational Env. Update	Add / modify / delete tested OEs	$2,500	No
CVE	Security-relevant CVE or bug fix	$2,500	No
ALG / TRNS / PHYS / NSRL / RBND	Algorithm, transition, physical, rebrand	$2,500	No
VUP / VAOE	Vendor information; vendor-affirmed OE	$0	No
ESV – Entropy Source Validation	Entropy source (never expires)	$5,500	n/a
ESVUP – ESV Add OE	Extend an ESV to new OEs	$2,500	n/a

© 2026 Cisco and/or its affiliates. All rights reserved.

The “shift left” proposition

Entropy – ESV is the reusable asset

ESV – the current mechanism

A separate entropy source validation with its own E# certificate.

Required for new submissions that need an entropy assessment.

No more allowances for “unknown entropy sources”

ESV certificates have NO expiration date. (MM §4.8)

What this means for reuse

One noise source → one ESV → many modules.

Every module on the platform can cite the same entropy certificate, provided each reaches the source through its own direct GetEntropy() path.

Adding platforms later is an ESVUP, not a new ESV.

© 2026 Cisco and/or its affiliates. All rights reserved.

Key management

Key generation

- A key is never stronger than the entropy behind it

SSP Entry and Output

If the EVM is embedded in the IUT then the key is travelling inside the cryptographic boundary

If the EVM is bound to the IUT, then all entry/output rules between two cryptographic modules must be applied

Zeroization

- A module shall zeroise all unprotected SSPs and key components within the module
- Except at security level 4, zeroisation of protected PSPs, encrypted CSPs, or CSPs otherwise physically or logically protected within an additional embedded validated module is not required

ISO/IEC 19790: 2012, 7.9.7

© 2026 Cisco and/or its affiliates. All rights reserved.

Self-tests and integrity

MAY be delegated

Software / firmware integrity

Assertion [05.05] permits the integrity technique to be applied “by the cryptographic module itself; or by another validated cryptographic module operating in an approved mode of operation.”

.

MAY NOT be delegated

Your module's own self-testing

A bound IUT cannot rely on the EVM to perform its self-tests. AS10.02 requires no external controls and no externally provided input test vectors — and the EVM is external to your boundary.

Why the distinction exists

Integrity is applied TO the module. Self-testing is performed BY the module.
The standard permits the former across a boundary

© 2026 Cisco and/or its affiliates. All rights reserved.

The challenges

The coupled lifecycle

Doing nothing – the default outcome



Year 0
EVM validated

Year 2
Your IUT validated against it

Year 5
EVM sunsets

Year 5 + 1 day
YOUR certificate goes Historical

The EVM sunset date sets the date for the whole chain.

The answer: a synchronised revalidation programme

Schedule an UPDT on the EVM in year 4, then the dependents. UPDT is one of only three scenarios that resets the 5-year clock – and it works on Active or Historical modules.

© 2026 Cisco and/or its affiliates. All rights reserved.

Level and environment congruence

Security level asymmetry (IG 1.A 4.b)

BOUND – EVM must be the same or higher level for all sections except Mitigation of Other Attacks.

Consequence: a Level 1 EVM can never be bound to a Level 2 IUT. Check this before you select an EVM.

Operational environment congruence (IG 1.A 3.a)

For software, firmware and hybrid bound modules, the IUT's tested OEs must be the same as the EVM's, or a subset of them.

Consequence: you cannot add a platform to your own certificate until the EVM supports it first.

How to manage both

- Select the EVM against your **CEILING**, not your current product. Target the highest security level and the widest OE list you expect to need.

- **Plan for OE Updates.** Consider VAOE as an alternative to OEUP. At OE Level 1, vendor affirmation costs $0 in NIST fees – but carries no CMVP or CAVP assurance.

© 2026 Cisco and/or its affiliates. All rights reserved.

The rest of the risk register

Operational tests cannot be delegated
AS10.02 / IG 1.A 3.b

Build a delegation register: for every requirement met via the EVM, record which other assertions it touches.

Only currently-approved EVM services may be claimed
IG 1.A 4.e

An EVM can be Active while containing a transitioned algorithm. Re-check the EVM's algorithm list at submission, not at design.

Documentation burden is under-scoped
IG 1.A §5

Assign an owner for Security Policy architecture from day one. [EVM] separation must be coherent end to end.

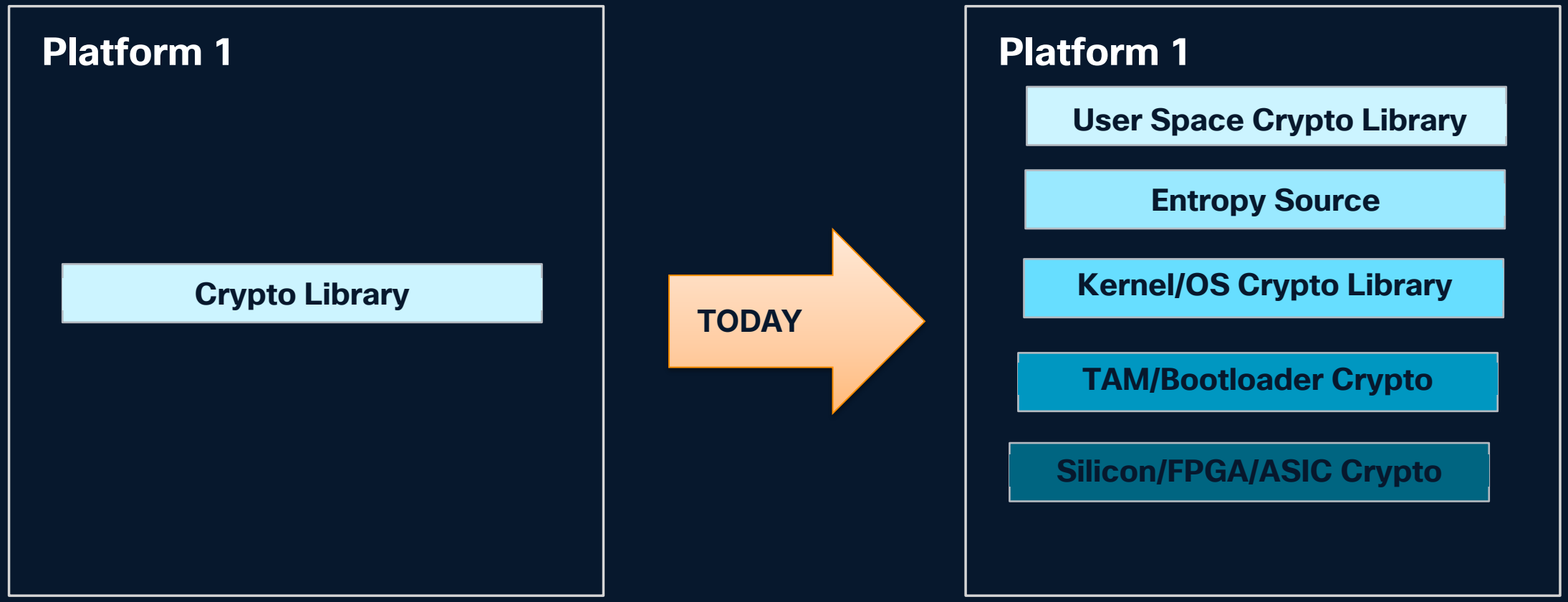
No contractual leverage inside the CMVP process
MM §7.1.8

If you do not own the EVM, your only instrument is the OEM agreement. Negotiate OE, CVE and revalidation commitments up front.

© 2026 Cisco and/or its affiliates. All rights reserved.

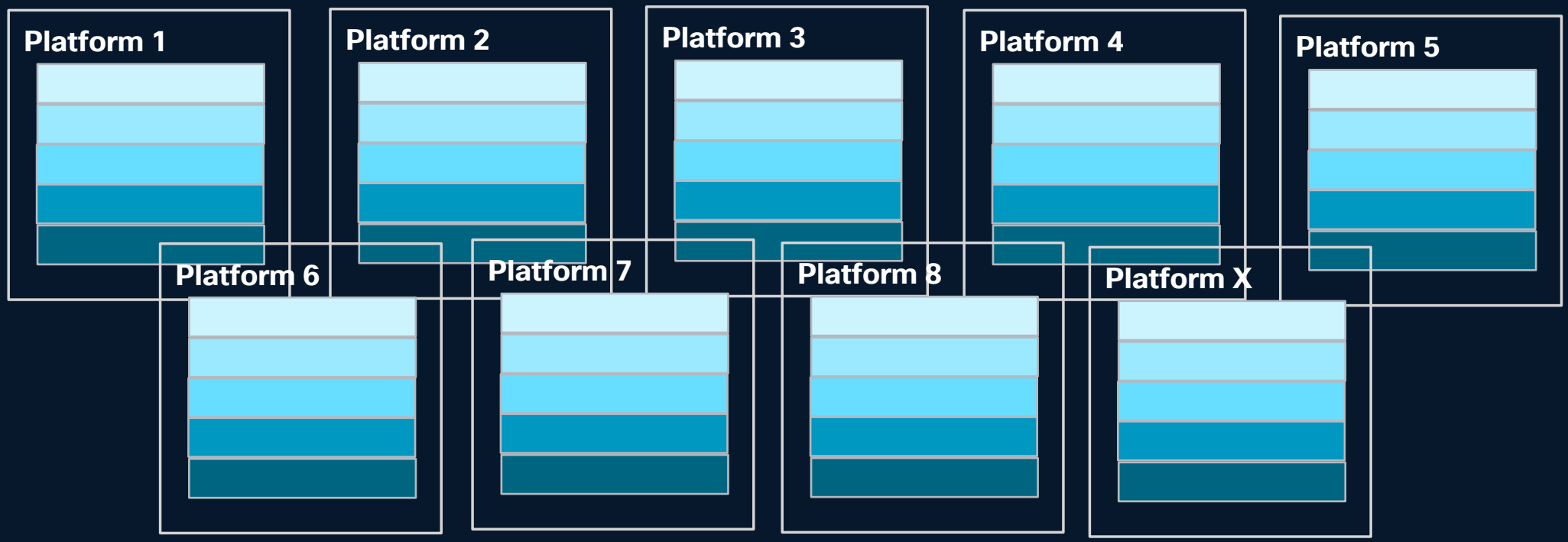
The certification roadmap

Crypto is not in one place anymore



© 2026 Cisco and/or its affiliates. All rights reserved.

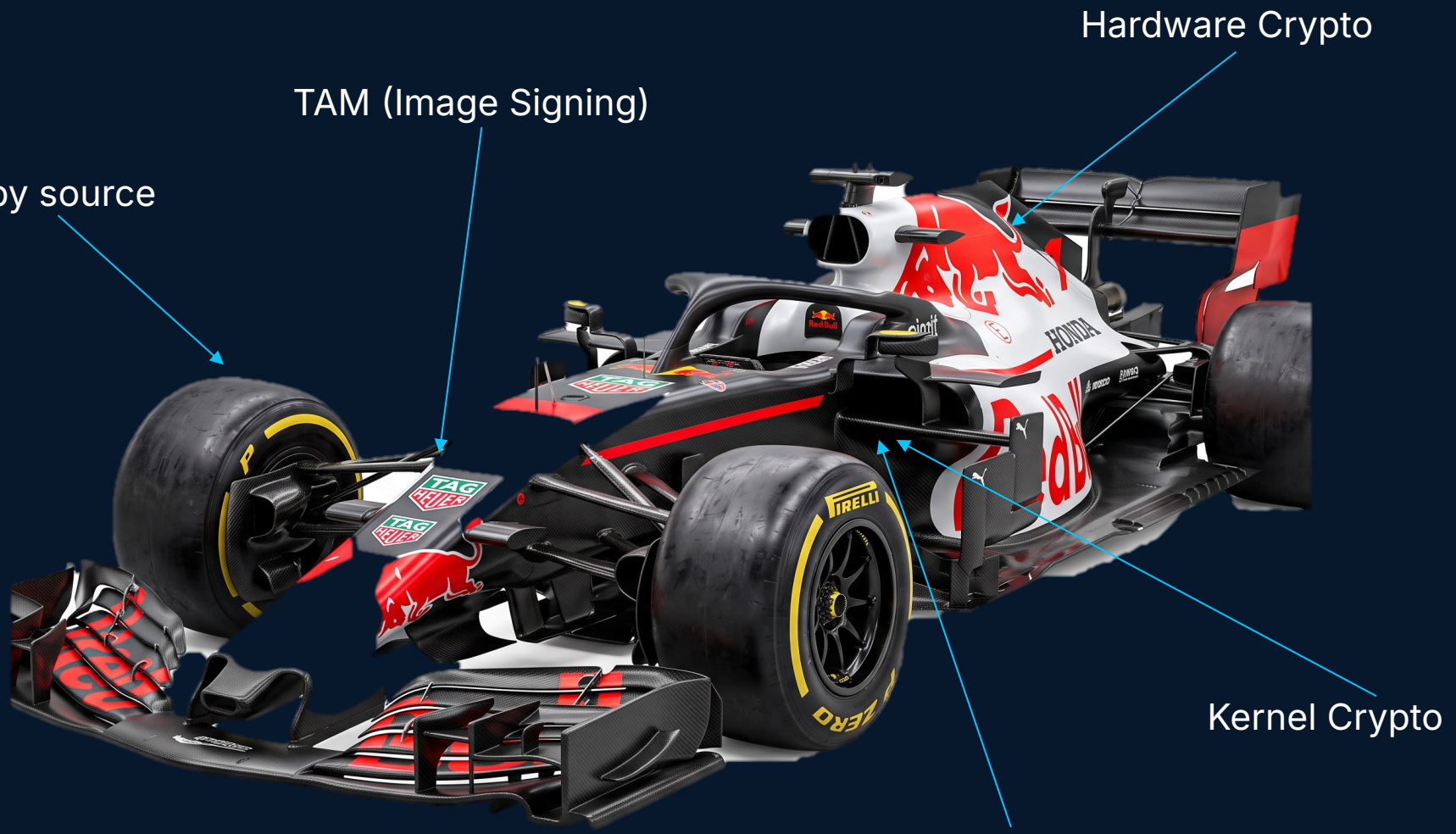
Today’s approach – validate each platform



Each full stack submission is $16 - $17.5K in CMVP fees, plus extensive lab costs. Each validation is **18 – 24** months to completion, clogging the queue and validation team resources

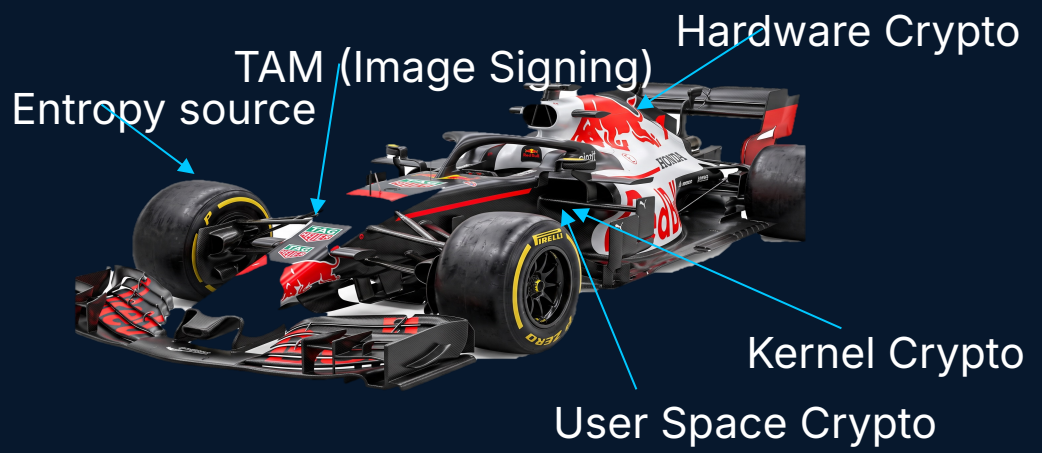
© 2026 Cisco and/or its affiliates. All rights reserved.

The certification puzzle



© 2026 Cisco and/or its affiliates. All rights reserved.

Build the car



1 **Entropy source validation (ESV/90C)**
→ **E# certificate issued**

- Perform heuristic analysis and collect entropy samples
- Must COMPLETE first. Entropy can no longer ride along in a module submission

2 **CAVP algorithm validation (ACVTS)**
→ **A# certificates issued**

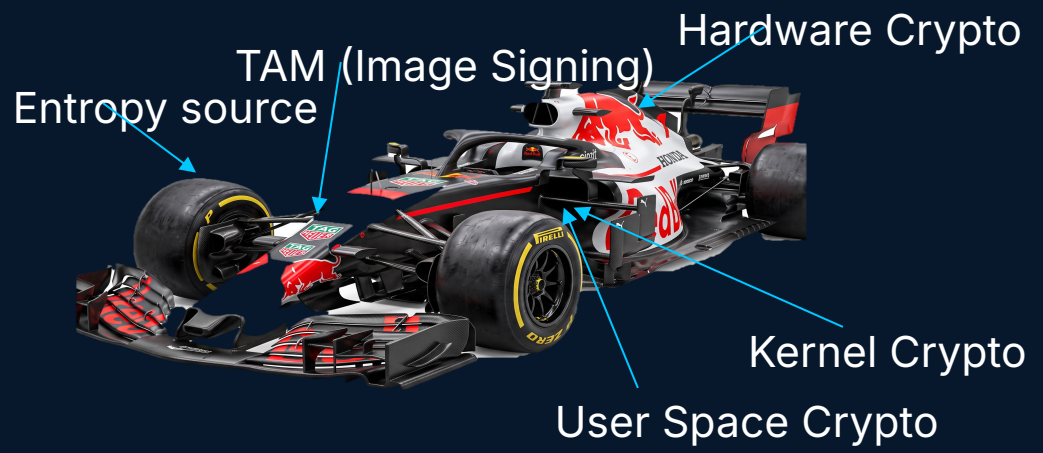
- Required for each EVM

3 **Validate each EVM**
→ **EVM certificate must be Active before moving forward**

- Complete validations in parallel
- IG 1.A 4.d – the EVM must be Active when the IUT is submitted

© 2026 Cisco and/or its affiliates. All rights reserved.

Validate each EVM



1 **Crypto Library (User Space and Kernel)**

- Identify validation path – full validation or rebrand
- Compile complete list of operational environments (tested and vendor affirmed)
- Ensure OEs claimed on the ESV

2/3 **TAM (Image Signing)**

- Identify manufacturer – may need third-party assistance
- Confirm all other FIPS requirements met without a platform
- May be done in parallel with other EVM validations

2/3 **Hardware Crypto**

- Identify manufacturer – may need third-party assistance
- Can the hardware be certified standalone, or should it be bound to the crypto library for key generation?
- Confirm all other FIPS requirements are met without a dependency on the platform
- May be done in parallel with other EVM validations

© 2026 Cisco and/or its affiliates. All rights reserved.

Leverage the options

OEUP

- May be performed on each module in the car – kernel crypto, user space crypt, hardware crypt, and TAM
- Least expensive option with fastest return on investment
- Must perform testing to add OE to ESV and ACVP certificates
- Minimal regression testing
- Sufficient to meet many regulatory requirements

Embedded Submission

- Utilized when the platform must have its own certification
- Full submission price, longer time to completion, but not as long as a full submission with each crypto component being validated
- Claim embedded modules – testing and source code review only required to show how the EVMs are used within the IUT

Pursue validation approach based on customer needs

© 2026 Cisco and/or its affiliates. All rights reserved.

The sustaining loop


Planning and well timed pit stops take the checkered flag
Dropbox
Gemini
cisco
workday
intel

The sustaining loop – this is what makes the strategy work

Certificates last 5 years. Review in years 2 – 3, act in year 4 – the chain must be revalidated in order, and order takes time.

YEAR 2 - 3

Review

- Confirm budget for next cycle
- Audit the full dependency chain
- Confirm EVM still Active
- Check upcoming algorithm transitions
- If significant code changes, perform FULL submission

YEAR 4 Q1

EVM first

- Submit UPDT on the EVM
- Resets the EVM sunset to 5 years
- Must COMPLETE before dependents file

YEAR 4 Q3

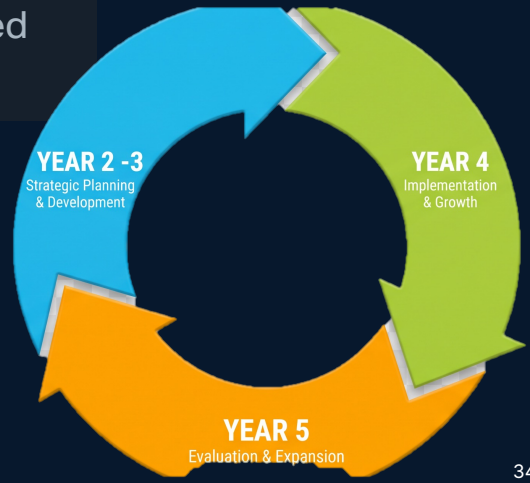
Dependents

- Submit UPDT on each dependent IUT
- Only after the EVM validation completes
- Resets each dependent's sunset
- Chain is now realigned on one date

YEAR 5

Clear

- All certificates Active
- Sunsets synchronized, not drifting
- Master clock resets
- Repeat



© 2026 Cisco and/or its affiliates. All rights reserved.

The value proposition

Fixed Costs

ESV Validation

Algorithm Validation

Building the Car

EVM = $16,000 x 4 (plus lab fees) – 18 – 24 months to complete – run in parallel

OEUP - $5,500 (plus lab fees) for ~20 additions – 2 – 3 months to complete minimal testing

Full EVM Submissions - $16,000 but use these sparingly – shorter completion time as all crypto is validated

The Traditional Approach

Full Submission = $16,000 x ? (plus lab fees) – 18 – 24 months to complete

Full source code review and operational testing of all crypto providers with each submission

Difficult to run more than two in parallel

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

The take aways

Continue the conversation with the Cryptographic Module Users Forum

Join today!

www.cmuf.org



© 2026 Cisco and/or its affiliates. All rights reserved.

The next 90 days

01 Identify each EVM

- Identify each crypto provider
- If an EVM is validated, record each sunset date. Can the EVM be updated to restart the clock
- Map the FULL dependency chain, not one level

02 Classify each pairing

- Bound or embedded, per IG 1.A 2 / 3
- Check security level compatibility (4.b)
- Check OE congruence for bound pairs (3.a)

03 Fix the entropy architecture

- Direct GetEntropy() access from every module
- One ESV, cited platform-wide
- Size the source to your strongest future key

04 Build the delegation register

- Every requirement met via the EVM
- Which other assertions it touches (IG 1.A 3.b)
- Confirm self-tests are NOT delegated

06 Initiate the validations

- Contract and initiate full submissions
- OE-addition commitments with dates
- CVE notification and remediation duties

05 Stand up the program calendar

- Master clock = earliest sunset in the chain
- Year-3 review, year-4 UPDT — EVM first
- Named owner and funded budget line

© 2026 Cisco and/or its affiliates. All rights reserved.

Key takeaways

The opportunity

Binding and embedding is an explicit, testable validation option.

Complete the puzzle and have multiple validation paths going forward

The catch

Understand how all parts of the car fit together.

EVM sunset dates set scheduling for the chain. Ensure all FIPS requirements are met across the EVMs.

The answer

Once the puzzle is built, run the race, ensuring effective pitstops along the way.

Cryptographic security is a program, NOT a project.

Build the car,
run the race

© 2026 Cisco and/or its affiliates. All rights reserved.

Questions?




CISCO