

Navigating the OCP S.A.F.E.™ Process for Vendors



Rob Wood
Managing Partner

Rickey Wang
Security Consultant



AUGUST 11-12, 2026
TAIPEI, TAIWAN

Outline

- 1 What is OCP S.A.F.E.™
- 2 Preparing for Security Assessment
- 3 Engagement Process
- 4 What is OCP S.O.L.I.D.
- 5 Caplitra Trademark Review

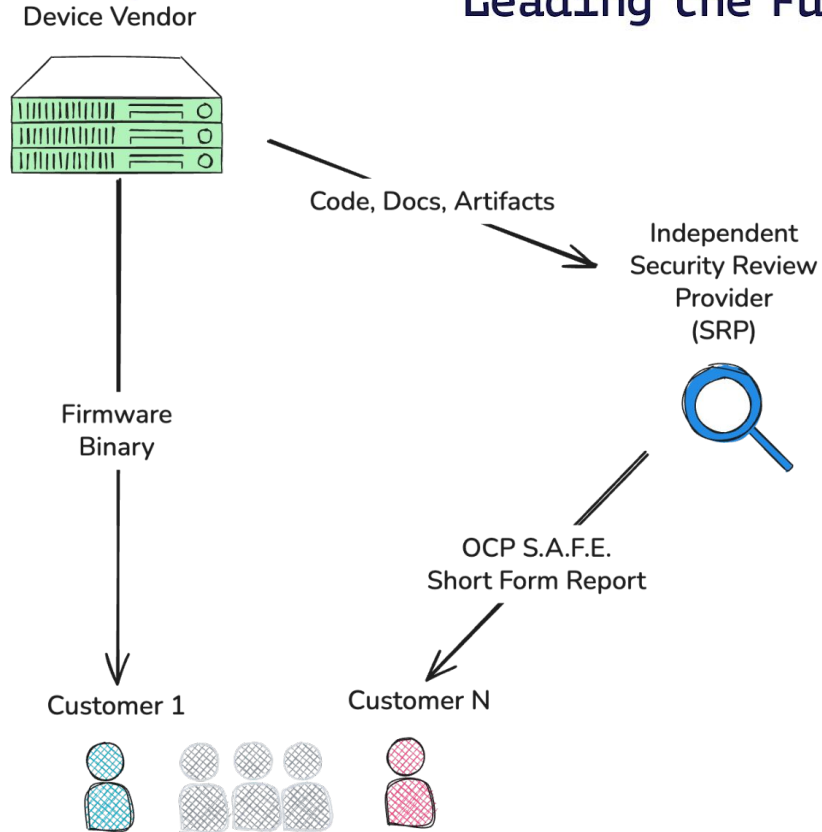
What is OCP S.A.F.E.™

- Framework for reusable security assessments
- Evidence that a security review was performed
- Short-Form Report (SFR) is accepted and reusable across customers
- SFR is published to OCP S.A.F.E.™ GitHub repository



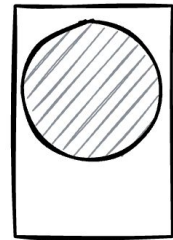
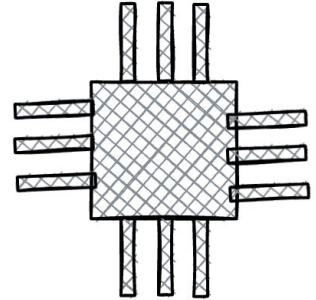
Leading the Future of AI

Common customer acceptance
Harmonized security standards
Transparent and verifiable



Who is OCP S.A.F.E.™ for?

- Device or firmware vendors:
 - Storage devices (SSD/HDD, NVMe, CXL, etc)
 - CPUs
 - GPUs and accelerators
 - Network devices
 - Power systems
 - Cooling systems
- UEFI vendor requiring Microsoft UEFI signing (as of 2025)



" I have to **fix every vulnerability**,
have my flaws **published for everyone to see**,
with all the **review being done by AI**"

~~"I have to fix every vulnerability,
have my flaws published for the world to see,
with all the review being done by AI"~~

None of these are true!

Before you start...

- Select a Security Review Provider (SRP) from the OCP-approved list
 - Available on OCP S.A.F.E.™ Github Repo
- Engage **early** to avoid rewrites or re-spins
 - Architectural definition
 - Major milestones
- Development-phase review findings are **private**

1 - Determine Target and Scope

Joint discussion between Security Review Provider (SRP) and Vendor
(often input from Customer)

Target

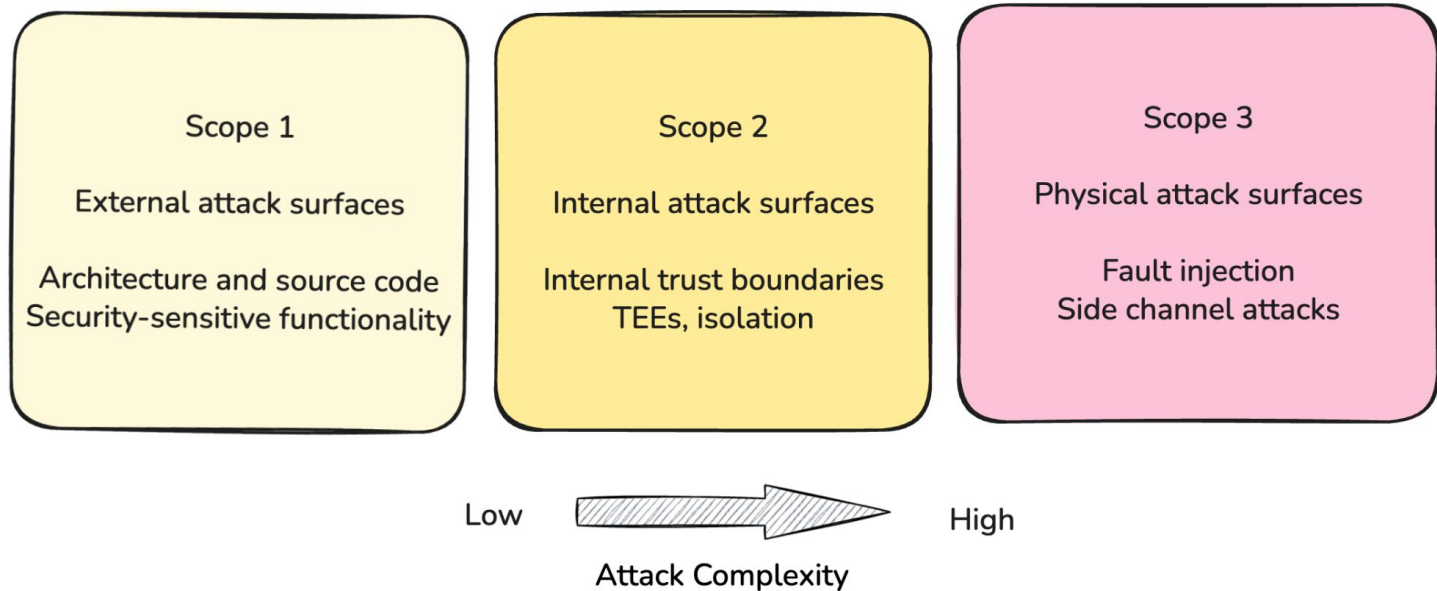
What is being tested

- What is the product, how is it used
- Hardware, ROM, Firmware?
- Third party components?

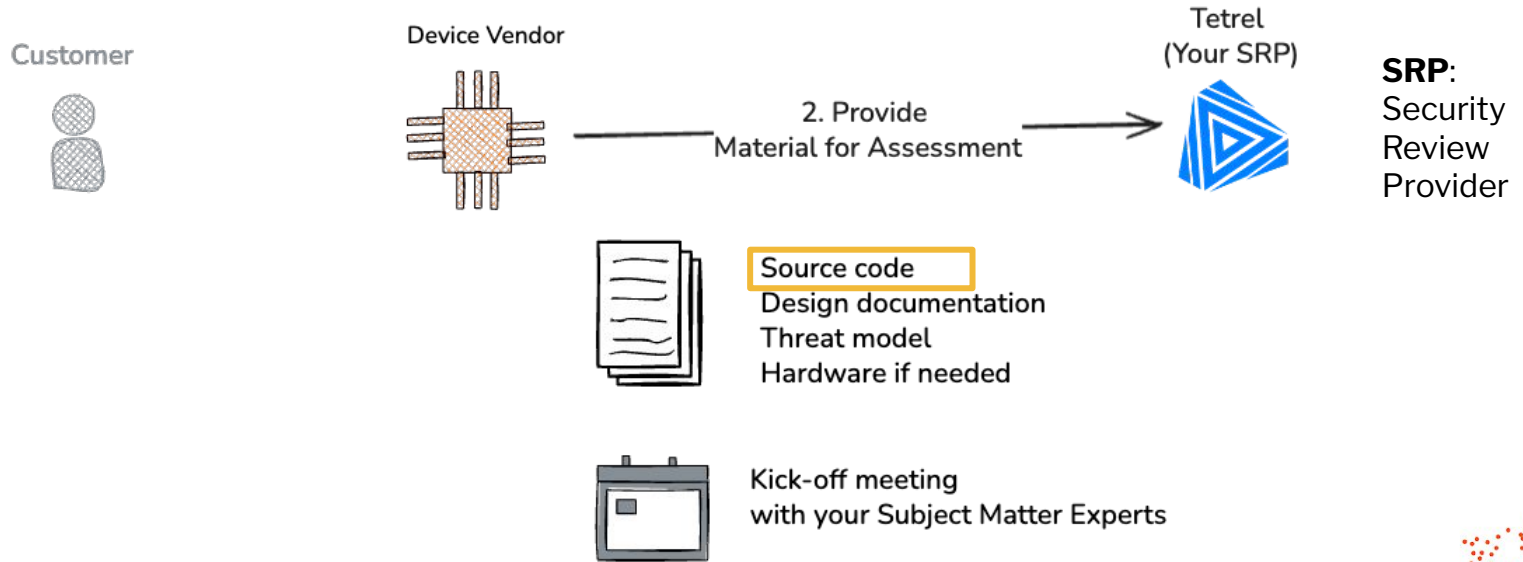
Scope

How deep is the Threat Model

OCP S.A.F.E.™ Review Scopes

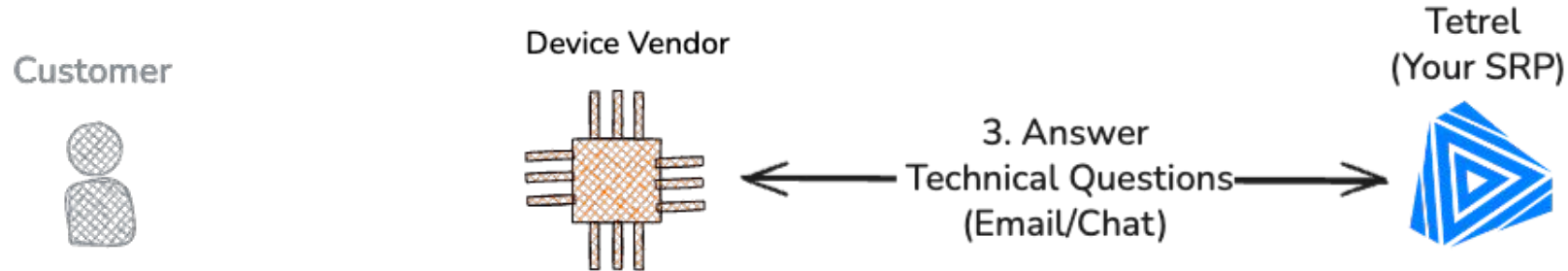


2 - Prepare Materials



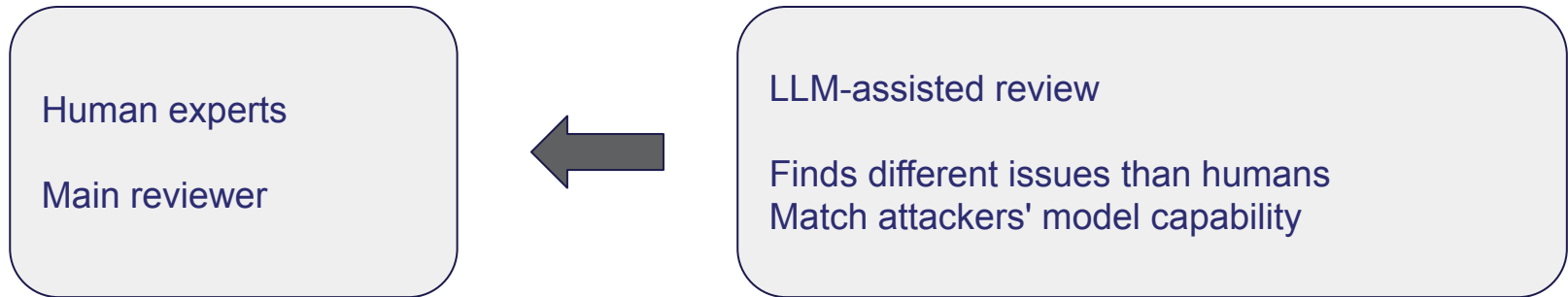
3 - Code Review

- Primarily expert-led manual review
- Additional LLM-assisted review (required by Jan 2027)



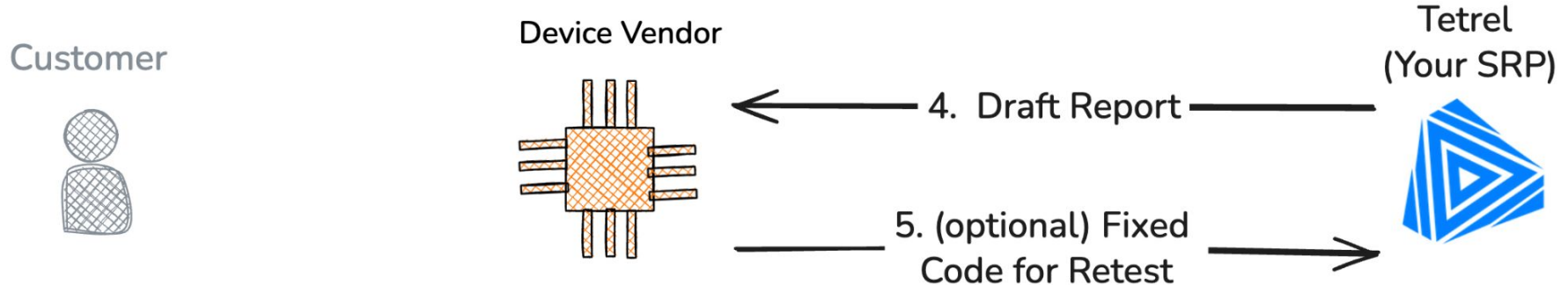
3 - Code Review

- Primarily expert-led manual review
- Additional LLM-assisted review (required by Jan 2027)

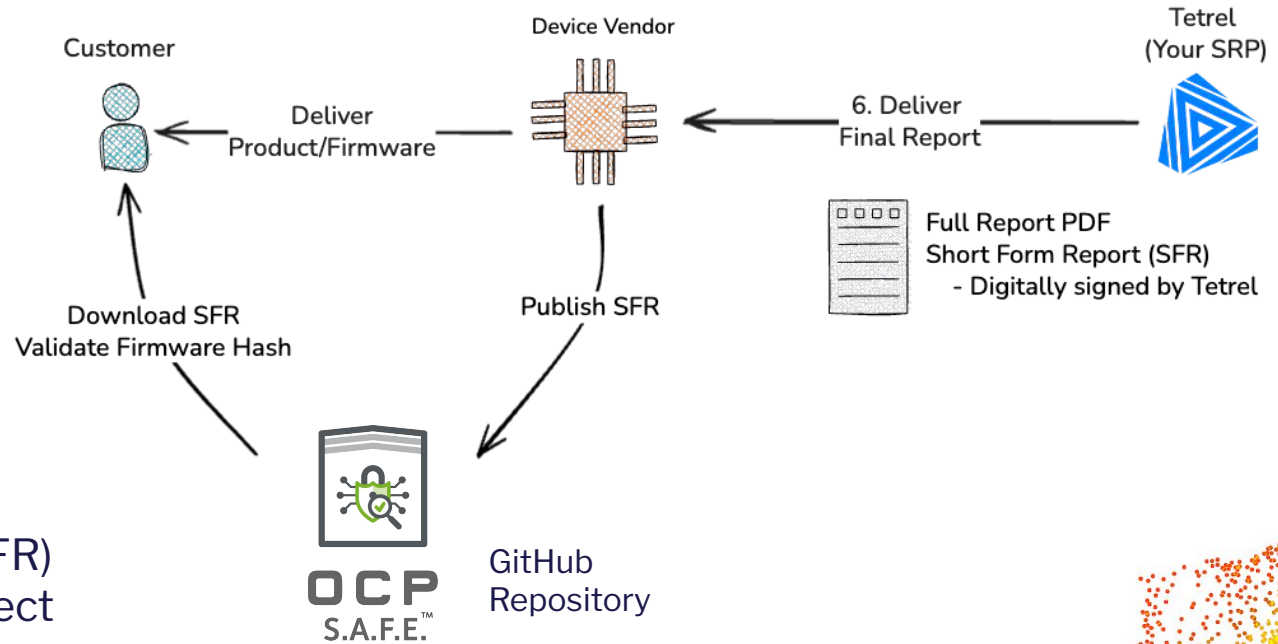


4 & 5 - Draft Report / Retest

- OCP S.A.F.E.™ has **no** minimum acceptance criteria
- SRP does not mandate fixes
- Mandatory for UEFI signing and OCP S.O.L.I.D. (more on that later)



6 - Publish



Vendor publishes
Short-form Report (SFR)
to OCP S.A.F.E.™ Project

6 - Publish

Submissions to OCP S.A.F.E.™ git repo
must come from the vendor

Vendor controls timing and messaging

SRP does not publish anything



GitHub
Repository



AUGUST 11-12, 2026
TAIPEI, TAIWAN

Navigating the OCP S.A.F.E.™ Process for Vendors
中英文術語對照表 tetrelsec.com/ocp



Common Timeline Risks

- Contract paperwork
 - Often slowest with large companies
- Kick-off delays
 - Access to code is necessary to start review
- Project size
 - Multiple reviewers are often assigned to help constrain timeline
- Remediation delays
 - Fixes can take time, and (occasionally) multiple iterations
 - Depends on Vendor development activities
- Final firmware hash generation
 - If SRP cannot build final binary, Vendor must provide the hash digest
 - This can delay if it requires post-tape-out testing, or final fuse configuration

Common Questions

- Multiple related product SKUs
- Fees
 - Depends on complexity
 - Efficiencies for multiple related products
- Efficiencies with other security programs
 - Significant overlap with technical testing aspects of **IEC-62443, EU CRA/RED, EN 17927 SESIP**



OCP S.O.L.I.D.

- Describes what security features a product must have
 - Self-assessment is checked for gaps during OCP S.A.F.E.™ review
- Long-Form Report contains a short compliance summary



AUGUST 11-12, 2026
TAIPEI, TAIWAN

Navigating the OCP S.A.F.E.™ Process for Vendors
中英文術語對照表 tetrelsec.com/ocp





Caliptra Trademark

- Caliptra: open source Root-of-Trust
 - RTL, firmware, reference interface libraries
 - Free to use!
- Trademark usage is subject to integration review requirements.
 - i.e., integration must be correct!
- Trademark review uses the same set of trusted Security Review Providers as OCP S.A.F.E.™
- Review is largely documentation-based, but some RTL evidence is required



You do **NOT** have to fix everything

Findings do **NOT** have to be published

AI is **NOT** replacing human reviewers

Thank You!

tetrelsec.com/ocp

OCP S.A.F.E.™ 中英文術語對照表
Example Short-Form Report
Links to OCP S.A.F.E.™ Github repository
FAQs

