بسمه تعالی

درخواست طرح پیشنهادی (RFP)

طراحی و تجاری‌سازی تراشه

TPM (Trusted Platform Module)

مرکز ملی پیشران طراحی تراشه
National Chip Design Center

شهریور ۱۴۰۵

۱- مقدمه

ماژول پلت‌فرم مورد اعتماد[۱](TPM) از نظر محل و نحوه پیاده‌سازی به ماژول پلتفرم مورد اعتماد مجزا[۲]، ماژول پلتفرم مورد اعتماد یکپارچه[۳]و ماژول پلتفرم مورد اعتماد مبتنی بر میان‌افزار[۴]تقسیم می‌شوند. طرح پیشنهادی حاضر صرفاً مربوط به طراحی یک Discrete TPM 2.0 است. TPM یک تراشهٔ امنیتی است که برای ایجاد ریشه اعتماد سخت‌افزاری[۵]در تجهیزات رایانه‌ای، مخابراتی و مراکز داده به کار می‌رود. وظیفه اصلی آن حفاظت از کلیدهای رمزنگاری، تأیید صحّت سیستم و جلوگیری از دستکاری نرم‌افزار و سخت‌افزار است. در تجهیزات ارتباطی و داده مانند روتر، سوئیچ، مودم، سرور، فایروال، ایستگاه پایه مخابراتی و تجهیزات شبکه، TPM معمولاً روی برد اصلی نصب شده و از طریق گذرگاه‌هایی مانند SPI یا I^2C به پردازنده اصلی متصل می‌شود. TPM در تجهیزات بسیاری رایج است از جمله: روترهای سازمانی، سوئیچ‌های لایه سوم فایروال‌ها، مودم‌های PON، تجهیزات 5G، ایستگاه‌های پایه، سرورها، تجهیزات شبکه گسترده مبتنی بر نرم‌افزار[۶]، تجهیزات رایانش لبه‌ای چنددسترسی[۷]، سیستم‌های IoT صنعتی. TPMها چند وظیفه اساسی دارند که به شرح زیر می‌باشد:

- تولید کلیدهای رمزنگاری: تولید کلیدهای RSA، تولید کلیدهای ECC، تولید اعداد تصادفی واقعی (TRNG)؛
- ذخیره امن کلیدها: کلید خصوصی هرگز از تراشه خارج نمی‌شود. حتی سیستم‌عامل نیز نمی‌تواند آن را بخواند.
- Secure Boot: هنگام روشن شدن دستگاه ابتدا ROM Boot اجرا می‌شود، سپس Bootloader، بعد Firmware و نهایتا سیستم عامل. TPM هش (Hash) هر مرحله را ذخیره می‌کند. TPM اندازه‌گیری‌های مربوط به اجزای زنجیره بوت را در PCRها ثبت و برای گواهی وضعیت و اعمال سیاست‌های امنیتی فراهم می‌کند. تصمیم‌گیری درباره ادامه، توقف یا بازیابی فرآیند boot توسط platform Firmware/boot policy انجام می‌شود و TPM به‌تنهایی مسئول توقف boot نیست.
- اندازه‌گیری سلامت سیستم (Measured Boot): TPM دارای رجیسترهایی به نام PCR و Platform Configuration Registers است. مثلاً: PCR0 = BIOS Hash، PCR1 = Bootloader Hash، PCR2 = Kernel Hash، PCR3 = Driver Hash. با استفاده از این

---

[۱] TPM = Trusted Platform Module

[۲] Discrete TPM

[۳] Integrated TPM

[۴] Firmware TPM

[۵] Hardware Root of Trust

[۶] SD-WAN = Software-Defined Wide Area Network

[۷] MEC = Multi-access Edge Computing

رجیسترها، بعداً سرور مدیریت می‌تواند بررسی کند که دستگاه دقیقاً با چه Firmware بوت شده است.

- تائید وضعیت امنیتی از راه دور[۸]: این قابلیت برای تجهیزات شبکه بسیار مهم است. فرض کنید هزار روتر در سطح کشور نصب شده‌اند. مرکز مدیریت می‌تواند از هر روتر سؤال کند که ثابت کن Firmware تو دستکاری نشده است و TPM امضای دیجیتال PCRها را ارسال می‌کند. به این ترتیب مرکز مدیریت مطمئن می‌شود که دستگاه سالم است.
- ذخیره گواهی دیجیتال: TPM می‌تواند اعتبارنامه‌های تأییدکننده، موارد کلید رمزنگاری، مؤلفه‌های رمزنگاری‌شده و مؤلفه‌هایی را که تحت کنترل سیاست‌های امنیتی قرار دارند ایجاد، مدیریت و نگهداری کند. کلیدهای خصوصی TPM به‌صورت آشکار و بدون حفاظت، از مرز امنیتی هدف ارزیابی (TOE) خارج نمی‌شوند. با این حال، برخی مؤلفه‌های TPM را می‌توان به‌صورت داده‌های حفاظت‌شده و رمزنگاری‌شده، موسوم به بلاب (Blob)، در خارج از TPM ذخیره کرد؛ به‌گونه‌ای که استفاده از آن‌ها همچنان تابع سازوکارهای حفاظتی و سیاست‌های امنیتی TPM باشد.
- رمزنگاری دیسک: TPM می‌تواند از طریق sealing/unsealing و policy-based key release، از کلیدهای رمزنگاری مورد استفاده برای حفاظت از داده‌های ذخیره‌شده پشتیبانی کند.اگر SSD جدا شود، اطلاعات قابل خواندن نخواهد بود.
- حفاظت از Firmware: TPM می‌تواند از UEFI، BIOS، Bootloader و Secure Boot Keys محافظت کند.
- قابلیت‌های رمزنگاری: اکثر TPMهای جدید دارای Hash، SHA-1، SHA-256، و SHA-384 هستند. همچنین قادر به رمزنگاری نامتقارن (RSA-2048، RSA-3072، ECC P-256، ECC P-384) هستند.
- HMAC: TPMها معمولاً دارای HMAC[۹] برای احراز اصالت پیام هستند.
- مشتق‌سازی کلید: TPMها معمولاً دارای KDF[۱۰] برای مشتق سازی کلید هستند.

یک TPM برای آنکه قابل استفاده در صنعت باشد، معمولاً ضروری است که مطابق یا فراتر از استاندارد Trusted Platform Module 2.0 باشد. برای اینکه TPM قابل استفاده در تجهیزات ارتباطی مانند مودم‌های PON، روترها یا سرورها باشد، علاوه بر پیاده‌سازی استاندارد TPM 2.0، باید الزامات گواهی‌های امنیتی مانند Common Criteria و در صورت نیاز FIPS 140-3 را نیز از ابتدای طراحی سخت‌افزار و نرم‌افزار در نظر گرفت، زیرا این الزامات بر معماری، طراحی ضد دستکاری و فرآیند توسعه تأثیر مستقیم دارند. در نسل فناوری ۴۰

---

[۸] Remote Attestation

[۹] Hash-based Message Authentication Code

[۱۰] Key Derivation Function

نانومتر میکس‌سیگنال، چنین تراشه‌ای معمولاً مساحتی در حدود 20 میلی‌متر مربع دارد (بسته به اندازه حافظه امن، شتاب‌دهنده‌های رمزنگاری و ویژگی‌های ضد دستکاری)، و توان مصرفی آن معمولاً از چند ده تا چند صد میلی‌وات متغیر است. بازار TPM نسبتاً متمرکز است و تعداد کمی از شرکت‌ها بخش عمده آن را در اختیار دارند. از نظر فروش جهانی، کاربردها به سه دسته اصلی تقسیم می‌شوند:

- رایانه‌های شخصی و لپ‌تاپ؛
- سرورها و مراکز داده؛
- تجهیزات شبکه، مخابراتی و صنعتی.

اگر فقط «تراشه‌های TPM مستقل» را بشماریم، بزرگترین تولیدکنندگان TPM عبارتند خواهند بود از:

شرکت	جایگاه بازار	حوزه اصلی
Infineon Technologies	شماره ۱	PC، سرور، تجهیزات صنعتی، خودرو
Nuvoton Technology	شماره ۲	PC، سرور، Embedded
STMicroelectronics	شماره ۳	Industrial، IoT، Automotive
Microchip Technology	سهم کمتر	Embedded، Industrial
Texas Instruments	بسیار محدود	برخی محصولات امنیتی، نه تمرکز اصلیTPM

نکته مهم: مجری مجاز است و اکیداً توصیه می‌شود که هر اقدامی را که به امنیت بیشتر تراشه کمک می‌کند. حتّی اگر در این RFP قید نشده باشد یا حتّی اگر بر خلاف این RFP باشد، اعمال نماید. این RFP صرفاً بیان حداقل‌های مدنظر است.

۲- ضرورت منشاء نیاز

برای کاربردهای حساس همانند زیرساخت‌های حیاتی، تجهیزات دولتی، دفاعی یا برخی سامانه‌های مخابراتی، اتکا به TPM ساخت آمریکا یا کشورهای تحت سلطهٔ آن، دارای مخاطرات معناداری است. در اکثر کشورها منشأ قطعه می‌تواند بر تصمیم خرید اثر بگذارد. استفاده از TPMهای خارجی، بخصوص TPMهای ساخت آمریکا یا کشورهای تحت سلطه‌اش، مخاطرات بسیار جدّی زیر را در بر دارد:

- **ریسک نفوذ در زنجیره تأمین:** مهم‌ترین ریسک استفاده از TPM خارجی مشکلات زنجیرهٔ تأمین است. TPM ریشه اعتماد (Root of Trust) سیستم است. اگر در زنجیره تأمین آن مشکلی رخ دهد، کل امنیت دستگاه زیر سؤال می‌رود. این ریسک‌ها شامل: جایگزینی تراشه با نسخه تقلبی، دستکاری در مرحله تولید، تغییر Firmware پیش از تحویل، نفوذ به فرآیند Provisioning کلیدها است. این ریسک‌ها برای هر کشوری وجود دارند، اما در شرایط تنش سیاسی، ارزیابی اعتماد به زنجیره تأمین اهمیت بیشتری پیدا می‌کند.

- **ریسک تحریم و توقف تأمین:** حتی اگر TPM از نظر فنی کاملاً سالم باشد، ممکن است: صادرات آن محدود شود، دریافت به‌روزرسانی Firmware دشوار شود، پشتیبانی فنی قطع شود، یا تأمین قطعات یدکی مختل شود. برای محصولی که قرار است ۱۰ تا ۱۵ سال در میدان عملیاتی باشد، این موضوع اهمیت زیادی دارد.
- **ریسک آسیب‌پذیری‌های کشف‌نشده:** این نگرانی‌ها درباره هر TPM، صرف‌نظر از کشور سازنده، وجود دارد: خطای طراحی، باگ Firmware، پیاده‌سازی ضعیف الگوریتم‌های رمزنگاری، ضعف در تولید اعداد تصادفی (TRNG). به همین دلیل محصولات معتبر معمولاً توسط آزمایشگاه‌های مستقل ارزیابی می‌شوند.
- **وجود Backdoor**: از نظر فنی، هر تراشه پیچیده‌ای می‌تواند دارای آسیب‌پذیری یا قابلیت مخفی باشد. با توجّه به اینکه کشف چنین مشکلی در یک TPM تقریبا غیر ممکن است و این تراشه در بسیاری از اوقات در کاربردهای حسّاس استفاده می‌شود، بسیار بعید بنظر می‌رسد که کشورهای سازنده در آن راه نفوذی برای خود تعبیه نکرده باشند. چنین مشکلی در TPM دست کشورهای متخاصم برای نفوذ و آسیب زدن به سامانه‌های کشور را بسیار باز می‌گذارد.

۳- هدف و الزامات فنّی فراخوان

هدف از این فراخوان، شناسایی و انتخاب تیم مناسب برای پژوهش، طراحی، نمونه‌سازی، تست و تدوین دانش فنی یک Discrete TPM 2.0 عمومی با قابلیت به‌کارگیری در سرورهای سازمانی، رایانه‌های کاربری، رایانه‌های صنعتی و تجهیزات شبکه، با تمرکز و اولویت نخست بر سرورهای سازمانی است. به‌گونه‌ای که محصول نهایی از نظر کارایی، سطح امنیت، مصرف توان و امکان اخذ گواهی‌های امنیتی و فنی، توان رقابت و مقایسه با محصولات شاخص و مطرح موجود در بازار را داشته باشد. این TPM باید hardware Root of Trust باشد و نباید به یک MCU عمومی با Firmware امنیتی ساده تبدیل شود. این پروژه نیازمند CPU را بزرگی نیست و ارزش این محصول در CPU نیست؛ بلکه در TPM 2.0 compliance + key isolation + NV architecture + PCR/attestation + crypto + physical attack resistance + certification است. ریسک قابلیت‌های مخفی، undocumented functionality یا آسیب‌پذیری عمدی/غیرعمدی در زنجیره تأمین باید در threat model و supply-chain security analysis در نظر گرفته شود. طراحی و تأمین محصول باید به‌گونه‌ای باشد که قابلیت ممیزی مستقل، کنترل Firmware و کلیدهای provisioning و ارزیابی امنیتی را برای کارفرما فراهم کند. با توجه به الزامات این پروژه شامل TPM 2.0، حافظه‌های امن، شتاب‌دهنده‌های RSA/ECC، TRNG/PUF، حفاظت‌های فیزیکی و به‌ویژه شتاب‌دهنده‌های سخت‌افزاری ML-KEM-1024، HQC-256، ML-DSA-87 و SLH-DSA در NIST Security Category 5، مساحت die در فناوری 40nm Mixed-Signal در مرحله معماری حدود 20 mm² برآورد می‌شود. مقدار هدف طراحی در بازه ۱۵ تا ۲۵

mm² (بسته به معماری نهایی PQC و RHBD) برآورد می‌شود. تجاوز از 25 mm² نیازمند تأ ییید کتبی کارفرما خواهد بود. مجری موظف است پیش از تثبیت نهایی مساحت، یک مرحله Prototype Synthesis با استفاده از کتابخانه واقعی PDK و Memory Macroها انجام داده و بودجه Area، Power و Timing را به تفکیک بلوک‌ها ارائه کند. عدد نهایی Die Size پس از تأیید این گزارش توسط کارفرما، به‌عنوان الزام قطعی پروژه تثبیت خواهد شد. الزامات فنّی که این تراشه باید داشته باشد شامل موارد زیر می‌باشد.

۳ -۱ - محصول هدف

- نوع محصول: نسخه نخست محصول با تمرکز بر کاربردهای سرورهای سازمانی و مراکز داده توسعه خواهد یافت؛ معماری محصول باید به‌گونه‌ای طراحی شود که در نسل‌های بعدی، امکان ایجاد گونه‌های محصولی (SKU) ویژه رایانه‌های کاربر، رایانه‌های صنعتی و تجهیزات شبکه، با حداقل تغییرات در میان‌افزار، پیکربندی و یکپارچه‌سازی با پلتفرم، فراهم شود.
- هدف: x86-64 / ARM64 servers ، و Motherboard و Server Management Platform؛
- نسل فناوری: 40 nm - Si CMOS؛
- نوع بسته‌بندی: QFN یا BGA؛ package size و pin-count باید توسط تیم طراحی بر اساس electrical, thermal, security, DFT و OSAT constraints پیشنهاد و با تأئید کارفرما نهایی شود؛
- محدوده دمایی: از -40 °C تا +125 °C؛
- ولتاژ تغذیه: 1.8/3.3 V according to the platform’s I/O؛
- آمادگی تطابق با: حدّاقلّ Common Criteria EAL4+؛ ترجیحاً EAL5+ و FIPS-140 level 3

بلوک	Specification
CPU	RV32IMC + Zicsr + Zifencei
Hart	1
Pipeline	4-stage in-order pipeline preferred; 3-stage acceptable if justified by area/power/security trade-off
CPU clock	50-150 MHz, target 100MHz
Boot ROM	64 KB
Flash	1 MB
Protected NVM	64 KB
SRAM	64 KB
Secure Key RAM	8 KB
Crypto RAM	8 KB
OTP/eFuse	4 KB
PCR	24 × SHA-256 minimum
RSA	2048/3072/4096
ECC	P-256/P-384/P-521

بلوک	Specification
PQC KEM	ML-KEM-1024 — NIST Security Category 5 — mandatory hardware accelerator
PQC KEM Backup	HQC-256 — NIST Security Category 5 — mandatory hardware accelerator; implementation shall track the final NIST/FIPS specification
PQC Signature	ML-DSA-87 — NIST Security Category 5 — mandatory hardware acceleration
PQC Signature Diversity	SLH-DSA-SHAKE-256f mandatory; SLH-DSA-SHA2-256f preferred/architecture-ready.
PQC Signature Backup	FN-DSA-1024 (Falcon-1024) — Category 5, subject to final NIST/FIPS standardization status; architecture shall reserve a crypto-agile interface
PQC Hybrid KEM	Mandatory hybrid ML-KEM-1024 + HQC-256 operation
PQC Hybrid Signature	ML-DSA-87 + SLH-DSA-SHAKE-256f
PQC Security Category	All mandatory PQC security-critical operations shall support NIST Security Category 5 or stronger
PQC Hardware	ML-KEM-1024 and HQC-256 shall not be software-only
PQC Crypto-agility	Mandatory
AES	128/256
SHA	256/384/512
HMAC	SHA-256/384/512
KDF	TPM-required KDFs
TRNG	HW + health tests
DRBG	HW-assisted
Key Manager	Dedicated
NV Manager	Dedicated
Atomic NVM	Yes
A/B update	Yes
Anti-rollback	Yes
Secure Boot	Yes
Recovery	Yes
Host interface	SPI mandatory; I²C/SMBus-compatible interface architecture-ready; interface selection shall be finalized according to target platform requirements.
Locality	0–4
Command FIFO	8 KB
Watchdog	Independent
Clock monitor	Independent
Brownout	Yes
Voltage monitor	Yes
Temperature sensor	Yes
Tamper detector	Yes
Fault response	Yes

بلوک	Specification
Key zeroization	Yes
Secure Debug	Yes, production locked
DFT	Scan + MBIST + secure test
ECC	SEC-DED
Operating temp.	−40 to +125 °C
Process target	40 nm initially
Package	QFN/BGA
Security target	CC EAL4+ minimum; EAL5+ and FIPS-140 level 3 preferred
FIPS	140-3 capable

پیاده‌سازی‌های ML-KEM-1024 و HQC-256 باید از مسیرهای داده رمزنگاری (Cryptographic Datapath) با کنترل مستقل استفاده کنند و باید قادر باشند به‌صورت مستقل از یکدیگر اجرا شوند. ML-KEM-1024 و HQC-256 باید مسیرهای داده رمزنگاری شده‌ای داشته باشند که سیاست امنیتی سخت‌افزار اجرای مستقل، محدودسازی خطای مستقل، صفرسازی مستقل و گزارش‌دهی رویداد امنیتی مستقل را پشتیبانی کنند. منظور از استقلال مسیر داده، لزوماً تکرار کامل تمام منابع محاسباتی و حافظه‌ای (مانند واحدهای SHA یا حافظه‌های موقت) نیست. اشتراک‌گذاری کنترل‌شده primitiveها مجاز است، مشروط بر اینکه جداسازی امنیتی، Zeroization مستقل، Fault Containment و عدم ایجاد Single Point of Compromise به‌صورت رسمی در مرحله Formal Verification اثبات شود و نشان داده شود که باعث ایجاد آسیب‌پذیری حالت مشترک که بتواند هر دو الگوریتم را به خطر بیندازد نمی‌شود.

CPU / Control Core - ۲- ۳

توجّه شود که نیازی به CPU بسیار سریع نیست و بخش سنگین کار باید در crypto accelerator ها انجام شود. هسته RV32IMC صرفاً به‌عنوان یک Embedded Secure Control Processor جهت اجرای Firmware و مدیریت State Machine عمل می‌کند و نباید به‌عنوان یک MCU عمومی با قابلیت اجرای کد دلخواه خارج از مرز امنیتی TPM تفسیر شود.

مشخصه	پیشنهاد
CPU	RV32IMC + Zicsr + Zifencei
Hart	Single-hart
Pipeline	4-stage in-order pipeline preferred; 3-stage acceptable if justified by area/power/security trade-off
Frequency	50-150 MHz
Execution	In-order
PMP	حداقل ۸ region

Privilege	M-mode mandatory; U-mode optional; S-mode only if justified by the Firmware architecture; MMU not required; PMP ≥8 regions mandatory.
Secure boot	Mandatory
Debug	Internal JTAG/SWD but production-locked
MPU/PMP	Mandatory

۳ -۳ - حافظه

512 KB Flash شاید برای یک TPM بسیار ساده کافی باشد، اما برای TPM سروری که Firmware، command implementation، NV storage، recovery و future features دارد، 1 MB ارجح اســت. نوع حافظه غیرفرار (NVM) باید از نوع Embedded Flash (eFlash) یا MTP (Multi-Time Programmable) با قابلیت Endurance مناســب برای NV Storage و Anti-rollback باشــد. انتخاب نهایی تکنولوژی NVM بر اساس Trade-off بین مساحت، امنیت و هزینه در مرحله Architecture Freeze به تأیید کارفرما می‌رسد.

Memory	مقدار پیشنهادی
Boot ROM	64 KB
Internal Flash/Code NVM	768 KB–1 MB target; final capacity shall be determined by Firmware sizing and security architecture.
Protected/High-Endurance NVM	≥64 KB target
SRAM	≥64 KB
Secure Key RAM	≥8 KB
Crypto scratch RAM	≥64 KB
OTP/eFuse	2–4 KB equivalent, with exact security-fuse requirements defined during architecture

۳ -۴ - TPM 2.0 Engine

این بخش باید تقریباً کامل و مطابق TCG TPM 2.0 Library 1.85 باشــد و مجموعه الزامی فرمان‌های[1] زیر را داشته باشد:

- Startup / Shutdown;
- Self-Test;
- GetCapability;
- PCR operations;
- NV operations;
- Object creation;
- Object loading;
- Key management;

[1] Mandatory command families

- Hash;
- HMAC;
- MAC;
- Random;
- RSA;
- ECC;
- Authorization;
- Sessions;
- Context management;
- Quote;
- Sign;
- Verify;
- Attestation;
- NV Index management;
- Dictionary-attack protection;
- Hierarchy management;
- PCR policy;
- Platform hierarchy;
- Endorsement hierarchy;
- Lockout hierarchy.

خط مبنای پروژه در زمان آغاز باید TPM 2.0 Library Specification Version 185 باشد. هرگونه اصلاحیه، بازنگری یا مشخصات فنی جدید که پس از نهایی‌شدن الزامات منتشر شود، تنها پس از بررسی آثار و پیامدهای آن و با تأیید کارفرما، در خط مبنای پروژه اعمال خواهد شد.

PCR - ۵- ۳

برای server TPM، حداقل 24 PCR registers با:

- SHA-256 PCR bank;
- Support for multiple PCR banks according to the TPM specification;
- PCR Extend;
- PCR Read;
- PCR Reset in authorized cases;
- PCR Policy;
- locality support.

Cryptography - ۶- ۳

الگوریتم ها باید مطابق TPM 2.0 Library Specification v185 و TCG Algorithm Registry انتخاب شوند. در حداقل profile موردنیاز پروژه، پشتیبانی سخت‌افزاری از AES-128/256، SHA-256/384/512، HMAC، RSA-2048/3072/4096 و ECC profiles موردنیاز TCG الزامی است. هر الگوریتم یا mode خارج از TPM mandatory/selected profile باید به‌صورت optional مشخص شود.

Symmetric:

- AES-128;
- AES-256;
- AES-CFB;
- AES-CBC;
- AES-CTR when required internally;
- AES-GCM when platform-specific requirements arise.

Hash:

- SHA-256;
- SHA-384;
- SHA-512.

HMAC:

- HMAC-SHA-256;
- HMAC-SHA-384;
- HMAC-SHA-512;

RSA:

- RSA-2048;
- RSA-3072;
- RSA-4096.

ECC:

- NIST P-256;
- P-384;
- P-521.

Post-Quantum Cryptography

ترا شه باید دارای زیر سیستم مستقل و سخت‌افزاری PQC با شد. پشتیبانی PQC صرفاً به صورت software library یا Firmware implementation قابل قبول نیست. حداقل الگوریتم‌ها و پارامترهای اجباری عبارتند از:

KEM
ML-KEM-1024 — NIST Security Category 5
HQC-256 — NIST Security Category 5

Digital Signature
ML-DSA-87 — NIST Security Category 5
SLH-DSA-SHAKE-256f — NIST Security Category 5
SLH-DSA-SHA2-256f — NIST Security Category 5

معماری باید به‌گونه‌ای باشـــد که FN-DSA-1024، بدون بازطراحی Root of Trust و Crypto API قابل اضافه‌شدن باشد.

Heterogeneous Hybrid Post-Quantum Cryptography

تراشه باید امکان اجرای همزمان یا مستقل حداقل دو الگوریتم PQC با مفروضات ریاضی متفاوت را فراهم کند. برای KEM، زوج اجباری ML-KEM-1024 + HQC-256 خواهد بود. ML-KEM مبتنی بر structured/module lattice است، در حالی که HQC مبتنی بر error-correcting codes است؛ بنابراین دو الگوریتم دارای فرض امنیتی و primitive ریاضی متفاوت هستند. NIST نیز HQC را مشخصاً به‌عنوان backup برای ML-KEM و با مبنای ریاضی متفاوت انتخاب کرده است. در Hybrid KEM، تراشه نباید صرفاً ciphertext دو الگوریتم را پشت سر هم ارسال کند. دو shared secret باید به یک hybrid shared secret توسط یک KDF/combiner امن و domain-separated تبدیل شوند و باید بتواند حالت‌های زیر را انتخاب کند:

ML-KEM-1024 only;
HQC-256 only;
ML-KEM-1024 + HQC-256 hybrid;
Classical + ML-KEM-1024 hybrid;
Classical + HQC-256 hybrid;
Classical + ML-KEM-1024 + HQC-256, if required by the platform.

در حالت hybrid، compromise شدن یکی از دو الگوریتم نباید به‌تنهایی موجب افشای کلید نهایی شود.

کاربرد	الگوریتم اصلی Level 5	زوج ناهمگون پیشنهادی	دلیل
KEM	ML-KEM-1024	HQC-256	Module-lattice + code-based
KEM	HQC-256	ML-KEM-1024	عکس حالت بالا
Digital Signature	ML-DSA-87	SLH-DSA-SHAKE-256f	lattice + hash-based
Digital Signature	SLH-DSA-SHAKE-256f	ML-DSA-87	hash-based + lattice
Digital Signature	SLH-DSA-SHA2-256f	ML-DSA-87	hash-based + lattice
Digital Signature	ML-DSA-87	SLH-DSA-SHA2-256f	lattice + hash-based
Future signature	FN-DSA-1024	ML-DSA-87 یا SLH-DSA-256f	NTRU-lattice + ML-lattice یا hash-based

TRNG - ۷- ۳

این بخش سخت‌افزاری باید شامل بلوک‌های زیر باشد:

- Ring oscillator / metastability entropy source;
- Online health test;

- Startup health test;
- Entropy conditioning;
- DRBG;
- Continuous monitoring;
- Failure indication;
- Zeroization on severe failure.

لازم به ذکر است که TRNG باید مستقل از CPU باشد.

۳-۸- Key Hierarchy

این قسمت قلب TPM است و باید دارای موارد زیر باشد:

- Endorsement Key;
- Storage Root Key;
- Attestation Key;
- Signing Keys;
- Encryption Keys;
- HMAC Keys;
- Derivation Keys;
- NV authorization;

Private key material نباید به CPU یا host export شود.

۳-۹- Key isolation

باید شامل Secure Key RAM و Key Manager بوده و CPU فقط handle یا reference دریافت کند، نه private key خام.

۳-۱۰- NV Storage

باید دارای موارد زیر باشد:

- NV indices;
- NV counters;
- NV bits;
- NV extend;
- NV write/read;
- Authorization;
- Policy authorization;
- Owner/platform/endorsement hierarchy;
- Lock-on-read;
- Lock-on-write;
- Write-once;
- Read-once when required;
- Anti-tearing;
- Atomic update;
- Wear leveling:
- ECC.

ترجیحاً 64 KB high-endurance protected NVM به‌همراه Atomic NVM Controller.

۳ -۱۱- A/B Firmware Update

باید دارای ویژگی‌های زیر باشد:

- Signed Firmware;
- Secure boot;
- Anti-rollback;
- Version counter;
- Atomic activation;
- Power-loss recovery;
- Recovery image;
- Firmware authenticity;
- Firmware integrity.

۳ -۱۲- Host Interface

SPT Interface به‌عنوان اینترفیس اصلی و اجباری محصول تعریف شود. I²C/SMBus و LPC/eSPI در نسخه اول محصول اجباری نیستند و در صورت نیاز به SKUهای آینده منتقل شوند. برای سرورهای جدید، SPI TPM با مشخّصات زیر احتمالاً انتخاب مناسبی است:

- 4-wire;
- Mode 0;
- High-speed;
- DMA is not required on the host;
- Internal FIFO;
- Command/response buffering;
- Timeout;
- Malformed-command detection;
- Bus fault detection.

البته مشخصات بالا اجباری نیستند و Interface باید مطابق specification مربوط به TPM platform profile انتخاب‌شده پیاده‌سازی شود. معماری باید به‌گونه‌ای باشد که در نسل‌های بعدی، پشتیبانی از eSPI (Embedded SPI) با حداقل تغییرات ممکن‌پذیر باشد.

۳ -۱۳- TPM Command FIFO

پیشنهاد می‌شود 4–8 KB command/response buffer با مشخّصات زیر باشد:

- Command length checking;
- Response length checking;
- Bounds checking;
- Timeout;
- Malformed packet detection;
- Authorization/session validation.

۳ -۱۴ Locality

برای TPM سروری Locality 0–4 را پشتیبانی کند. این برای تفکیک سطح دسترسی platform/Firmware/security operations مهم است.

۳ -۱۵ Platform Reset / Power

TPM باید نسبت به وضعیت platform حساس باشد و شامل بلوک‌های زیر باشد:

- POR;
- Brownout detector;
- Voltage monitor;
- Clock monitor;
- Watchdog;
- Reset controller;
- Tamper reset;
- Secure reset state;
- Power-loss detection.

۳ -۱۶ Clock

TPM باید دارای نوسان‌ساز مرجع داخلی یا منبع کلاک مستقل باشد. وجود کلاک امنیتی مستقل برای پایش امنیتی و اجرای سازوکارهای تشخیص دست‌کاری و خطا الزامی است. محدوده فرکانس هدف کلاک پردازنده/سامانه باید ۵۰ تا ۱۵۰ مگاهرتز (با هدف MHz۱۰۰) باشد. Sign-off نهایی باید مبتنی بر سناریوهای PVT و MCMM واقعی فناوری هدف انجام شود. اولویت اصلی صرفاً فرکانس کلاک نیست؛ بلکه وجود قابلیت‌های تشخیص اختلالات لحظه‌ای کلاک، پایش فرکانس، واکنش به خطای کلاک و کلاک امنیتی مستقل، الزامی و تعیین‌کننده است.

۳ -۱۷ Tamper Protection

داشتن امکانات زیر حتّی‌المقدور توصیه می‌شود:

- Voltage glitch detection;
- Clock glitch detection;
- Frequency anomaly detection;
- Temperature sensor;
- Reset anomaly detection;
- Fault injection detection;
- Memory ECC;
- Bus integrity checks;
- Secure state machine;
- Active shield;
- Light sensor;
- Die-level tamper mesh;
- Differential sensors;
- Magnetic/EM anomaly detection.

۳ -۱۸- Fault response

یک TPM کارآمد نباید صرفاً به شناسایی حملات یا رخدادهای امنیتی محدود شود، بلکه باید برای هر نوع رخداد، سازوکار پاسخ‌گویی مشخص و از پیش تعریف‌شده‌ای نیز داشته باشد. ازاین‌رو، لازم است رخدادهای امنیتی بر اساس میزان اهمیت و شدت آن‌ها در سطوح مختلف طبقه‌بندی شوند: اطلاع‌رسانی، قابلیت بازیابی، نقض امنیتی و دستکاری بحرانی.

۳ -۱۹- Secure Debug

در مرحله توسعه، رابط JTAG باید فعال و در دسترس باشد تا امکان اشکال‌زدایی، آزمون و عیب‌یابی تراشه فراهم شود. بااین‌حال، در مرحله تولید، این رابط باید به‌صورت امن قفل و غیرفعال شود. بنابراین، لازم است یک سازوکار امنیتی مطمئن برای موارد زیر در نظر گرفته شود:

- Manufacturing test;
- Failure analysis;
- RMA.

۳ -۲۰- DFT / Test

در این تراشه باید بخش‌های زیر طراحی شوند:

- Scan;
- MBIST;
- LBIST when required;
- SRAM BIST;
- ROM BIST;
- Crypto self-test;
- TRNG health test;
- Boundary scan;
- Production test mode;
- Secure test-mode entry;
- Lifecycle-dependent test access.

الزامی است که Secure DFT Architecture از ابتدای طراحی در معماری تست لحاظ شود. این معماری باید شامل Lifecycle-dependent access، Scan masking/exclusion برای داده‌های حساس (Security-Critical Registers) و کنترل سخت‌افزاری ورود به Test Mode باشد. صرفاً قفل‌کردن JTAG در حالت Production کافی نیست و امنیت مسیرهای DFT باید به‌صورت مستقل مورد بررسی و اثبات قرار گیرد.

۳ -۲۱- ECC و Memory Protection

برای SRAM، protected NVM، key storage، و internal buses حداقل بایدSEC-DED ECC برای حافظه‌های مهم وجود داشته باشد. برای رجیسترها نیز باید parity، duplication و consistency check در نقاط بحرانی وجود داشته باشد.

۳ -۲۲- Internal Security Bus

الزامی است که یک Security-Aware Interconnect / Hardware Firewall سخت‌افزاری جهت کنترل و فیلتر کردن دسترسی‌های CPU، Host Interface و DFT به نواحی حساس (شامل Key RAM، OTP/eFuse، Lifecycle State و Security Registers) پیاده‌سازی شود.

۳ -۲۳- TPM Firmware

Firmware باید شامل موارد زیر باشد:

- Boot ROM;
- Secure bootloader;
- TPM command dispatcher;
- TPM state manager;
- Object manager;
- Session manager;
- Authorization engine;
- Key manager;
- NV manager;
- PCR manager;
- Crypto HAL;
- Entropy manager;
- Power/reset manager;
- Fault manager;
- Firmware update manager.

۳ -۲۴- Certification Target

این تراشه باید قابل انطباق با استانداردهای زیر باشد، البته بدیهی است که اخذ گواهی‌نامه هیچیک از این استانداردها یا مراجعه به سازمان‌های خارجی الزامی نیست و تمامی آزمون‌ها و ارزیابی‌ها توسّط نهادهای ایرانی انجام خواهند شد.

- TCG TPM 2.0
  - TPM Library 2.0 Rev. 1.85;
  - TPM 2.0 PC/Server platform-specific specifications;
  - TSS compatibility.

  (آخرین Library specification رسمی TCG در حال حاضرRev. 1.85 ، مارس ۲۰۲۶ است).

- حدّاقلّ Common Criteria EAL4+ ؛ ترجیحاً EAL5+ و FIPS-140 level 3

برای TPM باید Protection Profile مربوط به PC Client Specific TPM 2.0 یا profile مناسب platformهدف را مبنا قرار دهید؛ TCG صراحتاً می‌گوید Security Target باید با PP مربوطه منطبق باشد. FIPS 140-3 بهتر است از ابتدا در architecture در نظر گرفته شود.

۳ -۲۵- Radiation Hardening By Design (RHBD)

طراحی باید مانع شود که یک وقفه یا اختلال ناشی از تشعشع مستقیماً باعث آزادسازی غیرمجاز کلید، ارتقای چرخه عمر، باز کردن اشکال‌زدایی، دور زدن سیاست امنیتی یا آسیب به وضعیت پایدار حیاتی امنیتی شود. فلذا اکیداً توصیه می‌شود که این تراشه با رویکرد Radiation-Hardening-by-Design (RHBD) طراحی شود. مجری در صورت صلاحدید می‌تواند بجای اعمال سراسری TMR یا DICE یا... به کل تراشه، جهت جلوگیری از افزایش شدید مساحت، توان و پیچیدگی Physical Design، سخت‌سازی را بر اساس Security Criticality و عمدتاً بر روی بلوک‌های حیاتی (Lifecycle، Debug Lock، Key Manager، Secure Boot، PCR، Tamper/Reset، Zeroization و State Machineهای امنیتی) انجام دهد. همچنین باید مرز مشخصی بین الزامات Fault Injection (امنیتی) و Radiation Reliability (هوافضایی) ترسیم گردد. الزامات RHBD بهتر است در موارد فوق‌الذکر، در معماری، انتخاب سلول‌ها، مدار، layout، memory architecture، clock/reset architecture، physical design، verification و qualification لحاظ شوند. اکیداً توصیه می‌شود مجری Radiation Design Specification و Radiation Design Verification Plan را در مرحله Architecture Freeze ارائه و به تأیید کارفرما برساند. اکیداً توصیه می‌شود که طراحی در موارد فوقالذکر حداقل در برابر مکانیزم‌های زیر مورد تحلیل و مقاوم‌سازی قرار گیرد:

- Total Ionizing Dose (TID)
- Single Event Upset (SEU)
- Single Event Transient (SET)
- Single Event Functional Interrupt (SEFI)
- Single Event Latchup (SEL)
- Single Event Burnout/Gate Rupture where applicable to the selected technology
- Displacement Damage (DD) where applicable.

RHBD در صورت لزوم شامل موارد زیر خواهد بود:

- radiation-aware transistor selection;
- enclosed-layout transistors (ELT) for radiation-sensitive devices;
- radiation-aware STI/layout techniques;
- guard rings and substrate isolation;
- increased spacing of radiation-sensitive devices;
- hardened standard cells for sequential and combinational logic;
- SEU-resistant flip-flops/latches;
- SET mitigation and pulse filtering;

- redundancy or error-detection/correction for security-critical state;
- TMR or equivalent fault-tolerant architecture where justified;
- hardened reset and clock-control circuits;
- radiation-aware memory architecture;
- ECC/parity/scrubbing for security-critical memories;
- protection of PCR, lifecycle, key-management and security-state registers;
- radiation-aware TRNG and entropy-source design;
- radiation-aware voltage, clock and tamper monitoring;
- fault containment and safe-state transition.

الزامات RHBD پیشنهادی به شرح زیر می‌باشند.

ردیف	حوزه	الزامات طراحی	روش / تکنیک مشخص	هدف اصلی	سطح کاربرد
1	TID	استفاده از ترانزیستورهای مناسب برای نواحی حساس	Long-L, low-leakage devices و characterization در TID	کاهش (V_{TH}) shift و leakage	Device
2	TID	محافظت transistorهای حساس در برابر STI leakage	Enclosed Layout Transistor (ELT)	کاهش TID-induced leakage	Layout
3	TID	کاهش اثرات STI	Radiation-aware STI layout، افزایش فاصله نواحی حساس از STIدر صورت امکان	کاهش parasitic leakage	Layout
4	TID	کنترل substrate/well potential	افزایش well/substrate taps	کاهش leakage و parasitic effects	Layout
5	TID/SEL	جلوگیری از parasitic conduction	P+/N+ guard rings	کاهش leakage و latch-up susceptibility	Layout
6	TID	استفاده از افزاره های با رفتار مشخص‌شده پس از تابش	Characterized transistor library	پیش‌بینی degradation	PDK/Library
7	TID	جلوگیری از عملکرد در شرایط	UVLO / Brownout detector	جلوگیری از malfunction در افت تغذیه	Circuit

ردیف	حوزه	الزامات طراحی	روش / تکنیک مشخص	هدف اصلی	سطح کاربرد
		خارج از مشخصات			
8	TID	پایش تغییرات تغذیه	Voltage monitor	تشخیص degradation/fault	Circuit
9	SEU	مقاوم‌سازی Flip-Flopهای بحرانی	DICE / RHBD Flip-Flop	جلوگیری از single-node upset	Standard Cell
10	SEU	مقاوم‌سازی stateهای بسیار بحرانی	TMR Flip-Flop + Majority Voter	یکmasking upset	Sequential
11	SEU	مقاوم‌سازی registerهای configuration	TMR یا ECC + periodic refresh	جلوگیری از تغییر configuration	Digital
12	SEU	مقاوم‌سازی FSMهای بحرانی	TMR / state encodingمقاوم به خطا	جلوگیری از خروج FSMاز حالت معتبر	RTL
13	SEU	جلوگیری از propagation خطا	Fault containment boundaries	محدود کردن دامنهfault	Architecture
14	SRAM	تصحیح خطای حافظه	SEC-DED ECC حداقل	تصحیح-single bit error	Memory
15	SRAM	مقابله با-multi bit upset	DICE / RHBD SRAM cell	افزایش SEU tolerance	Memory Cell
16	SRAM	جلوگیری از چندبیتی شدن یک ECC word	Physical bit interleaving	کاهشMBU	Layout
17	SRAM	بازیابی خطاهای تجمعی	Memory scrubbing	پاک‌سازی خطاهای اصلاح‌شده	Architecture
18	SRAM	تشخیص خطای حافظه	ECC error counter/status	پایش-radiation induced errors	Digital
19	SET	کاهش انتشار transient	Pulse quenching	سرکوب SET در گره حساس	Circuit
20	SET	حذف پالس‌های بسیار کوتاه	Temporal filtering	جلوگیری از ثبت transient	Circuit

ردیف	حوزه	الزامات طراحی	روش / تکنیک مشخص	هدف اصلی	سطح کاربرد
21	SET	مقاوم‌سازی مسیرهای منطقی بحرانی	Redundant logic paths	افزایش SET tolerance	RTL/Cell
22	SET	جلوگیری از تغییر خروجی در اثر یک مسیر	Muller C-element در نقاط مناسب	Consensus / transient masking	Circuit
23	SET/SEU	جلوگیری از ثبت SET	Hardened sampling FF	جلوگیری از تبدیل SETبهSEU	Sequential
24	SET	افزایش charge لازم برای تغییر node	افزایش capacitance گره‌های بحرانی	افزایش critical charge (Q_{crit})	Device/Layout
25	SEE	جداسازی مسیرهای redundant	Spatial separation	کاهش simultaneous upset	Layout
26	SEE	جلوگیری از couplingبین nodeهای حساس	افزایش physical spacing	کاهش charge sharing	Layout
27	SEL	جلوگیری از latch-up	Guard ring + dense well/substrate contacts	کاهش parasitic SCR	Layout
28	SEL	کاهش مدت latch-up	Current limiter	محدودکردن (I_{DD})	Power
29	SEL	قطع domain معیوب	Power switch controlled by fault monitor	جلوگیری از آسیب دائمی	Power
30	SEL	تشخیص افزایش غیرعادی جریان	Fast over-current detector	تشخیصSEL	Power
31	SEL	جلوگیری از propagation fault	Power-domain isolation	محدود کردن fault	Architecture
32	Clock	مقاوم‌سازی clock source	Radiation-tolerant PLL/oscillator	جلوگیری از clock failure	Analog
33	Clock	تشخیص خرابی PLL	Lock detector	تشخیص-loss-of lock	Analog/Digital
34	Clock	کنترل صحت فرکانس	Frequency monitor	تشخیص clock anomaly	Digital

ردیف	حوزه	الزامات طراحی	روش / تکنیک مشخص	هدف اصلی	سطح کاربرد
35	Clock	جلوگیری از glitch	Hardened clock gating / glitch filtering	جلوگیری از clock-induced upset	Clock
36	Clock	افزایش availability	Redundant clock source	ادامه کار پس از failure	Architecture
37	Clock/CDC	جلوگیری از انتشار خطا بین domainها	Clock-domain isolation	fault containment	Architecture
38	CDC	جلوگیری از metastability	Radiation-aware synchronizer	کاهش خطای clock crossing	Digital
39	Reset	جلوگیری از resetناخواسته	Reset glitch filter	جلوگیری از SET-induced reset	Circuit
40	Reset	مقاوم‌سازی reset state	Hardened reset synchronizer	جلوگیری از reset corruption	Digital
41	Reset	recoveryاز malfunction	Independent watchdog reset	بازیابی سیستم	Architecture
42	Control	تشخیص malfunction پردازنده	Watchdog timer	تشخیص توقف/loop	System
43	Control	تشخیص خطای منطقی	Parity / CRC	تشخیص corruption	Digital
44	Control	ادامه کار پس از خطای transient	Fault detection + recovery controller	autonomous recovery	Architecture
45	Control	محدودکردن fault propagation	Fault containment region	جلوگیری از خرابی کلSoC	Architecture
46	Power	تنظیمrail های حساس	Radiation-aware LDO	تأمین تغذیه پایدار	Analog
47	Power	حفاظت در برابر افت ولتاژ	UVLO	جلوگیری از brownout malfunction	Power
48	Power	حفاظت اضافه‌ولتاژ	OVP	جلوگیری از electrical overstress	Power
49	Power	حفاظت اضافه‌جریان	OCP	محدودکردن fault current	Power

ردیف	حوزه	الزامات طراحی	روش / تکنیک مشخص	هدف اصلی	سطح کاربرد
50	Power	تفکیک تغذیه بلوک‌ها	Independent power domains	fault containment	Architecture
51	Power	جلوگیری از propagation domain از خاموش	Isolation cells	ایزوله‌کردن domain	Physical/RTL
52	Analog	مقاوم‌سازی reference	Radiation-aware bandgap/reference	کاهش drift	Analog
53	Analog	مقاوم‌سازی ADC	Redundancy / calibration / error detection	حفظ accuracy پس از TID	Analog
54	Analog	مقاوم‌سازی DAC	Redundant/reference monitoring	کاهش radiation-induced error	Analog
55	Analog	مقاوم‌سازی PLL	Hardened charge pump + monitoring	SET/TID tolerance	Analog
56	I/O	مقاوم‌سازی I/Oهای حساس	Radiation-tolerant input/output cells	کاهش SEE/TID effects	I/O
57	I/O	ارتباط differential مقاوم	Radiation-aware LVDS PHY	حفظ link integrity	PHY
58	Communication	تشخیص خطای packet	CRC	تشخیص corruption	Protocol
59	Communication	تصحیح خطای link	FECدر صورت نیاز	اصلاح bit errors	Communication
60	Communication	ادامه ارتباط پس از خطا	Link reset/recovery	افزایش availability	Protocol
61	Security	مقاوم‌سازی secure state	TMR/ECC security برای registers	جلوگیری از تغییر stateامنیتی	Security
62	Security	محافظت memory کلیدها	ECC + redundancy	جلوگیری از corruptionکلید	Security
63	Security	مقاوم‌سازی TRNG/PUF	health monitor + redundancy	حفظ entropy/security	Security

ردیف	حوزه	الزامات طراحی	روش / تکنیک مشخص	هدف اصلی	سطح کاربرد
64	Security	محافظتdebug	Hardened secure-debug controller	جلوگیری از fault-induced debug entry	Security
65	Physical	جداسازی سلول‌های redundant	Spatial separation	کاهش MBU/common-event failure	Layout
66	Physical	جداسازی مسیرهای redundant	Separate routing	کاهش simultaneous SET	Layout
67	Physical	کاهش coupling	Shielding / spacing در net های بحرانی	کاهش transient propagation	Layout
68	Physical	افزایش substrate control	Dense substrate/well contacts	کاهش parasitic effects	Layout
69	Physical	کنترل critical nodes	Critical-node identification و special layout	کاهش SET/SEU sensitivity	Layout
70	DFT	تستSRAM	MBIST + ECC injection test	verification خطا	DFT
71	DFT	تستlogic	LBIST / fault injection	verification RHBD	DFT
72	DFT	تستSEU	SEU fault injection	بررسیrecovery	Verification
73	DFT	تستSET	Transient injection	اندازه‌گیری SET propagation	Verification
74	Verification	شبیه‌سازی radiation faults	RTL/gate-level fault injection	اثبات fault tolerance	Verification
75	Verification	تحلیل critical charge	(Q_{crit}) extraction	تعیین SET/SEU susceptibility	Device
76	Verification	تحلیلTID	Pre/post-TID SPICE characterization	تعیین degradation	Device/Circuit
77	Verification	تستSEL	Heavy-ion/proton SEL test	اثبات عدم destructive latch-up	Qualification
78	Verification	تستSEU	Heavy-ion/proton irradiation	اندازه‌گیری SEU cross-section	Qualification
79	Verification	تستSET	Heavy-ion/laser transient testing	تعیین SET sensitivity	Qualification

ردیف	حوزه	الزامات طراحی	روش / تکنیک مشخص	هدف اصلی	سطح کاربرد
80	Verification	تستTID	Co-60/X-ray irradiation	تعیینTID limit	Qualification
81	Qualification	تست ترکیبی	Radiation + temperature + voltage corners	ارزیابی-worst case	Qualification
82	System	تعریف recovery strategy	Reset/reconfigure/restart	بازیابی autonomous	Architecture
83	System	ذخیره وضعیت معتبر	Checkpoint / redundant state	recoveryپس از fault	Architecture
84	System	کنترل سلامت تراشه	Telemetry/error counters	پایش-radiation induced faults	System
85	System	حالت امن	Fail-safe state machine	جلوگیری از رفتار خطرناک	Architecture

تیم طراحی توصیه می‌شود که تمام سلول‌های استاندارد حساس به تابش که در مسیرهای حیاتی امنیتی استفاده می‌شوند را شناسایی کند و در صورت نیاز از جایگزین‌های مقاوم یا مشخص‌شده در برابر تابش استفاده کند. تیم طراحی باید یک ماتریس استفاده از RHBD در سطح سلول ارائه دهد که آسیب‌پذیری در برابر تابش، تکنیک کاهش، سلول کتابخانه‌ای، و شواهد تأیید برای هر سلول حیاتی را مشخص کند.

Security-critical SRAM باید در صورت لزوم از ECC نوع SEC-DED یا قوی‌تر استفاده کند، و در جایی که منطقی باشد از تکثیر حالت محافظت‌شده یا افزونگی بهره ببرد، و مکانیزم‌هایی برای پاکسازی/بازیابی حافظه در برابر اختلالات ناشی از تابش داشته باشد. RAM کلیدی همچنین باید پاک‌سازی سریع در صورت بروز خطا را فراهم کند و نباید فقط به ECC برای محافظت امنیتی تکیه کند.

منبع آنتروپی و مدارهای تست سلامت TRNG باید تحت تابش اشعه بررسی شوند و کاهش آنتروپی ناشی از تابش را تشخیص دهند. خرابی TRNG ناشی از تابش باید منجر به رفتار بسته‌شده شود و نباید به‌طور خاموش خروجی رمزنگاری تولید کند.

محیط تابش پایه محیط زمینی با ارتفاع بالا / محیط هوافضا است؛ البتّه نیازهای نهایی تابش در زمان تثبیت معماری بر اساس محیط استقرار مورد نظر تعیین خواهند شد.

بلوک	اهمّیّت RHBD
Root of Trust	بسیار بالا
Lifecycle Controller	بسیار بالا
Key Manager	بسیار بالا

Zeroization Controller	بسیار بالا
Secure Boot	بسیار بالا
PCR	بسیار بالا
Authorization Engine	بسیار بالا
Debug Controller	بسیار بالا
Tamper Controller	بسیار بالا
Reset Controller	بسیار بالا
Clock Monitor	بسیار بالا
TRNG	بسیار بالا
SRAM Crypto RAM	بالا
Secure Key RAM	بسیار بالا
PQC engines	بالا
CPU	متوسط/بالا
Host SPI	متوسط
غیرامنیتیlogic	معمولی

۴- پروفایل حافظتی و اهداف امنیتی

۴ -۱ -پروفایل حفاظتی پیشنهادی

۴-۱-۱- عنوان

Project Security Profile – Discrete TPM 2.0

عنوان پیشنهادی:

Generic Discrete Trusted Platform Module 2.0 Protection Profile for Server, PC Client, Industrial Computer and Network Appliance

شناسه پیشنهادی: GTPM2-PSP v1.0

نسخه فعلی TPM 2.0 Library که باید baseline پروژه قرار گیرد، Version 185 / March 2026 است.

۴-۱-۲- دامنه PP

TOE یک Discrete TPM 2.0 IC است که به‌صورت یک تراشه مستقل روی پلت‌فرم نصب می‌شود.

چهار پلت‌فرم مورد نظر عبارت‌اند از:

- Enterprise Server;
- PC Client;
- Industrial Computer;
- Network Appliance.

Host OS، BIOS/UEFI، hypervisor و application software خارج از TOE هستند، مگر در مواردی که برای security functionality مشخصاً به‌عنوان external entity تعریف شوند.

۴-۱-۳- Security Problem Definition

داراییهای امنیتی به شرح جدول زیر هستند.

Asset	شرح
AK	Attestation Keys
EK	Endorsement Key
SRK	Storage Root Key
SK	Other secret keys
NV	TPM NV data
PCR	Platform measurements
TPM-State	Internal TPM state
Firmware	TPM Firmware
Boot-ROM	Root of Trust
Random	entropy/random data
Sessions	authorization/session state
Platform-Identity	Platform identity information
Audit/Events	security-relevant state

۴-۱-۴- تهدیدهای اصلی

برای این محصول حداقل تهدیدهای زیر مدّنظر هستند:

- T.PHYSICAL

مهاجم با دسترسی فیزیکی به تراشه تلاش می‌کند secret key استخراج کند؛ حافظه را دستکاری کند؛ clock/voltage glitch ایجاد کند؛ fault injection انجام دهد؛ debug interface را فعال کند؛ و یا Firmware را تغییر دهد.

- T.KEY_DISCLOSURE

مهاجم تلاش می‌کند EK، AK، SRK یا سایرprivate key ها را استخراج کند.

- T.UNAUTHORIZED_COMMAND

مهاجم از host تلاش می‌کند TPM command غیرمجاز اجرا کند.

- T.COMMAND_MANIPULATION

مهاجم command/response را روی رابط host دستکاری می‌کند.

- T.NV_MANIPULATION

مهاجم تلاش می‌کند NV index را تغییر دهد؛ counterرا rollback کند؛ policy را دور بزند؛ و یا NV data را corrupt کند.

- T.PCR_MANIPULATION

مهاجم تلاش می‌کند PCR measurementها را تغییر دهد؛ reset غیرمجاز کند؛ replay کند؛ و یا bypass کند.

- T.FIRMWARE_MODIFICATION

مهاجم تلاش می‌کند Firmware TPM را تغییر دهد؛ Firmware مخرب نصب کند؛ و یا Firmware قدیمی را نصب کند.

- T.ROLLBACK

مهاجم Firmware قدیمی ولی معتبر را نصب می‌کند تا vulnerability قدیمی را exploit کند.

- T.RNG_FAILURE

مهاجم یا fault باعث تولید random number غیرقابل اعتماد می‌شود.

- T.FAULT_INJECTION

مهاجم با voltage glitch، clock glitch، EM fault، temperature manipulation، و یا reset manipulation اجرای TPM را منحرف می‌کند.

- T.DEBUG

مهاجم تلاش می‌کند از JTAG، debug port، و یا test mode برای دسترسی به secret استفاده کند.

- T.DOS

مهاجم تلاش می‌کند TPM را با commandهای malformed یا excessive به وضعیت غیرقابل استفاده ببرد. Availability باید محافظت شود، ولی TPM الزاماً نباید در برابر DoS ناشی از خاموش‌کردن کامل host تضمین بدهد.

۵-۱-۴- فرضیات محیط عملیاتی

- A.PLATFORM_SECURITY

فرض می‌شود platform دارای حداقل سطحی از امنیت Firmware/boot است.

- A.PHYSICAL_ACCESS

در threat model باید فرض کنیم مهاجم می‌تواند به خود platform دسترسی فیزیکی پیدا کند؛ بنابراین TOE نباید صرفاً بر «محیط فیزیکی امن» متکی باشد.

- A.HOST_INTERFACE

HOST ممکن است malicious یا compromised باشد. این نکته برای TPM بسیار مهم است. TPM نباید به host اعتماد کند.

- A.POWER

پلت‌فرم شرایط تغذیه‌ای خارج از محدوده specification را عمداً اعمال نمی‌کند، ولی TPM باید در برابر glitchهای قابل انتظار مقاوم باشد.

- A.UPDATE_AUTHORITY

Firmware update فقط توسط entity مجاز انجام می‌شود.

۴-۱-۶ Security Objectives for TOE

TOE باید اهداف زیر را داشته باشد.

Objective	هدف
O.SECURE_BOOT	اجرای Firmware معتبر
O.KEY_PROTECTION	حفاظت از کلیدها
O.RNG	تولید entropy امن
O.PCR	حفاظت از PCR
O.NV	حفاظت از NV storage
O.AUTH	احراز هویت و authorization
O.ATTEST	Attestation امن
O.CRYPT	عملیات cryptographic صحیح
O.TAMPER	تشخیص tamper/fault
O.DEBUG	جلوگیری از debug غیرمجاز
O.UPDATE	Firmware update امن
O.ANTIROLLBACK	جلوگیری ازrollback
O.ISOLATION	جداسازی secretها
O.RATE_LIMIT	جلوگیری ازabuse
O.RECOVERY	recovery امن
O.FAIL_SECURE	ورود به حالت امن در fault بحرانی

۴-۱-۷ Security Objectives for Environment

پلت‌فرم باید Firmware معتبر اجرا کند؛ BIOS/UEFI measurement را انجام دهد؛ event log صحیح ایجاد کند؛ TPM را در برابر removal غیرمجاز محافظت کند؛ update authorization را مدیریت کند؛ interface را مطابق TCG استفاده کند.

۴-۱-۸- SFRهای پیشنهادی

Security Audit
FAU_GEN.1

تولید security-relevant events برای:

- Startup;
- Shutdown;
- Failed authorization;
- NV access;
- Key operation failure;
- Self-test failure;
- Tamper;
- Firmware update;
- Rollback rejection.

۴-۱-۹- Cryptographic Support

FCS_CKM

مدیریت lifecycle کلید:

- Generation;
- Derivation;
- Loading;
- Use;
- Destruction.

FCS_COP

عملیات:

- AES;
- SHA;
- HMAC;
- RSA;
- ECC;
- KDF;
- Signature verification.

مطابق Algorithm Registry و TPM Library انتخاب شوند.

۴-۱-۱۰- Identification and Authentication

FIA_UID

شناسایی entity ها.

FIA_UAU

احراز هویت:

- Authorization value;
- Password/session authorization;
- Policy authorization;
- Hierarchy authorization;

۴-۱-۱۱- User Data Protection

FDP_ACC

کنترل دسترسی به:

- NV;
- Keys;
- PCR;
- TPM objects;
- Hierarchy objects.

FDP_ACF

اجرایpolicy های access control.

۴-۱-۱۲- Security Management

FMT_MOF

مدیریت security functions.

FMT_MSA

مدیریت security attributes.

FMT_MTD

مدیریت:

- NV indices;
- Hierarchy state;
- PCR policy;
- Authorization data.

۴-۱-۱۳- Protection of TOE Security Functions

FPT_FLS
Fail Secure

در faultهای مهم باید Detection و رفتن به Secure State و Zeroization / Reset / Lock انجام شود.

FPT_TST

Self-test:

- CPU;
- ROM;

- RAM;
- Crypto;
- TRNG;
- NVM;
- Firmware integrity.

FPT_RCV

Recovery:

- Interrupted update;
- Corrupted state;
- Power failure;
- Failed boot.

FPT_PHP

Physical protection:

- Voltage;
- Clock;
- Temperature;
- Glitch;
- Physical tamper.

TOE Access -۴-۱-۱۴

FTA_SSL

Session/command timeout.

FTA_TSE

TSF-mediated execution. TPM باید قبل از اجرای commandهای sensitive بررسی کند که آیا command allowed، hierarchy allowed، authorization valid، object valid، locality valid، state valid؟

Trusted Path / Channel -۴-۱-۱۵

برای رابط host:

FTP_ITC

در صورت استفاده از secure transport.

TOE Security Functions -۴-۱-۱۶

TSF architecture برای این تراشه را پیشنهاد می‌شود:

- TSF-01 Secure Boot;
- TSF-02 TPM Command Processor;
- TSF-03 Authorization Manager;
- TSF-04 Key Manager;

- TSF-05 Crypto Engine includes: Classical Cryptographic Engine, PQC KEM Engine, PQC Signature Engine, Hybrid Cryptographic Combiner, KDF Engine, Cryptographic Policy Engine, and Crypto-Agility Controller;
- TSF-06 TRNG/DRBG;
- TSF-07 PCR Manager;
- TSF-08 NV Manager;
- TSF-09 Attestation Engine;
- TSF-10 Firmware Update Manager;
- TSF-11 Anti-Rollback;
- TSF-12 Tamper/Fault Manager;
- TSF-13 Secure Debug Manager;
- TSF-14 Lifecycle Manager;
- TSF-15 Self-Test Manager;
- TSF-16 Secure Reset/Recovery;
- TSF-17 PQC Key Management Engine;
- TSF-18 Hybrid Cryptography Controller.

۴ -۲- Security Target

عنوان پیشنهادی: GTPM2-100 Security Target

TOE :GTPM2-100 Discrete TPM 2.0

Hardware: 40 nm Si CMOS
Firmware: TPM Firmware + secure bootloader
Interface: SPI

Platform: Server ،PC ،Industrial Computer ،Network Appliance

۱-۲-۴- Security Functional Requirements در ST

Recommended target

+EAL4 با:

- ALC_DVS.2;
- ALC_FLR.2;
- AVA_VAN.4.

و ترجیحاً:

EAL5+ / AVA_VAN.5 و FIPS-140 level 3

۲-۲-۴- Security Claims اصلی ST

در سند ST باید موارد زیر اثبات شوند:

- ☐ SC-01 — Secure Boot

TPM فقط Firmware authentic و integrity-verified را اجرا می‌کند.

- ☐ SC-02 — Key Confidentiality

Private key material هرگز از TOE خارج نمی‌شود.

- SC-03 — PCR Integrity

PCRها فقط از مسیرهای مجاز TPM تغییر می‌کنند.

- SC-04 — NV Integrity

NV data در برابر unauthorized modification و rollback محافظت می‌شود.

- SC-05 — Attestation

Quote فقط با AK معتبر ایجاد می‌شود وPCR های واقعی TOE را منعکس می‌کند.

- SC-06 — RNG

Randomness مورد استفاده برای key generation از trusted entropy source تأمین می‌شود.

- SC-07 — Host Isolation

Compromise شدن host به‌تنهایی نباید موجب استخراج secretهای TPM شود.

- SC-08 — Firmware Update

فقط Firmware دارای signature معتبر و version مجاز پذیرفته می‌شود.

- SC-09 — Physical Attack Resistance

TOE در برابر حملات physical مشخص‌شده در attack potential مربوط به سطح assurance مقاومت می‌کند.

- SC-10 — Debug Protection

Production debug/test interface نمی‌تواند به‌secret ها دسترسی پیدا کند.

- SC-11 — PQC Security

TOE shall provide hardware-backed NIST Security Category 5 post-quantum cryptographic services including ML-KEM-1024, HQC-256, ML-DSA-87 and SLH-DSA Category-5 parameter sets.

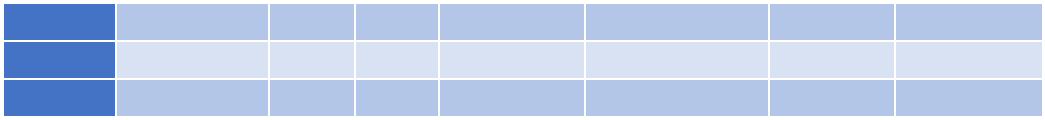
- SC-12 — Heterogeneous Hybrid Security

TOE باید از عملیات‌های رمزنگاری ترکیبی پشتیبانی کند که در آنها دو الگوریتم مستقل پساکوانتومی، مبتنی بر فرضیات ریاضی متفاوت درباره سختی محاسباتی، به‌صورت مشترک مورد استفاده قرار می‌گیرند؛ به‌نحوی که حتی در صورت شکسته‌شدن یا به خطر افتادن هر یک از الگوریتم‌ها، این امر به‌تنهایی نتواند موجب افشای راز نهایی ترکیبی یا بی‌اعتبار شدن سیاست امنیتی رمزنگاری ترکیبی شود.

۳-۲-۴- Threat، Objective ، SFR

مجری موظف است یک Security Traceability Matrix کامل ارائه کند که برای هر Threat، Security Objective، SFR، TSF، hardware/Firmware implementation، verification method و test case شناسه یکتا تعیین کند. این جدول باید دارای ستونهای زیر باشد:

Threat	Objective	SFR	TSF	RTL/FW	Verification	Test ID	Evidence



۴-۲-۴- در PP، Host را trusted فرض نکنید.

یعنی در صورت Server compromise و Attacker controls OS و Attacker controls TPM و driver و Attacker sends malicious TPM commands باید TPM امن باقی بماند. اما در صورت Attacker owns entire motherboard و replaces TPM و changes power rails و physically removes chip دیگر مسئله باید در physical attack model وplatform assumptions دقیقاً مرزبندی شود.

۵- روش اجرای طرح

طرح باید در فرآیند mixed signal نود فناوری ۴۰ نانومتر اجرا شود. در همین راستا، فایل‌ها و اسناد لازم شامل PDK فناوری مذکور، توسط مرکز ملی پیشران طراحی تراشه در اختیار مجری قرار خواهد گرفت و پشتیبانی‌های فنی و نرم‌افزاری از تیم مجری به عمل خواهد آمد. پس از اتمام طراحی، فایل‌های GDSII مربوطه توسط مرکز ملی پیشران طراحی تراشه و با حمایت برنامه ملی میکروالکترونیک، برای ساخت (Tape Out) به کارخانهٔ تولید کنندهٔ تراشه (Foundry) ارسال خواهد شد و مجری نیازی به تعامل شخصی با Foundry نخواهد داشت. تعامل رسمی و اجرایی با Foundry توسط کارفرما/مرکز مجری انجام خواهد شد؛ لیکن مجری طراحی موظف است کلیه technical queries، DRC/LVS waivers، process-specific constraints، tape-out checklist و sign-off documentation موردنیاز Foundry را تهیه و در فرآیند tape-out پشتیبانی کند. پس از ساخت تراشه، عملیات باندینگ توسط مرکز ملی پیشران طراحی تراشه و در نهایت تست و ارزیابی آن مشترکاً توسط مجری و مرکز ملی پیشران طراحی تراشه انجام خواهد گردید.

ارزیابی طرح‌های ارسالی پیمانکاران در دو مرحله انجام شود: مرحله اوّل بررسی جامعیّت معماری و تطابق با نیازمندی‌های امنیتی (Conceptual)، و مرحله دوم ارزیابی فنی امکان‌پذیری پیاده‌سازی و دفاع‌پذیری طرح از منظر PPA Feasibility. نظارت بر اجرای طرح نیز به‌صورت لایه‌ای و مرحله‌ای (Gate Review) انجام خواهد شد.

۶- خروجی‌ها و موارد تحویلی مورد انتظار

۶ -۱ -معماری و مشخصات فنی

گروه طراحی باید ابتدا این اسناد را تحویل دهد:

- System Specification;
- Hardware Security Architecture;
- TPM 2.0 Architecture;
- Block Diagram;
- IP Catalog;
- Memory Map;
- Register Map;
- Clock Architecture;
- Reset Architecture;
- Power Architecture;
- Security Boundary / TOE Boundary;
- Threat Model;
- Security Requirements Traceability.

مخصوصاً باید مشخص باشد هر درخواست از PP/ST دقیقاً در کدام hardware یا Firmware پیاده‌سازی شده است.

۶ -۲- RTL کامل

- Complete SystemVerilog/Verilog RTL;
- synthesizable RTL;
- All internal IPs;
- top-level RTL;
- Wrappers;
- Clock/reset logic;
- Security logic;
- Test logic;
- Memory controllers;
- Crypto accelerators: Includes: AES Accelerator, SHA/HMAC Accelerator, RSA Accelerator, ECC Accelerator, ML-KEM-1024 Hardware Accelerator, HQC-256 Hardware Accelerator, ML-DSA-87 Hardware Accelerator, SLH-DSA Category-5 Accelerator, PQC KDF/Combiner, Hybrid Cryptography Controller, PQC Key Manager, and PQC Zeroization Controller. ML-KEM-1024 and HQC-256 shall be implemented as independent cryptographic datapaths. The use of a single shared datapath in which the second algorithm is executed through software emulation is not acceptable for satisfying this requirement.
- TPM command engine;
- Key manager;
- PCR;
- NV controller;
- TRNG;
- Secure boot;
- Lifecycle controller;
- Tamper controller;
- RTL source;
- RTL hierarchy;
- Parameter files;
- Package files;
- Include files;

- Compile scripts;
- Lint scripts;
- Synthesis scripts.

۶ -۳ - IPهای شخص ثالث

برای هر IP باید موارد زیر تحویل شوند:

- IP name;
- Vendor;
- Version;
- License;
- Source availability;
- Modification rights;
- Foundry permission;
- OSAT permission;
- Redistribution rights;
- Security restrictions;
- Known vulnerabilities;
- Verification status;
- PDK compatibility.

خصوصاً مشخص کنید: آیا شما مالک دائمی RTL هستید یا فقط license استفاده دارید؟

۶ -۴ - Verification Package

Verification Environment

- UVM testbench;
- Testbench RTL;
- BFMs;
- Bus models;
- Memory models;
- Crypto reference models;
- Tpm host model;
- Firmware model;

Test

- Directed tests;
- Constrained-random tests;
- Regression tests;
- Corner-case tests;
- Negative tests;
- Security tests;
- Fault tests;
- Reset tests;
- Power-loss tests;
- ML-KEM-1024 KAT;

- HQC-256 KAT;
- ML-DSA-87 KAT;
- SLH-DSA-256f KAT;
- PQC key-generation tests;
- PQC encapsulation/decapsulation tests;
- PQC signing/verification tests;
- Hybrid KEM interoperability tests;
- Hybrid signature tests;
- Negative hybrid tests;
- Algorithm downgrade tests;
- Constituent-algorithm failure tests;
- Intermediate-secret zeroization tests;
- Simultaneous execution tests;
- Independent-engine isolation tests;
- Fault injection against each PQC engine;
- Side-channel tests against each PQC engine;

Functional Verification - ۵- ۶

- Code coverage;
- Functional coverage;
- Assertion coverage;
- FSM coverage;
- Branch coverage;
- Toggle coverage;
- Reproducible Coverage Report.

Formal Verification - ۶- ۶

Security-critical blocks

- Key Manager;
- Authorization Engine;
- Access Control;
- NV Controller;
- Secure Boot Controller;
- Lifecycle Controller;
- Debug Lock;
- Zeroization;
- PCR logic;
- Tamper FSM;
- Properties;
- Assertions;
- Formal testbench;

- Formal scripts;
- Proof reports;
- Unreachable-state analysis.

مثلاً باید بتوانید اثبات کنید که Host هیچ مسیر قانونی برای خواندن private key ندارد، یا Debug unlock در production lifecycle قابل فعال‌سازی نیست. ویژگی‌های امنیتی اصلی باید از ابتدای توسعه RTL دارای Assertion و Formal Property باشند و فرآیند Formal Verification به انتهای فرآیند طراحی موکول نشود.

۶ -۷- Synthesis + Physical Design

Synthesis
- Synthesis RTL;
- Constraints;
- SDC;
- Synthesis scripts;
- Timing reports;
- گزارش مساحت (Area Report): گزارش تفصیلی مساحت مربوط به بخش‌های PQC باید مساحت هر یک از موارد زیر را به‌صورت جداگانه ارائه کند: مساحت شتاب‌دهنده ML-KEM-1024، مساحت شتاب‌دهنده HQC-256، مساحت شتاب‌دهنده ML-DSA-87، مساحت شتاب‌دهنده SLH-DSA، مساحت حافظه RAM مربوط به PQC، مساحت ترکیب‌کننده Hybrid / واحد KDF، مساحت حافظه ذخیره‌سازی کلیدهای PQC، مساحت سربار ناشی از مسیریابی و ایزولاسیون امنیتی، مجموع مساحت بخش‌های PQC، مجموع مساحت کل تراشه (Die). گزارش‌ها باید در سه مرحله ارائه شوند: پس از سنتز RTL، پس از جایگذاری (Post-Placement)، پس از مسیریابی نهایی (Post-Route).
- Power report;
- Gate-level netlist.

Physical Design
- Floorplan;
- power plan;
- placement;
- CTS;
- Routing;
- DRC;
- LVS;
- Antenna;
- IR drop;
- EM;
- Crosstalk;
- Signal integrity.

۶ -۸- Tape-out Package

- GDSII / OASIS;

- GDS/OASIS;
- Final netlist;
- LEF/DEF;
- CDL;
- LVS deck;
- DRC deck;
- Layer map;
- Stream-out configuration;
- Timing files;
- Parasitic files;
- Tape-out checklist.

Final Sign-off Report

- DRC;
- LVS;
- ERC;
- Antenna;
- STA;
- IR drop;
- EM;
- Density;
- Metal fill;
- Reliability checks.

۶ -۹ - فایل‌های لازم برای Fab

گروه طراحی باید یک Foundry Submission Package آماده کند:

- GDS/OASIS;
- Netlist;
- CDL;
- Layer map;
- Waiver list;
- DRC/LVS reports;
- Seal-ring specification;
- Pad-ring specification;
- Bonding diagram;
- Die-size;
- Die orientation;
- Scribe-line;
- Process corner reports;

و مهم‌تر، Final Tape-out Release Checklist که توسط مدیر فنی گروه طراحی امضا شده باشد.

۶ -۱۰ - Package/OSAT Documentation

تیم طراحی باید اطلاعات لازم برای packaging را نیز تحویل دهد:

Package

- Package recommendation;

- Die dimensions;
- Die thickness;
- Pad coordinates;
- Pad size;
- Pad pitch;
- Bond-wire constraints;
- Bump information for flip-chip packaging;
- Die attach requirements;
- Maximum temperature;
- Package thermal requirements.

Bonding

مثلاً:

Pad 1 → SPI_CLK;
Pad 2 → SPI_MOSI;
Pad 3 → SPI_MISO.
...

به‌همراه:

- Bonding diagram;
- Wire-bond map;
- Pad electrical characteristics;
- ESD requirements.

۶ -۱۱- Firmware

باید Firmware کامل تحویل شود:

- Boot ROM source;
- TPM Firmware source;
- Secure bootloader;
- Secure bootloader;
- Update Firmware;
- Recovery Firmware;
- Manufacturing Firmware;
- Test Firmware;
- Source code;
- Build environment;
- Compiler version;
- Linker scripts;
- Libraries;
- Configuration files;
- Signing tools;
- PQC Crypto API;
- ML-KEM API;
- HQC API;
- ML-DSA API;
- SLH-DSA API;
- Hybrid KEM API;
- Hybrid Signature API;
- PQC key-management API;

- PQC algorithm-policy API;
- PQC KAT/self-test Firmware;
- PQC migration/algorithm-agility framework;

Firmware باید موتورهای رمزنگاری PQC را از طریق یک لایه انتزاع سخت‌افزاری (HAL) پایدار در اختیار نرم‌افزار قرار دهد و نباید به برنامه‌های کاربردی یا نرم‌افزار میزبان اجازه دهد سیاست امنیتی سخت‌افزار را دور بزنند. کلید signing مربوط به production نباید در اختیار گروه طراحی باقی بماند و فرآیند key ceremony باید تحت کنترل کارفرما خواهد بود.

۶ -۱۲- Manufacturing Test Package

گروه طراحی باید تولید کند:

DFT
- Scan chain;
- MBIST;
- boundary scan;
- JTAG;
- ATPG;
- test modes;

Test vectors
- Wafer test vectors;
- Final test vectors;
- Structural test;
- Functional test;
- Memory test;
- Crypto test;
- TRNG test.

Production Test Specification

باید دقیقاً مشخص شود که چگونه تشخیص داده خواهد شد که یک die سالم است.

۶ -۱۳- ATE Program

ATE program باید برای ATE platform مورد توافق کارفرما ارائه شود. در صورت مشخص نبودن مدل ATE در زمان RFP، مجری باید test vectors و machine-independent test specification را تحویل دهد و پس از تعیین ATE، program قابل اجرا تولید کند.ATE test program شامل موارد زیر خواهد بود:
- Pin configuration;
- Test sequence;
- Voltage;
- Frequency;
- Timing;
- Limits;
- Pass/fail criteria;
- Binning.

و برای wafer: Wafer Sort Program

۶ -۱۴- Silicon Bring-up Package

TPM Evaluation Board

- SPI;
- Power rails;
- Reset;
- Debug;
- Test headers;
- Logic analyzer access;
- Current measurement;
- Clock measurement.

۶ -۱۵- Silicon Validation Software

- Register-level test software;
- TPM command test suite;
- Host driver;
- Linux driver integration;
- Windows integration if targeted;
- Firmware update utility;
- Manufacturing provisioning software;
- Diagnostic software.

و برای هر TPM command: حداقل یک test case مثبت و چند negative test.

۶ -۱۶- TPM 2.0 Compliance Package

TPM 2.0 Compliance Matrix

مثلاً:

TPM Requirement	Implementation	RTL/FW	Test
TPM2_Startup	Startup Manager	FW	TST-001
TPM2_PCR_Extend	PCR Engine	HW/FW	TST-023
TPM2_Quote	Attestation Engine	HW/FW	TST-041
TPM2_NV_Write	NV Controller	HW/FW	TST-067

و

Requirement	Implementation	Test
ML-KEM-1024 KeyGen	HW/FW	PQC-KEM-001
ML-KEM-1024 Encaps	HW/FW	PQC-KEM-002
ML-KEM-1024 Decaps	HW/FW	PQC-KEM-003

HQC-256 KeyGen	HW/FW	PQC-KEM-004
HQC-256 Encaps	HW/FW	PQC-KEM-005
HQC-256 Decaps	HW/FW	PQC-KEM-006
ML-KEM + HQC Hybrid	HW/FW	PQC-HYB-001
ML-DSA-87 Sign	HW/FW	PQC-SIG-001
ML-DSA-87 Verify	HW/FW	PQC-SIG-002
SLH-DSA-256f Sign	HW/FW	PQC-SIG-003
SLH-DSA-256f Verify	HW/FW	PQC-SIG-004
ML-DSA + SLH-DSA Hybrid	HW/FW	PQC-HYB-002
Downgrade protection	Security controller	PQC-SEC-001
Zeroization	Key manager	PQC-SEC-002

Security Evaluation Package - ۱۷- ۶

ASE

- Security Target support;
- TOE definition;
- Security objectives;
- SFR mapping.

ADV

- Architecture;
- Functional specification;
- High-level design;
- Low-level design;
- Implementation representation.

AGD

- Administrator guidance;
- User guidance;
- Secure initialization;
- Provisioning procedure.

ALC

- Configuration management;
- Development environment;
- Delivery procedures;
- Flaw remediation;
- Lifecycle.

ATE

- Test plan;
- Test procedures;
- Test results.

AVA

- Vulnerability analysis;
- Attack surface analysis;

- Penetration-test support.

PQC Security Evaluation

- PQC threat model
- PQC attack-surface analysis
- ML-KEM side-channel analysis
- HQC side-channel analysis
- ML-DSA side-channel analysis
- SLH-DSA side-channel analysis
- PQC fault-injection analysis
- hybrid-combiner security analysis
- downgrade-resistance analysis
- algorithm-substitution analysis
- intermediate-key zeroization analysis
- PQC implementation-constant-time analysis

۶ -۱۸- X Radiation Verification (در صورت لزوم)

TID

TID irradiation with Co-60 or equivalent qualified source, including pre-, intermediate- and post-irradiation electrical/security characterization.

SEE

Heavy-ion and/or proton testing for SEU, SET, SEFI and SEL.

SEL

SEL testing over specified voltage and temperature corners.

SEU

SEU cross-section measurement.

SET

SET pulse amplitude, width, propagation and functional impact characterization.

- RTL SEU fault injection
- gate-level SEU fault injection
- SET injection
- clock/reset transient injection
- memory-bit upset injection
- PCR upset injection
- lifecycle-register upset injection
- key-manager upset injection
- security-policy register upset injection
- fault propagation analysis

- recovery verification
- fail-safe verification
- zeroization verification
- radiation-induced fault containment verification

هیچ تزریق خطای تک‌بیتی یا گذرا به یک حالت حساس امنیتی نباید منجر به انتشار غیرمجاز کلید، فعال شدن دیباگ، ارتقای چرخه عمر، یا دور زدن سیاست امنیتی شود. تأیید RHBD و صلاحیت در برابر تشعشع باید شامل گوشه‌های ولتاژ و دما مرتبط باشد، از جمله محدودیت‌های مشخص‌شده دمای عملیاتی.

۶ -۱۹ - Security Documentation مخصوص سخت‌افزار

- Security architecture;
- Attack surface;
- Fault model;
- Side-channel analysis;
- Fault injection analysis;
- Glitch analysis;
- EM attack analysis;
- Differential power analysis assessment;
- SPA/DPA countermeasures;
- Zeroization analysis;
- Key isolation analysis;
- Debug security analysis;

حتی اگر آزمایشگاه certification بعداً این موارد را خودش بررسی کند، گروه طراحی باید design evidence اولیه را تحویل بدهد.

۶ -۲۰ - Post-Silicon Failure Analysis

اگر اولین Silicon مشکل داشت، گروه طراحی موظف است:

- ✓ Failure reproduce کند.
- ✓ Root cause analysis انجام دهد.
- ✓ Errata صادر کند.
- ✓ Workaround ارائه کند.
- ✓ RTL/FW اصلاح کند.
- ✓ ECO یا Metal Fix در صورت امکان ارائه دهد.
- ✓ Revision جدید tape-out کند.

۶ -۲۱ - Source Code و مالکیت

کارفرما مالک یا دارای حق دائمی استفاده از:

- RTL;
- Firmware;
- Verification environment;
- Testbench;
- Scripts;
- Synthesis scripts;
- Physical-design scripts;
- Test vectors;
- Documentation.

خواهد بود.

۷- زمان‌بندی اجرای طرح

برای اجرای طرح 3 ماه زمان پیش‌بینی شده است:

	مرحله	مدت	بازه
1	Specification + PP/ST + Architecture	۸–۱۰ هفته	۰–۲٫۵ ماه
2	RTL architecture + IP integration	۵–۶ ماه	۲–۸ ماه
3	PQC architecture + implementation	۷ الی ۸ ماه	۲–۱۰ ماه
4	RTL verification + firmware	۶–۸ ماه	۷–۱۴ ماه
5	Security/Formal verification	۶–۸ ماه	۹–۱۶ ماه
6	Synthesis + DFT	۲–۳ ماه	۱۱–۱۴ ماه
7	Physical Design	۳–۴ ماه	۱۲–۱۵ ماه
8	Sign-off + Tape-out	۴ هفته	۱۵–۱۷ ماه
9	Fab / wafer fabrication	۵–۷ ماه	۱۷–۲۲ ماه
10	Wafer sort + dicing + packaging	۲–۳ ماه	۲۲–۲۵ ماه
11	Bring-up + characterization	۳–۴ ماه	۲۵–۲۹
12	Functional/security validation	۳–۶ ماه	۲۹–۳۶ ماه

پرداخت‌ها صرفاً بر اساس تحقق نقاط عطف فنی، تحویل اقلام و خروجی‌های تعیین‌شده و تأیید کتبی کارفرما انجام خواهد شد. صرف سپری شدن مدت قرارداد یا ارائه گزارش پیشرفت کار به‌تنهایی، مبنای پرداخت نخواهد بود.

#	Milestone	زمان هدف
M0	Requirements Freeze	۰
M1	Architecture Freeze	۳
M2	PQC Architecture Freeze	۵
M3	PQC RTL/KAT	۸
M4	Hybrid Crypto Freeze	۱۱
M5	RTL Freeze	۱۳
M6	Verification/Security Freeze	۱۶
M7	RHBD Design Freeze	۱۷
M8	Synthesis/DFT Freeze	۱۹
M9	Physical Design Complete	۲۲
M10	Sign-off	۲۴
M11	Tape-out	۲۴ ماه
M12	First Wafer	۲۸–۳۰
M13	Packaged Samples	۳۰–۳۲
M14	Bring-up	۳۲–۳۳
M15	Radiation characterization	۳۳–۳۶
M16	Final validation	۳۶ ماه

۸- ترکیب پیشنهادی تیم اجرایی طرح

تخصص	تعداد	مسئولیت اصلی
Project/Technical Lead	1	مدیریت فنی کل پروژه، معماری، تصمیم‌های trade-off، و پاسخگویی نهایی RTL/FW/PD/verification هماهنگی
TPM/Security Architect	1	TPM 2.0 architecture، command hierarchy، key hierarchy، PCR، NV، authorization، lifecycle و mapping به TCG/PP/ST
Hardware Security Architect	1	Root of Trust، key isolation، secure boot، tamper/fault model، zeroization، security boundaries

RV32 core ،memory map ،bus/interconnect ، interrupt ،privilege/PMP و integration architecture	1	**CPU/SoC Architect**
طراحی RTL: TPM command engine ،PCR ،NV controller ،lifecycle ،reset/clock ،host interface ، DMA/bus و سایر logicها	4	**RTL Digital Designers**
AES ،SHA-2 ،HMAC ،RSA ،ECC ،KDF ،modular arithmetic ،key isolation و crypto datapath	۵	**Cryptography Hardware Engineers**
TRNG ،entropy source ،health test ،PUF در صورت نیاز، voltage/clock/tamper sensors و analog security blocks	۲	**TRNG/PUF/Security Analog Designer**
TPM firmware ،command implementation ،secure boot ،startup/shutdown ،NV management ، update/recovery و low-level drivers	٤	**Firmware/Embedded Engineers**
توسعه، بهینه‌سازی و آزمون نرم‌افزاری الگوریتم‌های PQC و رابط‌های رمزنگاری.	۲	**PQC Software/Crypto Engineer**
UVM ،testbench ،functional verification ، regression ،coverage ،negative/security tests و TPM command compliance	۵	**Verification Engineers**
Formal properties ،assertion ،key isolation ،access control ،secure-state FSM ،zeroization و security invariants	۲	**Formal Verification/Security Verification Engineer**
Scan ،MBIST ،JTAG ،ATPG ،test modes ،wafer sort ،ATE vectors و production test architecture	1	**DFT/ATE Engineer**
synthesis ،floorplan ،placement ،CTS ،routing ، timing closure ،IR/EM ،DRC/LVS و tape-out	۵	**Physical Design Engineer**
DPA/SPA ،fault injection ،glitch ،EM ،physical attack countermeasures و security layout review	۲	**Physical Security/Side-Channel Engineer**
RTL/synthesis/PD automation ،CI/regression ، PDK ،scripts ،version control و reproducible build flow	1	**CAD/Flow Engineer**
pad ring ،ESD ،package ،bonding diagram ،SI/PI و ارتباط با OSAT	0.5–1	**Package/Signal-Integrity Engineer**
PP/ST ،SFR/SAR ،evidence ،traceability ، و هماهنگی با آزمایشگاه ADV/ATE/AVA/ALC	1	**Common Criteria/Security Certification Engineer**
evaluation board ،silicon bring-up ،TPM command testing ،characterization و post-silicon validation	۲	**System/Validation Engineer**
تعیین الزامات تابشی، تحلیل TID/SEU/SET/SEL و برنامه‌ریزی آزمون‌های تابشی.	1–2	**Radiation/Reliability Engineer**
1نفر از ۳ PD موجود، با تخصص مشخص	۲	**Radiation-aware Physical Design Engineer**
1نفر از TRNG/Analog یا فرد جدید	۱	**Radiation Device/Circuit Engineer**

۹- حمایت‌ها

این فراخوان با حمایت معاونت علمی، فناوری و اقتصاد دانش‌بنیان و همکاری دستگاه‌های دیگر از جمله وزارت صنعت، معدن و تجارت، صندوق نوآوری و شکوفایی و وزارت ارتباطات و فناوری اطلاعات، بانک مرکزی جمهوری اسلامی ایران و مرکز مدیریت راهبردی افتا و به منظور رفع‌نیازمندی حوزه‌های احراز هویت (اسناد شناسایی، امضای دیجیتال و ...)، مخابرات و ارتباطات (سیمکارت‌های نسل جدید، تلفن همراه و ...)، پولی و بانکی (کیف پول سخت‌افزاری، پرداخت و ...) و سایر حوزه‌های نیازمند تراشه امن، برگزار خواهد شد.

جزئیات حمایت‌ها و نقش هر یک از دستگاه‌های حامی در جدول زیر نشان داده شده است:

دستگاه	حمایت/خدمت/مشوق
معاونت علمی، فناوری و اقتصاد دانش‌بنیان	کمک‌هزینه طراحی تراشه
	کمک‌هزینه نمونه‌سازی (MPW) و باندینگ (Bonding) تراشه
	کمک هزینه تولید انبوه تراشه (ماسک و تولید پایلوت)
	کمک به بازارسازی از طریق ترک تشریفات مناقصه
	ارائه خدمات تست و ارزیابی تراشه و محصول
	کمک‌هزینه طراحی و نمونه‌سازی محصول با تراشه طراحی بومی
صندوق نوآوری و شکوفایی صندوق حمایت از تحقیقات و صنایع پیشرفته	سرمایه در گردش برای تولید انبوه تراشه
	تسهیلات به خریداران محصول با تراشه طراحی بومی
	ارائه ضمانت برای تأمین مالی، شرکت در مناقصه و ...
	منابع مالی برای هزینه‌های ثابت و جاری تولید
وزارت صنعت، معدن و تجارت	مشوق‌های تعرفه‌ای
	ارائه مجوزها و تاییدیه‌های لازم
وزارت ارتباطات و فناوری اطلاعات	تسهیلات و مشوق‌های توسعه محصول و بازار
	ارائه مجوزها و تاییدیه‌های لازم
مرکز مدیریت راهبردی افتا	ارائه مجوزها و تأییدیه‌های لازم عملیاتی و امنیتی لازم

۱۰- مالکیت معنوی

مالکیت کلیه دستاوردها و خروجی‌های فنی و علمی پروژه (شامل کدهای HDL ، بلوک‌های IP ، طرح فیزیکی GDSII، اسرار فنی، مستندات و ...) متعلق به طراح خواهد بود، لکن طراح ملزم به همکاری با مرکز ملی پیشران طراحی تراشه و ارائه اطلاعات و مستندات لازم (به عنوان دارایی‌های تحت تملک خود) جهت ثبت در بانک دارایی‌های فکری تراشه خواهد بود.