بسمه‌تعالی

درخواست طرح پیشنهادی (RFP)

طراحی و تجاری‌سازی تراشه سیم‌کارت‌های نسل جدید

مرکز ملی پیشران طراحی تراشه
National Chip Design Center

شهریور ۱۴۰۵

۱ - مقدمه

از دیدگاه طراحی تراشه، سیم‌کارت‌های امروزی شباهت زیادی به یک ماژول امن سخت‌افزاری[۱](HSM) دارند. این تراشه ترکیبی از یک پردازنده امن، حافظه غیرفرار محافظت‌شده، شتاب‌دهنده‌های رمزنگاری اختصاصی، مدار مولد اعداد تصادفی واقعی (جهت تولید کلیدهای رمزنگاری) و مدارهای مقاوم در برابر نفوذ است که همگی برای محافظت از داده‌های کاربران بهینه شده‌اند و در عین حال وظیفه احراز هویت درون شبکه مخابراتی را نیز به صورت ایمن انجام می‌دهد. سیم‌کارت در معماری مخابراتی صرفاً یک حافظه یا شناسه مشترک نیست؛ یک ریشه اعتماد[۲](RoT) قابل‌حمل است که هویت مشترک، کلیدهای احراز هویت، وضعیت‌های امنیتی، فایل‌های حساس و اجرای سرویس‌های کنترل‌شده کارت مدار مجتمع جهانی[۳] (UICC) را در برابر پایانه[۴]غیرقابل اعتماد، مودم آسیب‌دیده و مهاجم فیزیکی محافظت می‌کند. بنابراین هدف این فراخوان، طراحی یک هسته مالکیت معنوی منفرد (Intellectual Property Core یا IP Core) برای استفاده در تراشه‌های دیگر نیست. محصول نهایی باید یک تراشه سامانه‌برروی‌تراشه عنصر امن (Secure Element System-on-Chip یا SE-SoC) مستقل، کامل و قابل تولید انبوه باشد که سخت‌افزار، میان‌افزار پایه، درایورها، سرویس‌های امنیتی، رابط‌های استاندارد و منابع حافظه لازم برای استقرار و اجرای UICC Card OS، برنامه‌های SIM/USIM، جاواکارت (Java Card) و گلوبال‌پلتفرم (Global Platform) را فراهم کند.

هدف اصلی این فراخوان، طراحی، توسعه، ساخت نمونه و آزمون آزمایشگاهی و شبکه‌ای یک تراشه سیم‌کارت فعال و امن است که شامل بخش‌های آنالوگ، دیجیتال و نرم‌افزاری مورد نیاز باشد. طراحی محصول باید به‌گونه‌ای انجام شود که ضمن پاسخ‌گویی به نیازهای فعلی سیم‌کارت‌های نسل جدید (USIM)، قابلیت توسعه و تکامل برای نسل‌های بعدی فناوری، کاربردهای مخابراتی و خدمات امنیتی را نیز داشته باشد.

تراشه باید یک عنصر امن (SE) سخت‌افزاری واقعی باشد و در برابر حملات نرم‌افزاری، تزریق خطا[۵]، تحلیل کانال جانبی[۶] و حملات فیزیکی[۷]مقاومت متناسب با مدل تهدید ارائه دهد. این محصول باید امکان اجرای یک محیط امن[۸] و برنامه‌های کاربردی مبتنی بر کارت هوشمند جهانی (UICC)، سیم‌کارت (SIM)، سیم‌کارت جهانی نسل سوم و بالاتر (USIM)، جاواکارت (Java Card) و گلوبال‌پلتفرم (GlobalPlatform) را فراهم کند.

معماری محصول باید شامل ریشه اعتماد سخت‌افزاری[۹] مدیریت چرخه‌ی عمر، مخزن کلید امن و غیرقابل‌خروج (Key Vault)، حافظه فرار و غیر فرار امن، گذرگاه امن[۱۰]کنترل دسترسی حافظه، شتاب‌دهنده‌های رمزنگاری، مولد اعداد تصادفی

---

[۱] Hardware Secure Module
[۲] Root-of-Trust
[۳] Universal integrated circuit card
[۴] Terminal
[۵] fault injection
[۶] Side-Channel Analysis
[۷] Physical Attack
[۸] Secure Operating Environment
[۹] Hardware Root of Trust
[۱۰] Secure Bus

واقعی (TRNG)، سازوکار راه‌اندازی امن (Secure Boot)، کنترل ضدبازگشت نسخه[۱] و حفاظت در برابر حملات فیزیکی باشد. مجری موظف است بر روی نمونه اولیه سیلیکون (First Silicon)، یک پشته نرم‌افزاری مرجع و عملیاتی ارائه کند تا امکان راه‌اندازی تراشه، اعتبارسنجی عملکردی، آزمون رابط کارت، اعتبارسنجی سرویس‌های امنیتی، آزمون سازگاری با تجهیز پایانه یا مودم و ارزیابی آزمایشگاهی در سطح شبکه فراهم شود.

معماری سخت‌افزار و فیرمور پایه باید قابلیت اجرای Card OS، Java Card و GlobalPlatform را اثبات کند. این قابلیت حداقل شامل ظرفیت و پارتیشن‌بندی مناسب Flash/NVM و SRAM، جداسازی دامنه‌های اجرایی و داده‌ای، حفاظت حافظه و گذرگاه، عملیات پایدار و اتمی NVM، فایل‌سیستم امن قابل استقرار، مدیریت چرخه عمر، APDU و ISO/IEC 7816، سرویس‌های رمزنگاری و مدیریت کلید، به‌روزرسانی امن و رابط برنامه‌نویسی پایدار است.

استاندارد ETSI TS 102 221، یکی از مراجع اصلی تعامل‌پذیری میان UICC و تجهیز پایانه است و الزامات مرتبط با رابط فیزیکی و الکتریکی، پروتکل‌های انتقال، ساختار منطقی کارت، مدل فایل‌ها و تبادل فرمان‌های کارت هوشمند[۲](APDU) را تعیین می‌کند. مشخصات فنی، استانداردهای مرجع، معماری سخت‌افزار، الزامات امنیتی، روش آزمون و معیارهای پذیرش محصول در فصل‌های بعدی این مستند ارائه می‌شوند.

توسعه برنامه‌های اختصاصی اپراتور، سامانه تجاری شخصی‌سازی کارت[۳]، ماژول امنیت سخت‌افزاری عملیاتی[۴]، سامانه تجاری مدیریت کلید، سامانه عملیاتی OTA/Provisioning، کیت توسعه تجاری PC/SC، eUICC، آماده‌سازی از راه دور سیم‌کارت[۵](RSP)، SM-DP+، SM-DS و سایر نرم‌افزارها یا خدمات تجاری سطح سامانه، خارج از دامنه این طرح هستند. با این حال، ابزارها و رویه‌های محدود آزمایشگاهی برای Test Provisioning، اجرای APDU، تزریق داده و کلید آزمایشی، اجرای آزمون خودکار و اعتبارسنجی شبکه‌ای باید به‌عنوان بخشی از بسته راه‌اندازی و آزمون تحویل شوند.

تراشه باید به‌گونه‌ای طراحی شود که برای کاربردهای اصلی UICC/SIM/USIM و شبکه‌های مخابراتی نسل دوم تا پنجم قابل استفاده باشد. قابلیت‌ها، استانداردهای مرجع و وضعیت الزام هر کاربرد در فصل سوم تعیین می‌شوند.

پیاده سازی نخست، بر مبنای فرآیند ۴۰ نانومتری (40^{nm} Mixed-Signal CMOS) معرفی شده توسط کارفرما انجام خواهد شد. طراحی دیجیتال، معماری منطقی، رابط‌های داخلی، RTL، فیرمور پایه و لایه‌های انتزاع سخت‌افزار باید تا حد ممکن قابل انتقال میان فرآیندها (Process-Portable) طراحی شوند. با این حال، قابلیت انتقال به فرآیند دیگر تنها به بخش‌های مستقل از فناوری ساخت محدود می‌شود و نباید به‌عنوان تعهد انتقال بدون تغییر کل تراشه تفسیر شود.

اجزای وابسته به فرآیند ساخت و کارخانه تولیدکننده (Foundry-Dependent) شامل حافظه غیرفرار تعبیه‌شده[۶] (eNVM/eFlash)، حافظه یک‌باربرنامه‌پذیر یا فیوز الکترونیکی (OTP/eFuse)، مولد اعداد تصادفی واقعی[۷](TRNG)، حسگرهای آنالوگ امنیتی، حلقه پایه‌ها (Pad Ring)، حفاظت تخلیه الکترواستاتیکی[۸](ESD)، مدارهای ورودی/خروجی رابط

---

[۱] Anti-Rollback
[۲] Application Protocol Data Unit
[۳] Commercial Personalization System
[۴] Operational HSM
[۵] Remote SIM Provisioning
[۶] Embedded Non-Volatile Memory
[۷] True Random Number Generator
[۸] Electrostatic Discharge

ISO/IEC 7816، نوسان‌ساز و مدار ساعت، حافظه‌های SRAM/ROM، حفاظت‌های فیزیکی و پیاده‌سازی لایه فیزیکی امنیتی[1] هستند.

پیش از تثبیت معماری (Architecture Freeze)، کارفرما بسته طراحی فرآیند (Process Design Kit یا PDK) را در قالب یک baseline معتبر و قابل استفاده در طراحی در اختیار مجری قرار خواهد داد.

هر تغییر در PDK، کتابخانه‌ها، macroهای حافظه، rule deckها یا مدل‌های sign-off پس از تثبیت baseline، باید از طریق فرآیند کنترل تغییر (Change Control) مدیریت شود. این فرآیند باید شامل تحلیل اثر تغییر (Impact Analysis)، تعیین بلوک‌های متأثر، اجرای مجدد بررسی‌های لازم و تأیید مجدد نتایج sign-off باشد.

کارفرما یا مرکز ملی پیشران طراحی تراشه مسؤول تعامل رسمی با کارخانه تولیدکننده و هماهنگی نمونه سازی چندپروژه‌ای[2] (MPW) خواهد بود. با این حال، مجری مسؤول تهیه کامل بسته فنی Tape-out، پاسخ‌گویی به پرسش‌های فنی مطرح شده از سوی کارخانه، رفع موارد قابل اصلاح در محدوده طراحی، پشتیبانی از بررسی‌های sign-off، پشتیبانی فنی از MPW، آزمون ویفر، بسته‌بندی، برنامه آزمون خودکار (ATE) و راه‌اندازی نمونه اولیه سیلیکون است.

هزینه Tape-out، ساخت نمونه، خدمات MPW و آزمون‌های مورد توافق بر عهده برنامه ملی میکروالکترونیک و مرکز ملی پیشران طراحی تراشه خواهد بود. بودجه پرداختی به مجری، مگر آنکه در قرارداد به‌صورت دیگری تعیین شود، صرفاً هزینه‌های نیروی انسانی، توسعه، مستندسازی، آزمون‌های نرم‌افزاری و خدمات قراردادی مستقیم مجری را پوشش می‌دهد.

مساحت سیلیکان ترجیحاً باید کمتر از $8\ mm^2$ باشد. لیکن حداکثر مساحت قابل قبول با توجیه فنّی $12\ mm^2$ است.

[1] Multi-Project Wafer

[2]

۲ - دامنه فعالیت

دامنه پایه طرح شامل طراحی و توسعه یک تراشه عنصر امن مستقل برای کاربرد UICC/SIM/USIM، به‌همراه فیرمور پایه، درایورها، پشته مرجع اعتبارسنجی، ابزارهای آزمون آزمایشگاهی و بسته مهندسی قابل انتقال به تولید است.

پیشنهادهای ارائه شده باید طراحی، توسعه، شبیه سازی، راستی‌آزمایی، پیاده سازی فیزیکی و تحلیل پس از سنتز و جانمایی، آماده‌سازی برای ساخت، پشتیبانی فنی Tape-out، راه‌اندازی نمونه اولیه سیلیکون، ارزیابی و تحویل مستندات و خروجی‌های فنی مورد نیاز برای تراشه امن UICC/USIM را پوشش دهند.

پیشنهادها باید شامل طراحی، شبیه‌سازی، سنتز، ساخت، ارزیابی و ارائه حداقل نمونه مهندسی (Prototype) با قابلیت عملکرد در شبکه باشد. کلیه فعالیت‌های زیر برعهده مجری است:

فعالیت‌های اصلی مجری شامل موارد زیر است:

- تحلیل نیازمندی‌ها و تدوین مشخصات فنی محصول
- طراحی معماری کلان، معماری سخت‌افزار و معماری امنیتی
- طراحی و یکپارچه‌سازی پردازنده مرکزی (CPU)، حافظه، زیرسیستم امنیت، مدیریت کلید، رمزنگاری، راه‌اندازی امن، چرخه عمر، رابط ISO/IEC 7816 و سایر زیرسیستم‌های لازم
- طراحی RTL، شبیه‌سازی، راستی‌آزمایی و راستی‌آزمایی رسمی بخش‌های امنیتی بحرانی
- توسعه فیرمور پایه، درایورها، لایه انتزاع سخت‌افزار و پشته مرجع اعتبارسنجی
- توسعه ابزارها و روش‌های آزمایشگاهی لازم برای Bring-up، اجرای APDU، Test Provisioning، آزمون UICC/USIM و اعتبارسنجی شبکه‌ای
- طراحی برای آزمون‌پذیری (Design for Test یا DFT)، آزمون حافظه، MBIST و آماده سازی مشخصات آزمون تولید
- سنتز، طراحی فیزیکی، تحلیل زمان‌بندی ایستا، تحلیل توان، بررسی افت ولتاژ و الکترومایگریشن، و انجام بررسی‌های sign-off مورد نیاز
- آماده‌سازی و تحویل بسته Tape-out و پشتیبانی فنی از تعاملات مرتبط با کارخانه تولیدکننده (Foundry)
- پشتیبانی از نمونه‌سازی، آزمون ویفر، بسته‌بندی، ATE، راه‌اندازی First Silicon، Characterization و تحلیل نتایج.
- تهیه گزارش‌های فنی، امنیتی، آزمون، طراحی فیزیکی، Silicon Errata و مستندات انتقال مهندسی.

مجری مسؤول طراحی کامل تراشه، تحویل RTL و منابع طراحی مورد توافق، آماده‌سازی بسته Tape-out، توسعه میان‌افزار و پشته مرجع اعتبارسنجی، پشتیبانی فنی از ساخت و انجام فعالیت‌های Bring-up و تحلیل فنی نمونه اولیه است.

تراشه و فیرمور پایه باید دارای قابلیت‌های لازم برای این محصولات و خدمات باشند. این قابلیت‌ها شامل منابع حافظه مناسب، جداسازی دامنه‌ها، حفاظت حافظه و گذرگاه، سرویس‌های رمزنگاری، مدیریت کلید، مدیریت چرخه عمر، به‌روزرسانی امن، رابط ISO/IEC 7816، APDU و لایه انتزاع سخت‌افزار پایدار است.

خروجی‌های تفصیلی، الزامات معماری، الزامات رمزنگاری، الزامات امنیت حافظه، طراحی فیزیکی، Floorplanning، PDK، DFT، ATE، ابزارهای FPGA و Emulator، روش آزمون، معیارهای پذیرش و برنامه زمان‌بندی در فصل‌های بعدی سند تعیین خواهند شد.

هدف نهایی این طرح، تحویل یک تراشه UICC کامل، تجاری و قابل استفاده در شبکه‌های مخابراتی است. لذا مجری موظف است در پایان پروژه (First Silicon)، کلیه لایه‌های نرم‌افزاری شامل Secure OS، Java Card Runtime Environment (JCRE) و GlobalPlatform Services را به صورت کامل، یکپارچه و عملیاتی تحویل نماید.

تبصره مدیریت ریسک پیاده‌سازی: به منظور تسریع زمان‌بندی و کاهش ریسک‌های ذاتی توسعه نرم‌افزارهای پیچیده، مجری مجاز است برای پیاده‌سازی این لایه‌ها از سیستم‌عامل‌های بلادرنگ امن (Secure RTOS) استاندارد، IP های تجاری/متن‌باز اثبات‌شده، یا لایه‌های سازگاری (Compatibility Layers) استفاده نماید.

ملاک پذیرش نهایی: فارغ از روش پیاده‌سازی داخلی، محصول نهایی باید از نظر عملکردی (Functionally) و امنیتی قادر به اجرای Applet های استاندارد Java Card، مدیریت چرخه عمر مطابق با GlobalPlatform (شامل Secure Channel و Card Manager) و احراز هویت کامل در شبکه G/5G۴ باشد. هرگونه نقص در این قابلیت‌ها در زمان تحویل First Silicon، به منزله عدم تکمیل تعهدات پروژه تلقی خواهد شد

۳ - مشخّصات فنّی محصول هدف

۳- ۱- تعریف محصول و سطح هدف

محصـــول هدف این طرح، یک تراشـــه مســـتقل و قابل تولید برای کاربردهای ســـیم‌کارت قابل‌حمل (Removable SIM)، سیم‌کارت UICC و سیم‌کارت USIM است. تراشه باید به‌صورت یک سامانه‌برروی‌تراشه عنصر امن (SE-SoC) طراحی شود. محصـــول هدف صـــرفاً یک میکروکنترلر عمومی با شـــتاب‌دهنده رمزنگاری، یک هســـته مالکیت معنوی مجزا (Intellectual Property Core یا IP Core) یا یک نمونه آزمایشگاهی محدود نیست. معماری محصول باید به‌گونه‌ای باشد که بتواند نقش ریشه اعتماد سخت‌افزاری (Hardware Root of Trust) را در یک UICC ایفا کند.

تراشه باید در کنار اجرای فیرمور پایه و پشته مرجع اعتبارسنجی، حفاظت از کلیدهای احراز هویت، داده‌های حساس مشترک، اطلاعات فایل‌سیستم، وضعیت‌های امنیتی، داده‌های PIN/PUK، کلیدهای به‌روزرسانی و سایر اشیای امنیتی را فراهم کند.

محصول باید برای استفاده در شبکه‌های GSM، UMTS، LTE و 5G مناسب باشد. طراحی باید با الزامات UICC/USIM و استانداردهای مرتبط سازگار بوده و در حد دامنه تعیین‌شده، امکان اعتبارسنجی آزمایشگاهی، تعامل با پایانه/مودم و آزمون در سطح شبکه را فراهم کند.

کاربرد یا قابلیت	وضعیت	توضیح
سیم‌کارت قابل‌حمل (Removable SIM)	الزامی	محصول باید برای استفاده در قالب سیم‌کارت قابل‌حمل قابل طراحی و تولید باشد
UICC	الزامی	قابلیت‌های پایه سخت‌افزار و پشته مرجع باید نیازهای UICC را پوشش دهند
GSM SIM	الزامی	در سطح Reference Validation Stack و Test Flow مصوب
USIM	الزامی	در سطح Reference Validation Stack و Test Flow مصوب
احراز هویت LTE	الزامی	در سطح Crypto Service، Key Management و آزمون مرجع
احراز هویت 5G	الزامی	در سطح سرویس‌های رمزنگاری، مدیریت داده حساس و آزمون مرجع
حفاظت از SUPI و پردازش SUCI	الزامی	در حد نیاز پروفایل 5G و با مدیریت امن کلید/داده
ذخیره‌سازی امن credential	الزامی	برای کلید، داده هویتی، metadata و اشیای امنیتی
به‌روزرسانی امن firmware	الزامی	شامل Authentication، Integrity، Version Control، Anti-Rollback و Recovery
Java Card	کامل و آزمون‌شده	مجری مجاز است برای این بخش از IP های تجاری (Commercial IP) یا Open-Source های اثبات‌شده استفاده نماید.
GlobalPlatform	کامل و آزمون‌شده	مجری مجاز است برای این بخش از IP های تجاری (Commercial IP) یا Open-Source های اثبات‌شده استفاده نماید.
eSIM/eUICC	آمادگی معماری	باید از نظر معماری سخت‌افزاری و امنیتی برای توسعه آتی به‌عنوان eUICC/eSIM آماده باشد. این الزام در First Silicon به‌معنای پیاده‌سازی

کاربرد یا قابلیت	وضعیت	توضیح
		کامل پروتکل‌های RSP/SM-DP+/SM-DS infrastructure یا اخذ گواهینامه‌های GSMA نیست. اما حداقل باید قابلیتهای زیر را داشته باشد: • secure provisioning • profile isolation • profile lifecycle • encrypted profile handling • profile activation/deactivation • secure deletion • profile metadata protection • remote-management security همچنین در مستندات نشان داده شود که افزودن این قابلیت‌ها در نسل بعدی نیازمند Redesign اساسی نیست.
NFC/ISO 14443	اختیاری	فقط در صورت تعریف صریح محصول NFC-SIM یا Contactless UICC
SWP/HCI	قابلیت معماری	باید امکان پشتیبانی از Single Wire Protocol / HCI پیش‌بینی شود. اگر فعال شود، باید با profile مربوط به UICC/NFC سازگار باشد.
iSIM	قابلیت معماری	خارج از scope نمونه اولیه سیلیکون
احراز هویت اینترنت اشیا (IoT)	قابلیت کاربردی	در سطح Key Management، Crypto Service و Secure Credential Storage

محصـول باید از اسـتانداردهای UICC و USIM مورد توافق پشـتیبانی کند. حداقل مراجع فنی برای تعامل UICC با تجهیز پایانه و برای سـاختار و کاربرد USIM در جدول زیر آمده اسـت. در ابتدای پروژه، نسـخه، پروفایل، بندهای قابل‌اجرا و روش آزمون هر استاندارد در ماتریس انطباق (Compliance Matrix) تثبیت خواهند شد.

حوزه	مرجع یا الزام هدف	وضعیت
رابط کارت هوشمند	ISO/IEC 7816-3	الزامی
پروتکل کارت	T=0 و T=1	الزامی
تعامل‌پذیری UICC	ETSI TS 102 221	الزامی
پلتفرم UICC	3GPP TS 31.101	الزامی در سطح مرجع
کاربرد USIM	3GPP TS 31.102	الزامی در سطح مرجع
LTE/5G Security	پروفایل مورد توافق کارفرما	الزامی
Java Card	نسخه هدف در ماتریس انطباق	کامل و آزمون‌شده
GlobalPlatform	نسخه و پروفایل هدف در ماتریس انطباق	کامل و آزمون‌شده
NFC/PICC	ISO/IEC 14443 Type A/B	اختیاری
SWP/HCI	ETSI TS 102 613 در صورت کاربرد	اختیاری

حوزه	مرجع یا الزام هدف	وضعیت
آمادگی امنیتی	آمادگی لازم برای اخذ Common Criteria در سطح EAL5+ یا بالاتر در آینده	الزامی
TRNG	هدف AIS31 TG.2 مطابق دامنه مصوب	الزامی
PQC	FIPS 203، FIPS 204 و FIPS 205 در صورت فعال‌سازی	قابلیت معماری و توسعه‌ای

۳-۲- معماری کلان UICC امن

تراشه باید دارای مرز اعتماد مشخص[۱] باشد. مرز اعتماد باید در معماری سخت‌افزار، معماری امنیتی، نمودارهای جریان داده، نمودارهای جریان کلید، نقشه حافظه (Memory Map)، نقشه رجیسترها (Register Map) و برنامه Verification[۲] مشخص شود.

تمام مسیرهای دسترسی به کلیدها، حافظه‌های حساس، Flash/NVM، Key RAM، هسته رمزنگاری، رابط ISO/IEC 7816، Debug، DFT، DMA، Boot ROM و کنترل‌کننده چرخه‌حیات باید تحت کنترل Security Controller و سیاست Lifecycle قرار گیرند.

معماری باید به‌گونه‌ای باشد که پردازنده مرکزی صرفاً بتواند از طریق API یا سرویس رمزنگاری (Crypto Service) مجاز، درخواست انجام عملیات رمزنگاری یا مدیریت شیء امنیتی را ارائه کند. پردازنده مرکزی، Application، DMA، Debug Interface، DFT Interface، APDU Interface یا Host نباید بتوانند به private key، Ki، OPc، key wrapping key، intermediate crypto data، Key RAM یا اشیای امنیتی حساس به‌صورت خام دسترسی داشته باشند.

زیرسیستم	الزام فنی	هدف امنیتی
Hardware Root of Trust	Boot ROM غیرقابل تغییر، Root Key/Hash و Boot Policy	جلوگیری از اجرای کد غیرمجاز
Secure CPU	CPU ۳۲ بیتی، deterministic و in-order	اجرای فیرمور با رفتار قابل پیش‌بینی
Security Controller	کنترل متمرکز lifecycle، tamper، debug و policy	جلوگیری از bypass شدن سیاست‌های امنیتی
Lifecycle Controller	ماشین حالت یک‌طرفه یا policy-controlled	جلوگیری از بازگشت به وضعیت ناامن
Key Vault	ذخیره و استفاده غیرقابل‌خروج از کلیدها	حفاظت از کلیدهای خصوصی و Ki/OPc
Key Manager	اعمال owner، domain، purpose و usage policy	جلوگیری از استفاده نامجاز از کلید
Secure Bus/Interconnect	کنترل master، آدرس، privilege و lifecycle	جلوگیری از دسترسی غیرمجاز به منابع حساس
Memory Firewall	کنترل دسترسی CPU، DMA، Debug، DFT و Peripheral	حفاظت از Flash، SRAM و NVM حساس

[۱] Trust Boundary

[۲]

زیرسیستم	الزام فنی	هدف امنیتی
Crypto Service Interface	درخواست عملیات به‌جای export کلید	جداسازی کلید از نرم‌افزار عمومی
Secure NVM Controller	ECC، Integrity، Anti-Tearing و Recovery	حفاظت از داده‌های پایدار
TRNG/DRBG	entropy فیزیکی، health test و DRBG	تولید تصادفی امن برای کلید و پروتکل
ISO 7816 Controller	رابط تماس، Timing و APDU Transport	تعامل امن با پایانه
Tamper Controller	تشخیص و پاسخ به حملات محیطی	مقابله با fault و physical attack
Secure Watchdog	Watchdog مستقل و policy-controlled	جلوگیری از توقف کنترل‌های امنیتی
Debug/DFT Controller	کنترل مبتنی بر چرخه عمر	جلوگیری از نشت از مسیر آزمون
Monotonic Counter	شمارنده امن غیرقابل بازگشت	Anti-Rollback و مدیریت نسخه

همچنین باید پردازنده، کنترل‌کننده امنیت، کنترل‌کننده چرخه‌حیات و مدیریت کلیدها دارای مسؤولیت‌های تفکیک شده باشند. واحد Security Controller نباید صرفاً یک رجیستر وضعیت یا مجموعه‌ای از بیت‌های قابل پیکربندی از طریق نرم‌افزار باشد؛ این کنترل‌کننده باید بتواند در سطح سخت‌افزار، دسترسی به حافظه، Crypto Service، Debug، DFT، Boot Policy و Tamper Response را کنترل یا محدود کند.

۳-۳- معماری پردازنده، حافظه و گذرگاه امن

۳-۳-۱- معماری پردازنده

ترا شه باید از یک پردازنده امن ۳۲ بیتی ا ستفاده کند. هدف ا صلی پردازنده مرکزی در UICC، د ستیابی به حداکثر فرکانس یا throughput عمومی نیست؛ بلکه اجرای deterministic firmware، مصرف توان پایین، مساحت کم، قابلیت تحلیل زمانی، امکان اعمال isolation و قابلیت راستی‌آزمایی امنیتی اهمیت دارد. پردازنده باید از اجرای speculative، out-of-order و قابلیت‌هایی که تحلیل زمان، رفتار خطا یا کنترل اطلاعات را پیچیده می‌کنند اجتناب کند.

معماری پیشنهادی پیاده‌سازی معماری RISC-V با پشتیبانی از مجموعه دستورالعمل RV32IMC + Zicsr + Zifencei به صورت معماری هاروارد است. مشخصات معماری پیشنهادی به شرح زیر است:

پارامتر	الزام و ملاحظات
عرض بیتی	۳۲ بیت
تعداد هسته	تک هسته
مدل اجرا	In-order و deterministic
گام‌های خطلوله	۳ تا ۴ گام
فرکانس هدف	۳۰ تا ۵۰ مگاهرتز (نهایی پس از PPA و PVT)
Speculative Execution	مجاز نیست.

پارامتر	الزام و ملاحظات
Out-of-Order Execution	مجاز نیست.
Branch Prediction	اختیاری
MMU	نیاز نیست.
MPU/PMP	الزامی (حداقل ۸ ناحیه یا سازوکار معادل)
M-mode	الزامی
U-mode	اختیاری (در صورت نیاز به جداسازی نرم‌افزاری)
S-mode	نیاز نیست.
Cache	نیاز نیست. (در صورت استفاده نیازمند تحلیل امنیتی جداگانه)
FPU	نیاز نیست.
Vector Extension	نیاز نیست.
Debug	lifecycle-controlled
DMA	اختیاری (در صورت وجود، تحت Memory Firewall)

برای پردازنده مورد نظر باید مجموعه دستورالعمل (ISA)، افزونه‌ها، رفتار PMP، سطوح دسترسی و اجرا، معماری وقفه، ماژول عیب‌یابی، ابزارهای توسعه مانند کامپایلر، دیباگر و غیره و روش عیب‌یابی امن مشخص شوند.

۳-۳-۲- معماری حافظه

معماری حافظه باید برای اجرای Boot ROM، فیرمور پایه، سرویس رمزنگاری، Reference Validation Stack، داده‌های UICC/USIM، عملیات NVM atomic و استقرار Card OS، Java Card و GlobalPlatform کافی باشد.

نوع حافظه	ظرفیت هدف	حداقل قابل قبول	کاربرد
Boot ROM	64 KB	48 KB	Root of Trust، Boot و Recovery Policy
Embedded Flash/eNVM	1 MB	768 KB	فیرمور، داده، به‌روزرسانی و رزرو معماری
Protected/High-Endurance NVM	32 KB	16 KB	Lifecycle، Counter، Journal و Metadata
SRAM عمومی	24 KB	16 KB	Stack، Buffer و Runtime
Key RAM	4 KB	4 KB	کلیدها و داده میانی حساس
Crypto Working RAM	8 KB	4 KB	عملیات رمزنگاری و Buffer کنترل‌شده
SRAM	32 KB	24 KB	مجموع SRAM عمومی، Key RAM و Crypto RAM
OTP/eFuse	1 KB	512 B	UID، Root Hash، Lifecycle و Configuration

ظرفیت Flash باید به صورت ظرفیت مفید (Usable Capacity) بیان شود. ظرفیت اسمی ماکروی حافظه بدون درنظرگرفتن ECC، Metadata، Spare Area، Remap، Transaction Journal، فضای به‌روزرسانی، فضای Recovery و فضای رزرو قابلیت‌های آینده، معیار پذیرش نیست.

ناحیه	ظرفیت هدف	سیاست حفاظت
Bootloader و Secure Runtime	200 KB - 300 KB	Secure Boot، Integrity و Anti-Rollback
Firmware و Driverهای پایه	100 KB - 150 KB	Authenticated Update
Reference UICC/USIM Stack	100 KB - 180 KB	Integrity و Version Control
داده‌ها و فایل‌های آزمایشی	≥ 150 KB	ECC، Anti-Tearing و Access Control
فضای رزرو Java Card و GlobalPlatform	Memory Budget	قابلیت معماری، نه Runtime تولیدی
Image به‌روزرسانی	≥ 200 KB	Atomic Commit، Recovery و Rollback Protection
Recovery Image/Data	≥ 100 KB	Policy-Controlled و Integrity-Protected
Security Metadata و Journal	رزرو شده	Sequence، Commit و Recovery
فضای توسعه آینده	رزرو شده	Architecture-Controlled

۳-۳-۳- حفاظت حافظه و Secure Bus

فایل‌سیستم UICC، سیاست‌های MF/DF/ADF/EF، دسترسی PIN/ADM و semantics فرمان‌های UICC، در سطح سیستم‌عامل سیم‌کارت یا پشته نرم‌افزاری مربوطه پیاده سازی می شوند. سخت‌افزار نباید مسؤول اجرای semantics کامل فایل‌سیستم UICC تلقی شود. با این حال، سخت‌افزار باید primitiveهای لازم را برای اجرای امن سیستم‌عامل سیم‌کارت را فراهم کند. این موارد بنیادی شـامل firewall، secure partition، NVM atomicity، isolation، integrity و جلوگیری از bypass هستند.

قابلیت	الزام
Memory Firewall	کنترل دسترسی مبتنی بر master، privilege، lifecycle و security attribute
Secure Bus	کنترل مسیر CPU، DMA، Debug، DFT و Peripheralها به حافظه حساس
Key RAM Isolation	عدم دسترسی مستقیم CPU، DMA و Debug به Key RAM
DMA Filtering	محدودیت address، length، ownership و privilege در صورت وجود DMA
ECC	حفاظت از خطاهای حافظه و داده‌های حساس
Integrity Protection	برای metadata، counter، lifecycle و security object
Address/Data Scrambling	متناسب با Threat Model و PDK
Encryption	در صورت نیاز Threat Model برای داده پایدار حساس

قابلیت	الزام
Anti-Tearing	برای عملیات حیاتی NVM
Atomic Update	برای PIN Counter، Lifecycle، Update State و Metadata
Journal	ثبت تراکنش و recovery بعد از power loss
Sequence/Commit Marker	تشخیص rollback و incomplete update
Secure Zeroization	برای SRAM، Key RAM و رجیسترهای حساس
Cryptographic Erase	برای داده NVM محرمانه در صورت نیاز
Key Invalidation	برای ابطال دسترسی به داده رمزشده یا کلیدهای حساس
Remanence Mitigation	کاهش خطر باقی‌ماندن داده در حافظه volatile

برای هر شـــیء امنیتی پایدار و حســـاس، ســـاختار داده باید حداقل دارای Header، Object Type، Version/Epoch، Sequence Number، Payload، Integrity Value، Commit Marker و Recovery State باشد.

۳- ۴- فرایند بوت

Boot ROM باید غیرقابل تغییر باشد و ریشه اعتماد اولیه را تشکیل دهد. همچنین باید پیش از انتقال کنترل به Bootloader یا فیرمور، وضـــعیت چرخه‌حیات ، وضـــعیت Debug/Test، مجوز امضـــاءکننده، تمامیت image، version، anti-rollback counter و سیاست recovery را بررسی کند.

قابلیت	الزام
Immutable Boot ROM	الزامی
Root Key/Hash	در ROM، OTP/eFuse یا Secure NVM طبق معماری
Firmware Authentication	الزامی
Firmware Integrity	الزامی
Signer Authorization	الزامی
Version Control	الزامی
Anti-Rollback	الزامی
Anti-Replay	الزامی
Lifecycle Check	الزامی
Debug/Test State Check	الزامی
Atomic Commit	الزامی
Interrupted Update Protection	الزامی
Recovery Mode	Fail-Secure و Policy-Controlled
Bootloader پیش‌فرض	امضاء شده و تحت کنترل Boot ROM

قابلیت	الزام
جایگزینی Bootloader	فقط با امضاء کننده مجاز، policy، version و recovery
Firmware Encryption	در صورت نیاز Threat Model
کلید رمزگشایی فیرم‌ور	Device-Unique یا Wrapped (غیرقابل‌دسترسی برای CPU)
Classical Signature	الزامی
PQC/Hybrid Signature	قابلیت معماری؛ فعال‌سازی براساس profile و feasibility

سامانه عملیاتی OTA/Provisioning، مدیریت پروفایل مشترک و زیرساخت تجاری Remote Provisioning در این طرح پایه نیســـتند. با این حال، Secure Update Engine، APIهای لازم، مدیریت image و policyهای امنیتی باید به‌گونه‌ای طراحی شـــوند که در آینده بتوانند تحت یک ســـامانه OTA مجاز (مطابق با ETSI TS 102 226 برای مدیریت از راه دور و GSMA SGP.22 برای eSIM) مورد استفاده قرار گیرند.

۳- ۵- Firmware / Secure OS

مجری موظف است firmware لازم برای عملکرد کامل تراشه را تحویل دهد. حداقل شامل:

- Boot ROM
- Secure Bootloader
- Secure OS
- Hardware Abstraction Layer
- device drivers
- memory manager
- lifecycle manager
- cryptographic service layer
- key-management service
- secure storage service
- OTA/update manager
- random-number service
- APDU dispatcher
- ISO 7816 protocol stack
- SIM application framework
- USIM application
- security-event manager
- watchdog service
- tamper response
- diagnostic service
- manufacturing/personalization firmware

UICC Card OS باید کاملاً عملیاتی و کامل باشد، اما نباید از صفر (From Scratch) نوشته شود. منظور از UICC Card OS در این سند، مجموعه کامل نرم‌افزاری است که قابلیت‌های مدیریت فایل، APDU، Lifecycle و Security Domains

را ارائه می‌دهد. مجری مجاز است برای لایه هسته (Kernel) و مدیریت تسک‌ها، از یک سیستم‌عامل بلادرنگ امن (Secure RTOS) استاندارد و متن‌باز (مانند Zephyr یا FreeRTOS با پیکربندی امن) یا تجاری استفاده نماید.

با این حال، لایه‌های میانی (Middleware) شامل UICC Stack، Secure File System، APDU Engine، Lifecycle Manager و Key Management باید اختصاصاً برای این معماری طراحی و پیاده‌سازی شوند. مجری موظف است ایزولاسیون امنیتی بین اپلیکیشن‌ها (Applet Isolation) و حفاظت از حافظه را حتی در صورت استفاده از RTOS مشترک، به صورت سخت‌افزاری/نرم‌افزاری تضمین نماید.

۳- ۶- UICC / SIM Software Stack

ترا شه نباید صرفاً سخت‌افزار UICC با شد؛ بلکه باید software stack لازم برای اجرای SIM/UICC را نیز دا شته با شد.

حداقل شامل:

- UICC Platform
- ISO/IEC 7816 logical model
- APDU processing
- File system
- EF/DF hierarchy
- security attributes
- PIN management
- ADM authentication
- access-condition enforcement
- application selection
- logical channel management
- status-word handling
- SIM
- SIM application
- subscriber identity management
- authentication interface
- GSM authentication support
- USIM
- USIM application
- AKA-related operations
- USIM security parameters
- EF structures
- authentication service
- 3GPP security services (3GPP TS 31.102 مشخصات USIM application را تعریف می‌کند)

۳- ۷- 5G Security

۳- ۷- ۱- تراشه باید برای ۵ G subscriber authentication آماده باشد. حداقل شامل:

- 5G AKA cryptographic services
- key derivation
- SUCI-related cryptographic processing
- SUPI protection services
- home-network public-key handling where applicable
- secure storage of subscriber credentials
- domain separation
- anti-replay controls

۳- ۸- Secure File System

UICC filesystem باید hardware-enforced access control داشته باشد و از موارد زیر پشتیبانی کند:

- MF
- DF
- ADF
- EF
- application-specific files
- PIN-protected files
- ADM-protected files
- secure messaging
- access-condition enforcement
- atomic updates
- anti-tearing
- transaction recovery

۳- ۹- Cryptographic Engine

زیرسیستم رمزنگاری باید از نیازهای Secure Boot، به‌روز رسانی و ذخیره‌سازی امن، Test Provisioning، UICC/USIM validation، LTE/5G validation و قابلیت‌های آینده پشتیبانی کند.

گروه	الگوریتم یا قابلیت	وضعیت
رمزنگاری متقارن	AES-128	الزامی
رمزنگاری متقارن	AES-192 و AES-256	الزامی
Mode	CBC، CTR و CMAC	الزامی
Mode	GCM	الزامی
الگوریتم قدیمی	3DES سه‌کلیدی	فقط برای سازگاری قدیمی
Hash	SHA-256	الزامی
Hash	SHA-384 و SHA-512	الزامی

Hash قدیمی	SHA-1	فقط برای سازگاری قدیمی
MAC/KDF	HMAC و KDFهای مخابراتی	الزامی
KDF	HKDF	الزامی
Public Key	ECC P-256/P-384	الزامی (شتاب‌دهنده)
Public Key	RSA-2048	الزامی (شتاب‌دهنده)
Public Key	RSA-3072/4096	اختیاری با توجیه
Curve	X25519/Ed25519	در صورت نیاز پروفایل
Random	TRNG و DRBG	الزامی
Key Storage	Key Vault و Key Manager	الزامی
PQC	Crypto-Agile API و Memory Budget	الزامی
PQC Accelerator	Hardware/Hybrid Engine	مشروط به feasibility

عملیات private-key نباید توسط نرم‌افزار بدون countermeasure مناسب انجام شود. برای RSA، ECC و سایر الگوریتم های حساس، روش های Blinding، CRT Verification، Point Validation، Scalar Randomization، Constant-Time Implementation، Zeroization و Secure Intermediate Data Handling باید در معماری و برنامه آزمون لحاظ شوند.

TRNG باید دارای منبع entropy فیزیکی، startup health test، continuous health test، conditioning، failure detection، secure failure state، DRBG/CSPRNG، reseed mechanism و قابلیت جلوگیری از مصرف entropy نامعتبر باشد.

۳- ۱۰- Cryptographic Accelerators

Private-key operations نباید توسط software به‌صورت unprotected انجام شوند. مجری باید در Architecture Phase مقایسه کمی بین hardware accelerator، firmware implementation و hybrid implementation برای ML-KEM و ML-DSA از نظر area، latency، SRAM، power و side-channel resistance ارائه کند.

۳- ۱۱- Post-Quantum Cryptography (PQC)

لازم نیست که تمام ارتباطات تراشه PQC باشند و PQC بصورت انتخابی/ترکیبی با الگوریتمهای کلاسیک می‌تواند باشد تا اختلالی در کار با شبکه ایجاد نشود. تراشه بهتر است از Post-Quantum Cryptography به‌صورت crypto-agile پشتیبانی کند.

۳- ۱۱- ۱- Key Encapsulation

ML-KEM مطابق FIPS 203، حداقل ML-KEM-768 و ترجیحاً ML-KEM-1024 برای security-critical applications.

۳- ۱۱ -۲ Digital Signature

ML-DSA مطابق FIPS 204، حداقل ML-DSA-65.

۳- ۱۱ -۳ Hash-based Signature

SLH-DSA مطابق FIPS 205، حداقل یک parameter set مورد توافق برای استفاده در root-of-trust یا fallback signature verification.

۳- ۱۲ TRNG

TRNGباید hardware-based باشد. شامل:

- physical entropy source
- startup health test
- continuous health test
- entropy conditioning
- DRBG/CSPRNG
- reseed mechanism
- failure detection
- secure failure state

۳- ۱۳ Key Management

تراشه باید دارای Hardware Key Manager باشد. حداقل key domains:

- Root of Trust
- Device Identity Key
- SIM/USIM authentication keys
- OTA keys
- Secure Boot keys
- Firmware-signing verification keys
- Application keys
- Session keys
- Transport keys
- 5G security keys
- PQC root verification keys
- PQC firmware-signing verification keys
- PQC RSP/provisioning keys where applicable

- Hybrid classical/PQC key objects
- Algorithm identifier
- Parameter-set identifier
- Key-version / epoch

کلیدهای خصوصی هرگز نباید توسّط CPU، APDU interface، host، یا debug interface قابل خواندن باشند. معماری امنیتی تراشه باید crypto-agile باشد، به‌گونه‌ای که الگوریتم‌ها، parameter setها، key types، signature formats و cryptographic policyها بدون تغییر اساسی در سخت‌افزار قابل مدیریت و در صورت امکان از طریق firmware/security-policy update قابل توسعه باشند. پیاده‌سازی نباید به یک الگوریتم PQC یا یک parameter set خاص وابستگی غیرقابل تغییر داشته باشد.

۳-۱۴- Key Vault

Key Vault باید:

access-controlled باشد؛

lifecycle-aware باشد؛

zeroization داشته باشد؛

integrity-protected باشد؛

anti-replay باشد؛

hardware access policy داشته باشد؛

برای هر key، owner/domain/purpose را enforce کند.

قابلیت	الزام
Hardware Key Manager	الزامی
Key Vault	الزامی
Key Identifier	الزامی
Key Type	الزامی
Algorithm Identifier	الزامی
Version/Epoch	الزامی
Owner/Domain/Purpose	الزامی
Usage Permission	الزامی
Lifecycle Policy	الزامی
Export Policy	الزامی
Rotation/Revocation Policy	الزامی
Non-Exportable Private Key	الزامی
Access-Controlled	الزامی
Lifecycle-Aware	الزامی

قابلیت	الزام
Integrity-Protected	الزامی
Anti-Replay	الزامی
Zeroization Support	الزامی
Audit/Event Support	در صورت امکان معماری

کلیدهای Root of Trust، Device Identity، Secure Boot، Firmware Update، Transport/Wrap، Test Provisioning، UICC/USIM Test Credential، Session Key و کلیدهای مورد استفاده در 5G باید در دامنه‌های مجزا مدیریت شوند.

۳-۱۵- Debug، DFT و Tamper

چرخه‌حیات باید از ابتدا در معماری، RTL، NVM، Boot Policy، Debug Policy، DFT Policy و Test Plan لحاظ شود. صرف فهرست کردن وضعیت‌های چرخه‌حیات کافی نیست؛ برای هر transition باید trigger، authorization، persistent encoding، اثر روی دسترسی‌ها، رفتار rollback، رفتار reset/tamper و روش verification تعریف شود.

وضعیت	کاربرد	سیاست اصلی
Manufacturing	تولید و آزمون اولیه	بدون داده عملیاتی و کلید تولیدی
Test	DFT و آزمون مهندسی	دسترسی محدود، ثبت رویداد و کنترل‌شده
Development	توسعه و Debug	Debug صرفاً با Authentication
Initialization	تنظیم اولیه تراشه	اعمال configuration مجاز
Provisioning	تزریق داده/کلید آزمایشی	Test Provisioning محدود
Personalization	آماده‌سازی برای شخصی‌سازی	خارج از بهره‌برداری تجاری پایه
Operational	بهره‌برداری عادی	Debug/DFT غیرمجاز
Locked	حالت محدود	محدودیت سرویس‌ها بر اساس policy
RMA	تحلیل خرابی	بدون افشای کلید خصوصی یا Ki/OPc
Decommissioned	خروج از سرویس	Abortion/Invalidation سرویس‌های حساس

Tamper response باید بتواند:

- operation abort
- key zeroization
- secure reset
- interface lock
- lifecycle transition
- security-event recording

را اجرا کند.

قابلیت	الزام
Voltage Monitor	الزامی
Brownout Detector	الزامی
Over/Under-Voltage Detection	الزامی
Clock Monitor	الزامی
Clock Glitch Detection	الزامی
Frequency Anomaly Detection	الزامی
Reset Monitor	الزامی
Temperature Monitor	الزامی
Light Sensor	در صورت پشتیبانی PDK و Threat Model
Tamper Controller	الزامی
Secure Watchdog	الزامی
Independent Security Clock	الزامی
Memory Integrity Monitoring	الزامی
Security Event Recording	در صورت امکان معماری
Operation Abort	الزامی
Secure Reset	الزامی
Interface Lock	متناسب با policy
SRAM/Key RAM Zeroization	الزامی
NVM Key Invalidation/Crypto Erase	متناسب با policy
Lifecycle Escalation	در صورت نیاز policy

Side-Channel Protection

مجری باید در برابر موارد زیر countermeasure ارائه دهد:

- SPA
- DPA
- CPA
- timing analysis
- power analysis
- EM analysis

برای AES، RSA، ECC، ML-KEM، ML-DSA و سایر الگوریتم‌های asymmetric/PQC فعال در محصول حداقل باید:

- masking یا equivalent countermeasure
- randomized execution where appropriate
- constant-time implementation
- secure intermediate-data handling

وجود داشته باشد.

Fault Injection Protection

باید در برابر:

- clock glitch
- voltage glitch
- reset glitch
- instruction skip
- fault injection
- laser/optical attack

تا سطح threat model مورد توافق مقاومت طراحی شود. Fault attacks against PQC implementations، شامل instruction/data fault، coefficient/memory fault، rejection-check bypass و verification bypass نیز باید در threat model و security verification پوشش داده شوند.

۳-۱۶- پروتکل‌های ارتباطی

رابط تماس ISO/IEC 7816، رابط اصلی تراشه UICC است. این رابط باید با الزامات الکتریکی، timing و transport مورد توافق برای UICC سازگار باشد.

قابلیت	وضعیت
C1 تا C8 Contact Mapping	الزامی
VCC	الزامی
GND	الزامی
CLK	الزامی
RST	الزامی
I/O	الزامی
ATR	الزامی
PPS	الزامی
T=0	الزامی
T=1	الزامی
ETU Timing	الزامی

قابلیت	وضعیت
Protocol Timing	الزامی
APDU Transport	الزامی
Brownout/Reset Handling	الزامی
Class A	در صورت نیاز بازار و قابلیت PDK/Pad
Class B و Class C	الزامی
Physical Extended APDU support	قابلیت پشتیبانی

پشتیبانی از NFC یا ISO/IEC 14443 الزامی نیست. رابط SWP/HCI نیز فقط در صورتی الزامی است که UICC/eSE به کنترل‌کننده NFC متصـــل شـــود. در چنین حالتی، نقش UICC، نقش کنترل‌کننده NFC، Pad Assignment، Voltage Domain، Clock/Reset Ownership، Power Ownership، Secure Channel، HCI Profile، Test Profile و Lifecycle Policy باید به‌صورت مستقل تعریف شود.

۳-۱۷- طراحی فیزیکی (Physical Design) و Floorplanning

طراحی فیزیکی و Floorplanning باید با رویکرد Macro-First Floorplanning و Security Zoning انجام شـــوند. هدف، صـــرفاً رســـیدن به مســـاحت کوچک نیســـت؛ بلکه باید بین area، timing، power، NVM feasibility، physical attack resistance، pad/ESD، yield، DFT و قابلیت sign-off تعادل برقرار شود.

Boot ROM، Key Vault، Key RAM، Protected NVM، Crypto Engine، Security Controller، Lifecycle Controller، TRNG، Tamper Sensor، Clock Generator، ISO 7816 I/O و DFT Boundary باید از ابتدا دارای محدوده فیزیکی، Power Domain، Clock Domain، Reset Domain و Routing Policy مشخص باشند.

Key RAM، Key Vault و مســـیرهای عبور کلید باید از CPU، I/O Pad، Scan Chain، Debug Logic، مســـیرهای عمومی داده، Clock Tree پرنویز و nodeهای switching رمزنگاری، فاصله و جداسازی (isolation) مناسب داشته باشند.

استفاده از Shielding، Guard Ring، Top-Metal Shield، Tamper Mesh، Decoupling، Placement Blockage، Routing Blockage و Substrate Isolation باید متناسب با قابلیت PDK و Threat Model بررسی شود.

eNVM، TRNG، Analog Sensor، Oscillator، Clock Circuit و ســـایر مدارهای حســـاس آنالوگ باید تا حد ممکن از منابع switching، مســـیرهای پرجریان، منابع نویز substrate، Crypto Datapath، IR Drop و ناحیه‌های پرنویز دیجیتال جدا شوند.

موضوع	الزام	روش اثبات
رویکرد Floorplan	Macro-First Planning و Security Zoning	Floorplan Review

موضوع	الزام	روش اثبات
Boot ROM	ناحیه مشخص و حفاظت‌شده	Floorplan و Security Report
Key Vault/Key RAM	جداسازی از CPU، I/O، Scan و Debug	Layout/Route Review
Protected NVM	Power/Clock/Reset/Routing مستقل Policy	Physical Security Review
Crypto Engine	کنترل leakage و جداسازی مسیر کلید	SCA-Aware Layout Review
TRNG/Analog Sensor	جداسازی از Noise، IR Drop و Switching	Analog/Physical Review
Security Controller	مسیر tamper/reset اولویت‌دار	Micro-Architecture و Layout Review
Pad Ring/ESD	سازگاری با ISO 7816، PDK و Package	Pad/ESD Feasibility Report
Guard Ring	مطابق PDK و Threat Model	Layout Guideline
Shielding	برای Critical Net و Key Path	Shield Coverage Report
Tamper Mesh	در صورت پشتیبانی PDK و Threat Model	Physical Security Review
Power Mesh/Decoupling	کنترل IR Drop و Noise	IR/EM/Power Report
Clock Isolation	حفاظت Security Clock و Clock Tree حساس	CTS/Clock Report
Congestion	کنترل Macro Halo، Channel و Blockage	Congestion Report
DFT Isolation	عدم bypass Key/Data Path حساس	DFT Security Review
DRC/LVS/ERC/Antenna/DFM	Sign-off کامل	Sign-off Report
IR/EM/Thermal	براساس PDK و Power Budget	Power Integrity Report

مرحله	خروجی‌های اجباری
پس از Macro Placement/Floorplan	Die/Core Utilization، Macro Placement، Macro Halo، Routing Channel، Congestion، Pad Feasibility، Memory Macro Feasibility، Area/PPA Risk
پس از CTS/Route	Timing Margin، Clock Skew/Jitter، Routing حساس، Shield Coverage، IR Drop، EM، DFT Isolation، DRC/LVS/ERC/Antenna/DFM Status
پیش از Tape-out	Final Sign-off، GDSII/OASIS، Tape-out Checklist، Risk Closure، PPA Report و Release Approval

هدف مساحت ترجیحاً کمتر از 8 mm^2 و سقف 12 mm^2 فقط پس از تأیید PDK، macroهای واقعی حافظه، Pad Ring، ESD، Floorplan، congestion، IR/EM و نتایج checkpointهای فوق قابل نهایی‌سازی است. این اعداد نباید پیش از اثبات feasibility به‌عنوان تعهد مطلق پذیرش شوند.

۳-۱۸- شرایط عملیاتی، توان و پکیج

تراشه باید در شرایط Brownout، Reset مکرر، قطع و وصل VCC، تغییر Clock، تغییر دما و رفتارهای غیرعادی Terminal، وارد وضعیت ناامن نشود. رفتار هر حالت باید در Reset Policy، Tamper Policy، NVM Recovery Policy و Test Plan تعیین شود.

حوزه	الزام
فرآیند ساخت	40^{nm} Mixed-Signal CMOS
ولتاژ کارت	Class B و Class C الزامی (Class A در صورت نیاز و قابلیت PDK)
دمای عملیاتی	-40 to 105°C
دمای نگهداری	-40 to 125°C
Data Retention	براساس macro واقعی و Reliability Target
Flash/NVM Endurance	براساس macro، ECC، wear-leveling و usage model
ESD/Latch-Up	مطابق PDK، Pad Library و Test Target
Standby Power	حداقل ممکن و مطابق پروفایل کارت
APDU Processing Power	منطبق با محدودیت جریان ISO-7816
Crypto Peak Power	در Power Budget و IR/EM لحاظ می‌شود.
Package	سازگار با ماژول کارت هوشمند
Die Thickness	سازگار با ماژول و فرآیند کارت
Bond Pad Map	الزامی
Wire-Bonding Guideline	الزامی
Smart-Card Embedding	الزامی
QFN Engineering Package	در صورت نیاز برای Bring-up و Characterization

۳-۱۹- زیرسیستم‌های پشتیبان، قابلیت اطمینان، آزمون‌پذیری و کنترل‌های امنیتی

تراشه باید دارای زیرسیستم‌های کنترلی، زمانی، حافظه‌ای، آزمون‌پذیری، توان، پکیج و امنیتی لازم برای عملکرد مطمئن به‌عنوان یک عنصر امن UICC باشد. طراحی این زیرسیستم‌ها باید با معماری امنیتی، ریشه اعتماد سخت‌افزاری، مدیریت چرخه‌حیات، مدیریت کلید، راه‌اندازی امن، کنترل دسترسی حافظه، حفاظت فیزیکی و سیاست‌های مقابله با حمله یکپارچه باشد.

هیچ قابلیت جانبی، از جمله DMA، Clock، Reset، Debug، DFT، ATE، Test Mode، Power Management یا رابط خارجی، نباید امکان دورزدن Root of Trust، Security Controller، Key Vault، Memory Firewall، Lifecycle Controller، Secure Boot یا Tamper Response را فراهم کند.

تمام الزام‌های این بخش باید در System Architecture، Security Architecture، Register Map، Threat Model، Verification Plan، DFT Plan، Physical Design Plan، Test Plan و Acceptance Test Plan قابل ردیابی باشند.

۳- ۲۰- مدیریت انتقال داده و DMA

وجود کنترل‌کننده دسترسی مستقیم به حافظه[۱](DMA) برای محصول پایه UICC الزامی نیست. استفاده از DMA تنها در صورتی مجاز است که نیاز آن در معماری، تحلیل توان، تحلیل عملکرد و برنامه آزمون توجیه شود.

در صورت استفاده از DMA، این زیرسیستم باید تحت کنترل سخت‌افزاری Security Controller، Memory Firewall و Lifecycle Policy قرار گیرد. DMA نباید به Key Vault، Key RAM، OTP/eFuse حساس، Protected NVM، Root-of-Trust Data، Security Register، Crypto Intermediate Data یا ناحیه‌های حافظه محدودشده دسترسی مستقیم داشته باشد.

قابلیت DMA	الزام
وجود DMA	اختیاری
کنترل دسترسی حافظه	الزامی
کنترل مبدا و مقصد انتقال	الزامی
محدودیت طول انتقال	الزامی
کنترل مالکیت انتقال	الزامی
کنترل privilege	الزامی
سیاست وابسته به Lifecycle	الزامی
قطع انتقال هنگام Tamper/Security Reset	الزامی
دسترسی به Key Vault یا Key RAM	ممنوع
امکان bypass کردن Memory Firewall	ممنوع
ثبت رویداد امنیتی	در صورت امکان معماری

۳- ۲۱- Java Card

برای افزایش ارزش تجاری تراشه، Java Card compatibility هدف قرار داده شود. شامل:

- Java Card runtime support
- applet isolation
- firewall

[۱] Direct Memory Access

- object protection
- secure object deletion
- APDU interface
- cryptographic APIs

اما Java Card را نباید به قیمت به خطر افتادن زمان پروژه یا silicon area به‌صورت uncontrolled توسعه داد. با توجه به پیچیدگی ذاتی Java Card Runtime Environment (JCRE) و محدودیت‌های زمان‌بندی پروژه، مجری مجاز است به جای پیاده‌سازی کامل این استانداردها از صفر (From Scratch)، از یکی از راهکارهای زیر استفاده نماید:

- استفاده از IP های تجاری یا Open-Source موجود (با ارائه مستندات Security Pedigree).
- استفاده از یک RTOS امن (Secure RTOS) و پیاده‌سازی یک لایه سازگاری (Compatibility Layer) که API های استاندارد Java Card را شبیه‌سازی کند.

شرط پذیرش: در هر صورت، محصول نهایی (Production Silicon) باید از نظر عملکردی (Functionally) قادر به اجرای Applet های استاندارد Java Card باشد. مجری موظف است در فاز Validation، اجرای حداقل دو Applet استاندارد و برقراری Secure Channel را روی First Silicon به اثبات برساند.

۳- ۲۲- GlobalPlatform

برای configurationهایی که Java Card/eSIM استفاده می‌کنند:

- GlobalPlatform card lifecycle
- Security Domain
- application loading
- application deletion
- secure channel
- key management
- application isolation

باید پشتیبانی شود. با توجه به پیچیدگی ذاتی GlobalPlatform (GP) و محدودیت‌های زمان‌بندی پروژه، مجری مجاز است به جای پیاده‌سازی کامل این استانداردها از صفر (From Scratch)، از یکی از راهکارهای زیر استفاده نماید:

- استفاده از IP های تجاری یا Open-Source موجود (با ارائه مستندات Security Pedigree).
- استفاده از یک RTOS امن (Secure RTOS) و پیاده‌سازی یک لایه سازگاری (Compatibility Layer) که Secure Channel های GlobalPlatform (SCP02/SCP03) را شبیه‌سازی کند.

شرط پذیرش: در هر صورت، محصول نهایی (Production Silicon) باید از نظر عملکردی (Functionally) قادر به مدیریت چرخه عمر مطابق با GlobalPlatform باشد. مجری موظف است در فاز Validation، اجرای حداقل دو Applet استاندارد و برقراری Secure Channel را روی First Silicon به اثبات برساند.

۳- ۲۳- OTA Update

تراشه باید امکان secure OTA update داشته باشد. باید شامل موارد زیر باشد:

- classical-signed, PQC-signed, or hybrid-signed firmware image according to lifecycle and security policy
- PQC algorithm identifier and parameter-set identifier
- cryptographic-agility metadata
- backward-compatible verification policy
- encrypted image where required
- anti-rollback
- version counter
- atomic commit
- recovery
- interrupted-update protection

۳- ۲۴- زمان‌سنج، Clock، Watchdog و Reset

تراشه باید دارای زیرسیستم زمان‌سنج، Watchdog و Clock مستقل باشد تا عملکرد ISO/IEC-7816، مدیریت timeout، کنترل عملیات امنیتی، تشخیص ناهنجاری clock و مقاومت در برابر حملات glitch فراهم شود.

Security Clock و Watchdog Clock نباید توسط فیرمور، application، DMA، Debug یا رابط خارجی غیرمجاز متوقف، bypass یا تغییر داده شوند. در صورت تشخیص Clock Glitch، Frequency Anomaly، Brownout یا Tamper Event، Security Controller باید مطابق سیاست امنیتی تعریف‌شده، عملیات حساس متوقف شده و تراشه وارد Secure Reset، Recovery یا حالت محدود شود.

زیرسیستم	الزام
General-Purpose Timer	حداقل دو عدد
ISO/IEC 7816 ETU Timer	الزامی
Protocol Timeout Timer	الزامی
Secure Watchdog	الزامی
Watchdog Clock مستقل	الزامی
Security Timer	الزامی
Monotonic Counter	الزامی
Timestamp Source	در صورت نیاز Audit یا Diagnostic
Internal Oscillator	الزامی
External Clock	در صورت نیاز profile یا معماری
Clock Divider	الزامی
Clock Monitor	الزامی

زیرسیستم	الزام
Clock Glitch Detector	الزامی
Frequency Anomaly Detection	الزامی
Security Clock	الزامی
Low-Power Clock	توصیه‌ای
Power-On Reset	الزامی
Brownout Reset	الزامی
Watchdog Reset	الزامی
Security Reset	الزامی
Tamper Reset	الزامی
Software Reset	الزامی
Host/Terminal Reset Handling	الزامی
Reset Isolation	الزامی

رویداد	حداقل واکنش
Power-On Reset	مقداردهی اولیه امن و اجرای Secure Boot Policy
Brownout	توقف عملیات حساس، بررسی وضعیت NVM و اجرای Recovery Policy
Watchdog Timeout	Reset کنترل‌شده و ثبت رویداد در صورت امکان
Clock Anomaly	Abort Operation یا Security Reset
Tamper Event	Abort، Zeroization volatile و Policy Escalation
Security Reset	توقف Crypto Operation، پاک‌سازی Key RAM و بررسی Lifecycle
Terminal Reset	رفتار سازگار با ISO/IEC 7816 بدون افشای داده حساس
Software Reset	فقط از مسیر مجاز و بدون bypass Security Controller

۳- ۲۵- ذخیره‌سازی امن و Anti-Tearing

تمام عملیات‌های حســـاس بر روی Flash/NVM باید در برابر قطع ناگهانی تغذیه، Brownout، Reset غیرمنتظره، خطای برنامه‌ریزی، حمله glitch، rollback و corruption مقاوم باشـــند. این الزام برای Lifecycle State، PIN/PUK Retry Counter، Anti-Rollback Counter، Firmware Update State، Key Metadata، Security Policy، Debug/DFT Lock State، Provisioning Data و داده‌های فایل‌سیستم آزمایشی ضروری است.

قابلیت	الزام
Atomic Update	الزامی
Anti-Tearing	الزامی
Power-Loss Recovery	الزامی
Interrupted Program/Erase Detection	الزامی
Journal/Transaction Record	الزامی برای اشیاء امنیتی حساس

قابلیت	الزام
Commit Marker	الزامی
Sequence Number	الزامی
Version/Epoch	الزامی
Integrity Value	الزامی
ECC	ECC / Parity |الزامی برای Key RAM و Boot ROM؛ برای Flash و SRAM عمومی مطابق macro ولی با الزام به پیاده‌سازی مکانیزم تشخیص خطا (Error Detection) در سطح کنترلر حافظه
Rollback Detection	الزامی برای Lifecycle، Update و Counter
Wear-Leveling یا Allocation Policy	الزامی برای داده‌های پرتغییر (توسط Secure File System یا FTL سخت‌افزاری/نرم‌افزاری)
Secure Zeroization برای SRAM/Key RAM	باید قابلیت Trigger سخت‌افزاری مستقل از CPU در صورت تشخیص Tamper را داشته باشد
Cryptographic Erase برای NVM	در صورت نیاز Threat Model
Key Invalidation	الزامی برای داده حساس رمزشده
Remanence Mitigation	الزامی برای داده volatile حساس

برای هر شـــیء امنیتی پایدار حســـاس، ســـاختار داده باید حداقل شـــامل Header، Object Type، Version/Epoch، Sequence Number، Payload، Integrity Value، Commit Marker، Access Policy و Recovery State باشد.

۳- ۲۶- قابلیت‌های مرجع UICC، PIN و APDU

پشته مرجع اعتبارسنجی باید قابلیت آزمون عملکردهای پایه UICC/SIM/USIM را فراهم کند. هدف این پشته، Bring-up، Functional Validation، آزمون ISO/IEC-7816، APDU testing، آزمون حافظه، آزمون Crypto Service، آزمون Lifecycle و اعتبارسنجی آزمایشگاهی در شبکه است.

پشته مرجع اعتبارسنجی (Bring-up & Validation Stack): مجری موظف است یک پشته نرم‌افزاری حداّقلّی اما عملیاتی (Minimal Operational Stack) را برای فاز Bring-up، Functional Validation و آزمون‌های اولیه شـبکه ارائه نماید. تذکر مهم: این پشته صرفاً جهت تسریع فاز Validation است و مجری را از الزامات بخش‌های ۳,۲۱ (Java Card) و ۳,۲۲ (GlobalPlatform) و ۳,۵ (Secure OS) برای محصول نهایی (Production Silicon) معاف نمی‌کند. محصول نهایی باید شامل JCRE، GlobalPlatform و Card OS کامل باشد.

قابلیت	وضعیت در Scope پایه
APDU Parser (CLA/INS/P1/P2/Lc/Le)	الزامی
APDU کوتاه و توسعه‌یافته	الزامی
Status Word & ISO/IEC 7816 Transport	الزامی
T=0 و T=1 Test Flow	الزامی
فایل‌سیستم آزمایشی MF/DF/ADF/EF))	بصورت حداّقلی الزامی است
USIM Application (AKA/Milenage)	الزامی (برای تست شبکه)
PIN1/PIN2/PUK/ADM & Retry Counter	الزامی
Logical Channel	در صورت نیاز Test Profile
Secure Messaging (SCP02/03)	الزامی (برای تست‌های ETSI)
UICC Card OS	الزامی (Full OS)
JCRE / GlobalPlatform	الزامی (کامل و آزمون‌شده)

PIN، PUK، ADM Credential، Retry Counter و داده‌های حساس آزمایشی نباید به‌صورت متن آشکار (Plaintext) یا بدون حفاظت Integrity در حافظه باقی بمانند. داده‌ها و کلیدهای آزمایشـــی باید از کلیدهای واقعی تولید، Root Key و داده مشترکین واقعی تفکیک شوند. استفاده از کلیدهای Production در فاز Validation یا برعکس، ممنوع بوده و مجری مسئول هرگونه نشت اطلاعات ناشی از این اشتباه خواهد بود.

۳- ۲۷- جداسازی دامنه‌های امنیتی

معماری باید امکان جدا سازی دامنه‌های اجرایی، داده‌ای، کلیدی و حافظه‌ای را فراهم کند. این جدا سازی نباید صرفاً مبتنی بر قرارداد نرم‌افزاری باشـــد و باید در ســـطح Memory Firewall، MPU/PMP، Secure Bus، Lifecycle Policy، Key Manager و Security Controller قابل اعمال و قابل آزمون باشد.

دامنه معماری	هدف
Boot and Root-of-Trust Domain	Boot ROM، Root Key/Hash و Secure Boot Policy
Security Management Domain	Lifecycle، Tamper، Debug، Reset و Security Policy
Key and Crypto Domain	Key Vault، Key RAM، Crypto Engine و Intermediate Data
Secure NVM Domain	Lifecycle Metadata، Counter، Update State و Security Object
Firmware Runtime Domain	Firmware پایه، HAL و Driverهای مجاز
APDU/Test Domain	APDU Stack، Test Provisioning و Validation Service

دامنه معماری	هدف
Debug/DFT Domain	Debug، Scan و Test با کنترل Lifecycle
Future Card OS Domain	قابلیت معماری برای Card OS آینده
Future Java Card Domain	قابلیت معماری برای Java Card/JCRE آینده
Future GlobalPlatform Domain	قابلیت معماری برای GlobalPlatform آینده
Future eUICC Domain	قابلیت معماری برای eUICC آینده

۳-۲۸- Secure Debug، DFT و ATE Readiness

Debug و DFT برای توسعه، تحلیل خرابی، افزایش yield و آزمون تولید ضروری هستند؛ اما نباید به مسیر استخراج کلید یا bypass کنترل‌های امنیتی تبدیل شوند.

حالت چرخه‌حیات	وضعیت Debug	محدودیت
Manufacturing	فعال و محدود	فقط عملیات کارخانه و بدون کلید تولیدی
Test	فعال و کنترل‌شده	فقط با Test Credential و ثبت رویداد
Development	فعال و احراز هویت‌شده	مطابق Development Policy
Provisioning	محدود	فقط برای Test Provisioning مجاز
Operational	غیرفعال یا کنترل رمزنگاری‌شده	بدون دسترسی به داده یا کلید حساس
Locked	غیرفعال	بدون مسیر Debug
RMA	محدود و policy-controlled	بدون export کلید یا داده حساس

قابلیت DFT/ATE	الزام
Scan	الزامی
MBIST	الزامی
SRAM Test	الزامی
ROM Test	الزامی
Flash/NVM Test	الزامی
Stuck-at Test	الزامی
Transition Fault Test	الزامی
At-Speed Test	در صورت نیاز DFT Flow
DFT Lifecycle Control	الزامی
DFT Security Review	الزامی
Wafer Sort Test Specification	الزامی
Final Test Specification	الزامی

قابلیت DFT/ATE	الزام
Test Limit Table	الزامی
Binning Specification	الزامی
Traceability Specification	الزامی
Source/Pattern یا ATE Program	طبق RACI مصوب
ISO/IEC 7816 Electrical Test	الزامی
Crypto Functional Test	الزامی
TRNG Health Test	الزامی
Lifecycle/Debug Lock Test	الزامی
Tamper Test	متناسب با Threat Model
IDDQ Test	در صورت امکان فرآیند و Test Flow

در حالت عملیاتی، هیچ مسیر Scan، Debug، Test Register، MBIST Control، Memory Test Mode یا DFT Interface نباید دسترسی به Key Vault، Key RAM، Protected NVM، OTP حساس، Security Register، Lifecycle State یا Crypto Intermediate Data فراهم کند.

۳- ۲۹- شاخص‌های عملکرد، PPA و معیارهای پذیرش

عملکرد محصول باید تحت شرایط آزمون تعریف شده، شامل نسخه PDK، گوشه فرآیند/ولتاژ/دما (PVT Corner)، ولتاژ تغذیه، فرکانس پردازنده مرکزی، نسخه فیرمور، وضعیت چرخه‌حیات، نوع پکیج و Test Profile اندازه‌گیری شود. هیچ شاخص عملکردی بدون تعریف محیط آزمون مبنای پذیرش نخواهد بود.

شاخص	وضعیت	روش تعیین یا پذیرش
فرکانس پردازنده مرکزی	هدف ۳۰ تا ۵۰ مگاهرتز	پس از STA و PVT Sign-off
زمان Boot تا آماده‌بودن APDU	تعیین در Architecture Freeze	Boot Test روی First Silicon
زمان ATR	مطابق ISO/IEC-7816 و Profile	Terminal Interoperability Test
زمان PPS	مطابق ISO/IEC-7816 و Profile	Protocol Test
زمان پردازش APDU	براساس APDU Test Set	APDU Benchmark
زمان AES/SHA/HMAC/KDF	براساس Test Vector	Crypto Benchmark
زمان تولید TRNG/DRBG	براساس Entropy/DRBG Policy	TRNG Characterization
زمان Secure Update	براساس Image Size و Profile	Update Test
زمان Recovery پس از به‌روزرسانی ناقص	تعیین در Test Plan	Power Interruption Test

شاخص	وضعیت	روش تعیین یا پذیرش
زمان Recovery بعد از Brownout	تعیین در Test Plan	Brownout Test
زمان Zeroization Key RAM	تعیین در Security Architecture	Tamper/Security Reset Test
توان Standby	تعیین در Power Budget	Silicon Measurement
جریان APDU	مطابق ISO/IEC-7816	Electrical Test
Crypto Peak Current	تعیین در Power Budget	Silicon Test و IR/EM
ظرفیت مفید Flash	براساس Usable Capacity	Memory Report و Software Footprint
مساحت Die	پس از Floorplan و Sign-off	Final PPA Report
Yield/DFT Coverage	طبق برنامه DFT/ATE	ATE/DFT Report

۴ - خروجی‌ها و موارد تحویلی مورد انتظار

تمام اقلام این فصل باید با مرز دامنه مصوب در فصل‌های یک تا سه این مستند سازگار باشند. تحویل‌های پایه شامل سیلیکون، RTL، فیرمور پایه، HAL، driver، نرم‌افزارها و پشته مرجع اعتبارسنجی، ابزارهای آزمون آزمایشگاهی، اسناد طراحی، شواهد verification و بسته انتقال مهندسی است.

۴- ۱- اصول حاکم بر تحویل، نسخه‌بندی و پذیرش

کلیه خروجی‌های پروژه، شامل اسناد، RTL، فیرمور، نرم‌افزار، محیط آزمون، نتایج verification، databaseهای طراحی فیزیکی، بسته Tape-out، نتایج Bring-up، گزارش‌های امنیتی، ابزارها و مستندات، باید کامل، نسخه‌دار، قابل ردیابی، قابل بازتولید و قابل پذیرش باشند. هر خروجی باید دارای شناسه یکتا، نسخه، مسؤول فنی، وابستگی‌ها، معیار پذیرش، Release Note، محدودیت‌های شناخته‌شده و ارتباط با Requirement/Compliance Matrix باشد.

موضوع	الزام
شناسه، نسخه وRelease Tag	الزامی
Change Log، Known Issue وErrata	الزامی
Tool/PDK Version Manifest	الزامی
IP/License Manifest	الزامی
Release Manifest،Artifact Hash	الزامی
Build/Rebuild Instruction	الزامی
Requirement/TestتاTraceability	الزامی
معیار پذیرش و گزارش نتیجه	الزامی

۴- ۲- خروجی‌های نیازمندی، معماری و امنیت

مجری باید پیش از Architecture Freeze، مجموعه اسناد baseline شامل SRS، Compliance Matrix، Requirements Traceability Matrix، System/Hardware/Security Architecture، Trust Boundary، Data/Key Flow، Threat Model، Security Target Draft، TOE Description، TSS Draft، Memory/Register Map، Clock/Reset/Power Architecture، Lifecycle/Debug/DFT Policy، PPA Budget، PDK Acceptance Report، Risk Register و Change-Control Record را تحویل و برای تصویب ارائه کند.

۴- ۳- خروجی‌های سخت‌افزار، RTL و IP

تحویل‌های این بخش شامل RTL/HDL کامل، RTL Hierarchy، Micro-Architecture Specification، Register Definition، Memory Initialization، IP Manifest، Third-Party IP/License List، Configuration/Parameter Files، SDC و سایر Constraints، scripts ساخت و شبیه‌سازی، Lint/CDC/RDC/Formal Configuration، Netlist، Tool Version Manifest و Artifact Hash Manifest است.

۴- ۴- خروجی‌های فیرم‌ور، نرم‌افزار و پشته مرجع اعتبارسنجی

مورد	وضعیت	توضیح
Boot ROM Source/Image	الزامی	مطابق معماری Root of Trust، Anti-Rollback و PQC-Hybrid Verification.
Secure Bootloader و فیرم‌ور پایه	الزامی	Bring-up، Recovery و کنترل کامل زیرسیستم‌های امنیتی.
HAL و Device Driverها	الزامی	درایورهای کامل برای Clock/Reset/NVM/Crypto/TRNG/Tamper/ISO7816.
UICC Card OS (Secure OS)	الزامی (کامل)	سیستم‌عامل کامل و عملیاتی. (تبصره: مجری مجاز است برای لایه Kernel از یک Secure RTOS استاندارد استفاده کند، اما لایه‌های UICC Middleware، File System و APDU Dispatcher باید اختصاصی و کامل باشند).
SIM/USIM Application Stack	الزامی (کامل)	پیاده‌سازی کامل استانداردهای GPP/ETSI۳ برای احراز هویت در شبکه‌های ۲G/4G/5G شامل AKA/Milenage و SUCI).
Java Card Runtime (JCRE)	الزامی (کامل)	قابلیت اجرای امن Appletهای استاندارد و Applet Isolation. (تبصره: جهت مدیریت ریسک، مجری مجاز به استفاده از IP تجاری/Open-Source یا لایه سازگاری (Compatibility Layer) است، مشروط به پاس کردن آزمون‌های انطباق).
GlobalPlatform Services	الزامی (کامل)	Card Manager، Secure Channel (SCP02/03)، Application Loading/Deletion و مدیریت چرخه عمر.
Crypto، Secure Update و Secure Storage	الزامی	سرویس‌های کامل رمزنگاری (کلاسیک و PQC)، Secure OTA Update و Secure File System با Anti-Tearing.
APDU/ISO 7816 Engine	الزامی	پردازش کامل APDU، Logical Channels، Secure Messaging و Status Words.
Test Tools & PC/SC SDK	الزامی	ابزارهای سمت هاست (Host-side) برای Bring-up، Characterization و تست‌های اولیه.
Personalization/HSM/OTA Server	خارج از دامنه	زیرساخت عملیاتی سمت سرور. (فقط پیاده‌سازی API و پروتکل‌های استاندارد سمت تراشه برای اتصال به این سرورها الزامی است).

۴- ۵- شبیه‌ساز سخت‌افزاری، FPGA و ابزارهای توسعه

مجری باید موارد زیر را به عنوان ابزارهای Bring-up، Validation و توسعه تحویل دهد: Software Emulator / Virtual Card، FPGA Prototype قابل پیکربندی، FPGA Image، Source Code و Build Instructions، Regression Automation Scripts، Test Vectorها، Sample Scriptها، Diagnostic/Logging Tool، APDU Test Tool، و یک Virtual Card / PC-SC test environment کامل.

همچنین مستندات فنی شامل TRM (Technical Reference Manual)، Security Target (ST) / Secure Design Document، API Reference، Datasheet و راهنماهای کاربر باید ارائه شوند.

Emulator و FPGA صرفاً ابزارهای Bring-up و Validation منطقی هستند و به هیچ وجه جایگزین اثبات روی سیلیکان (Silicon Proof) برای ویژگی‌های آنالوگ و فیزیکی شامل eNVM (Anti-Tearing/Endurance)، TRNG آنالوگ (AIS31)، SCA (Side-Channel Analysis)، Tamper Detection، Physical Fault Injection و Contactless AFEدر صورت پیاده‌سازی) نخواهند بود.

۴- ۶- خروجی‌های Verification، UVM و آزمون نرم‌افزار

مجری باید کلیه خروجی‌های فرآیند Verification و Validation را به صورت مستند و قابل ردیابی تحویل دهد. این موارد شامل:

- سخت‌افزار و RTL: Verification Plan، UVM Environment، Unit/Subsystem/SoC Testbench، Directed و Constrained-Random Test، Assertionها، Coverage Plan/Database/Report، Lint، CDC/RDC، X-Propagation، و Formal Property/Result.
- نرم‌افزار و امنیت: Crypto KAT/Negative Test، Software Unit/Integration Test، Firmware Regression، APDU/Protocol Fuzzing، و Lifecycle/Debug/DFT Lock Test.
- مستندات و ردیابی:
  - Traceability Matrix: ماتریس ردیابی کامل از Requirement و Threat Model و SFRها (Security Functional Requirements)تا Testcase و Result نهایی.
  - Security Evaluation Reports: گزارش‌های جامع و مستند از کمپین‌های Side-Channel Analysis (SCA)، Fault Injection (FI) و Penetration Testing.
  - Security Verification Report: سند نهایی که وضعیت انطباق تمامی الزامات امنیتی و عملکردی را با استناد به نتایج تست‌ها تایید می‌کند.

۴- ۷- خروجی‌های DFT، سنتز و طراحی فیزیکی

مجری باید DFT Plan، Scan/MBIST/Memory-Test Architecture، DFT Security Review، Wafer Sort و Power، Macro Placement، Floorplan، Synthesis/STA scripts and reports، Final Test Specification Floorplan Security، DRC/LVS/ERC/Antenna/DFM، IR/EM، Congestion، Routing، CTS، Plan Review، CTS/Route Physical-Security Review، LEF/DEF، GDSII/OASIS، Tape-out Checklist و Final Sign-off Package را تحویل دهد.

۴-۸- خروجی‌های Tape-out، ATE، Bring-up و Silicon Validation

مجری مسؤول تهیه Tape-out-ready package، پاسخ فنی به Foundry Query، Waiver Analysis، ATE Source/Pattern یا Program طبق RACI، Test Limit/Binning/Traceability Specification، Package/Bond Guideline، Bring-up Plan/Checklist، Firmware Image، Characterization Plan/Report، ISO-7816 Electrical Report، TRNG/Crypto/Lifecycle/Debug-Lock Report، Silicon Errata و Corrective Action Plan است. ساخت wafer، تأمین نمونه، OSAT و اجرای ATE مطابق RACI بر عهده کارفرما یا مرکز منتخب خواهد بود.

۴-۹- خروجی‌های ارزیابی امنیت و Common Criteria Readiness

مجری باید Security Architecture، Threat Model، Asset Classification، Security Target Draft، TOE/TSS، Secure Boot/Lifecycle/Key Isolation/Memory Security/Debug-DFT، Assurance Evidence Plan Post-Silicon Security، Penetration-Test Plan، SCA/FI Countermeasure Report، Assessment Evaluation Plan، Vulnerability Analysis، Residual Risk Report و در صورت فعال‌سازی PQC، PQC Compliance Matrix، KAT، Benchmark و Crypto-Agility Test را تحویل دهد.

۴-۱۰- مستندات فنی، Datasheet و راهنماهای کاربر

مجری باید Datasheet اولیه و نهایی، TRM، Programming/Reference Manual، Hardware Integration Guide، Test/ATE Guide، Debug/DFT Guide، Security Guide، Firmware/Boot/Update Guide Test، Sample Code، API Reference، SSDP، FPGA/Emulator User Guide، Package/Bonding Guide Artifact Hash Manifest، Tool/PDK Version Manifest، SBOM، Release Guide، Vector Guide Build/Rebuild Instruction، Change Log و Errata را تحویل دهد.

۴-۱۱- بسته انتقال مهندسی به تولید

بسته انتقال مهندسی به تولید (Engineering to Production Transfer Package) شامل کلیه artefactهای طراحی، Tape-out، فیرمور، آزمون، ATE، پکیج، امنیت، مستندات، versioning و کیفیت لازم برای نمونه‌سازی، تولید آزمایشی (Pilot Run) یا تولید انبوه (Mass Production) است.

این بسته شامل راه‌اندازی و بهره‌برداری از زیرساخت‌های سمت سرور نظیر Personalization تجاری، HSM عملیاتی، KMS تولیدی، OTA Platform، eUICC RSP، SM-DP+ یا SM-DS نمی‌باشد؛ مگر آنکه در قرارداد یا بسته کاری (SOW) مستقل دیگری تصریح شده باشد

گروه	خروجی
طراحی	RTL، Netlist، Constraints، Scripts، IP Manifest و Database، Memory Compiler Models
Tape-out	GDSII/OASIS، Sign-off، Checklist و Waiver Record
Firmware	Source، Binary، Build، Release و Secure Update Guide
آزمون	UVM/Regression، Test Vector، ATE Pattern/Program و Test Limit و Loadboard/Probe Card Specs
تولید	Wafer Sort/Final Test، Binning و Traceability، Key Injection/Provisioning Guide
پکیج	Pad Map، Bonding Guide و Smart-Card Module Guide
امنیت	Threat Model، Key/Lifecycle Policy و Security Report، Secure Debug Lock Procedure
مستندات	TRM، Datasheet، Integration/Test/User Guides
کیفیت	Characterization Report ،Errata، Known Issue، Corrective Action و Final Acceptance

۵ - زمان‌بندی اجرا

برای اجرای طرح **حدّاکثر ۲ سال** پیش‌بینی شده است:

فاز	مدت
Requirements & Architecture	۱,۵ ماه
Security Architecture	۱,۵ ماه
RTL + Firmware + UICC Software	۷ الی ۸ ماه
Verification + Security + PQC validation	۶ الی ۷ ماه
Physical Design	۲,۵ ماه
Tape-out preparation	۱ ماه
Silicon fabrication	۴ الی ۵ ماه
Packaging + ATE	۱,۵ ماه
First Silicon Bring-up	۱,۵ ماه

۶ - ترکیب پیشنهادی تیم اجرایی طرح

تعیین ترکیب و اعضای گروه برعهده مجری و طبق نظر و تشخیص مجری خواهد بود. لیکن بدون هیچ الزامی پیشنهاد می‌شود گروه اجرای طرح شامل افراد زیر باشد:

تخصص	تعداد نفرات
Project Manager	۱
SoC/System Architect	۱
Security Architect	۲
CPU/SoC RTL	۲
Crypto RTL	۲
Memory/Security Controller RTL	۲
UICC/ISO 7816 Hardware	۱
Verification	۴
Formal/Security Verification	۲
Firmware/Secure OS	۳
SIM/USIM Software	۳
Physical Design	۳
DFT/ATE	۲
Security Evaluation	۲
Documentation/QA	۱
PQC Cryptography Engineer	۱
مجموع	۳۲ نفر

۷ - 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 غیره)، مخابرات و ارتباطات (سیم‌کارت‌های نسل جدید، تلفن همراه و غیره)، پولی و بانکی (کیف پول سخت‌افزاری، پرداخت و غیره) 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
	ارائه ضمانت برای تأمین مالی، شرکت در مناقصه و ...
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

۸ - مالکیت معنوی

مالکیت کلیه دستاوردها و خروجی‌های فنی و علمی پروژه (شامل کدهایHDL ، بلوک‌هایIP ، طرح فیزیکیGDSII ، اسرار فنی، مســـتندات و ...) متعلق به طراح خواهد بود، لکن طراح ملزم به همکاری با مرکز ملی پیشـــران طراحی تراشـــه و ارائه اطلاعات و مستندات لازم (به عنوان دارایی‌های تحت تملک خود) جهت ثبت در بانک دارایی‌های فکری تراشه خواهد بود.