بسمه‌تعالی

درخواست طرح پیشنهادی (RFP)

طراحی و تجاری‌سازی تراشه Security Element

برای کاربرد در حوزه

اسناد هویتی و کارت‌های هوشمند

مرکز ملی پیشران طراحی تراشه
National Chip Design Center

شهریور ۱۴۰۵

۱- مقدمه

این سند، RFP طراحی و توسعه یک تراشه امن بومی برای استفاده در اسناد هویتی الکترونیکی (گذرنامه و کارت ملّی) و کارتهای هو شمند را تعریف میکند. مح صول مورد نظر یک Secure Element/Smart-Card SoC کامل ا ست و صرفاً یک IP Core یا شتابدهنده رمزنگاری نی ست. تراشه باید مجموعه سختافزار امنیتی، پردازنده، حافظه، رابطهای تماس و بدون تماس، شتابدهندههای رمزنگاری، کنترلهای ضد دستکاری و نرمافزارهای پایه مورد نیاز برای اجرای سی ستم عامل امن کارت و کاربردهای هدف را فراهم کند. این سند مرجع همچنین بر پ شتیبانی از ام ضای دیجیتال، شناسایی/تصدیق هویت، Java Card/Native OS، PACE+EAC، ISO/IEC 7816، ISO/IEC 14443، الگوریتمهای RSA/ECC، رمزنگاری متقارن، SHA و رمزنگاری پساکوانتومی تأکید دارد.

Secure Elementها ریزترا شههای مقاوم در برابر حمله ه ستند که وظیفه آنها تولید، نگهداری، مدیریت و ا ستفاده از کلیدهای رمزنگاری و اجرای عملیات امنیتی به‌گونه‌ای است که حتی در صورت دسترسی کامل مهاجم به دستگاه، اسرار امنیتی قابل ا ستخراج نبا شند. فرض کنید یک کلید خ صو صی RSA یا ECC را داخل حافظه فلش یک میکروکنترلر معمولی ذخیره کنید. اگر مهاجم بتواند Firmware را بخواند، یا از حافظه Dump بگیرد، یا از طریق JTAG به پردازنده متصل شود، یا با حملات فیزیکی به تراشه د سترسی پیدا کند، می‌تواند کلید خصو صی را ا ستخراج کند. پس امنیت کل سیستم از بین می‌رود. ایده Secure Element این است که کلیدها هرگز از محیط امن خارج نشوند. مهمترین وظایف SEها عبارتند از:

۱. تولید کلیدهای رمزنگاری: SE معمولاً دارای یک TRNG (True Random Number Generator) داخلی است. از این TRNG برای تولید AES Keys، RSA Keys، ECC Keys، Session Keys، و Root Keys استفاده می‌شود. ویژگی مهم این است که کلیدها داخل خود تراشه تولید می‌شوند و از بیرون وارد نمی‌شوند، مگر در فرآیندهای امن مانند .Key Injection

۲. نگهداری امن کلیدها: نگهداری امن کلیدها مهم‌ترین وظیفه SE است. کلیدها در حافظه‌ای ذخیره می‌شوند که توسط CPU اصلی قابل خواندن نیست، از طریق JTAG قابل استخراج نیست، با میکروسکوپ الکترونی نیز به‌سختی قابل بازیابی است، و در صورت تشخیص حمله ممکن است به‌طور خودکار پاک شوند.

۳. اجرای عملیات رمزنگاری: هدف ا صلی SE این نی ست که سریع‌ترین موتور رمزنگاری با شد؛ هدف ا صلی آن این است که عملیات رمزنگاری را بدون افشای کلیدهای محرمانه انجام دهد. بنابراین، تفاوت اصلی بین یک Crypto Accelerator در SoC و یک Secure Element این ا ست که Crypto Accelerator برای سرعت طراحی شده ا ست. ولی Secure Element برای امنیت طراحی شده ا ست. فرض کنید CPU ا صلی نیاز به ام ضای یک پیام دارد. به‌جای دریافت کلید خصوصی، فقط پیام را به SE ارسال می‌کند. SE با کلید خصوصی امضای دیجیتال را ساخته و به CPU ارسال میکند. در این فرآیند کلید خصوصی هیچ‌وقت از SE خارج نمی‌شود. CPU هرگز کلید خصوصی را نمی‌بیند و تنها نتیجه (Signature) را دریافت می‌کند.

۴. احراز هو یت (Authentication): بیش از ۹۰٪ عملیات یک Secure Element در عمل به نوعی احراز هویت مربوط می شود. SE می‌تواند ثابت کند که این د ستگاه ا صل ا ست، یا این سیم‌کارت معتبر ا ست، یا این خودرو

متعلق به مالک اســت، یا این POS جعلی نیســت. به عبارت دیگر، SE ثابت می‌کند که "من همان دســتگاه، کارت یا کاربر اصلی هستم"، بدون اینکه راز (کلید خصوصی) را فاش کند.

۵. ایجاد Root of Trust: Root of Trust کوچک‌ترین مجموعه ســخت‌افزار و نرم‌افزار اســت که ذاتاً مورد اعتماد فرض می‌شود و امنیت کل سیستم بر آن بنا می‌شود. به بیان ساده‌تر Root of Trust اولین موجودیتی است که هیچ‌کس آن را تأیید نمی‌کند، بلکه خودش مبنای اعتماد به همه اجزای دیگر است. تقریباً تمام سیستم‌های امن از یک ریشــه اعتماد (Root of Trust) شــروع می‌شــوند. Secure Element معمولاً این نقش را ایفا می‌کند و تمام زنجیره اعتماد از آن آغاز می‌شــود. داخل SE معمولاً این موارد نگهداری می‌شــوند: Root Public Key، Device Private Key، Manufacturer Key، Certificate Chain، و Device Certificate. همه این‌ها پایه اعتماد سامانه هستند.

۶. Secure Boot: اگر در زمان راه‌اندازی ســامانه، کســی بتواند ســامانه را با firmware خود راه‌اندازی کند، به راحتی کنترل تمام سامانه را در دست خواهد داشت. SE با بررسی firmware تأیید میکند که آیا firmware دستکاری شده است یا خیر. اگر دستکاری شده باشد، مانع اجرای آن و راه‌اندازی سامانه با آن می‌شود.

۷. مدیریت چرخه عمر کلیدها: SE وظایفی مانند ایجاد کلید، تمدید، تعویض، حذف، و نابودی آنها در شــرایط اضطراری را انجام می‌دهد.

۸. مقابله با حملات فیزیکی: این ویژگی مهم‌ترین تفاوت SE با یک MCU معمولی اســت. به عنوان مثال: مهاجم ممکن ا ست برای چند نانوثانیه ولتاژ را از ۱/۲ ولت به ۰/۷ ولت کاهش دهد تا برر سی رمز عبور از کار بیفتد، یا به‌جای کلاک ۱۰۰ مگاهرتز، یک پالس ب سیار کوتاه یا ب سیار سریع تزریق کند تا یک د ستور اجرا ن شود، یا با لیزر را روی یک رجیســتر خاص بتاباند تا یک بیت از ۰ به ۱ تغییر کند، یا هزاران بار عملیات AES را اجرا کند تا از روی تغییرات بسیار کوچک جریان م صرفی کلید AES را ا ستخراج کند، یا بدون تماس م ستقیم با تراشه با یک آنتن بسیار حســاس نشــت الکترومغناطیســی را اندازه‌گیری و تحلیل کند، یا پس از برداشــتن لایه محافظ تراشــه پروب‌های میکروسکوپی را روی باس داخلی قرار دهد تا داده‌های عبوری خوانده شوند. یک Secure Element در برابر حملاتی مانند حمله ولتاژی، حمله فرکانســی، حمله لیزری، تحلیل توان مصــرفی ((DPA/SPA، تحلیل الکترومغناطیسی ((EMA، تزریق خطا، و Probe کردن گذرگاه‌های داخلی مقاوم ا ست و به محض وقوع این حملات، داده‌های حساس را نابود کرده و اجازه انجام هیچ اقدامی را به سامانه نمی‌دهد.

حمله	نوع	توضیح
حمله ولتاژی (Voltage Attack)	فعال	تغییر عمدی ولتاژ تغذیه برای ایجاد خطا یا دور زدن بررسی‌های امنیتی.
حمله فرکانسی (Clock/Frequency Attack)	فعال	تغییر فرکانس یا شکل موج کلاک برای ایجاد خطا در اجرای دستورها.
حمله لیزری (Laser Fault Injection)	فعال	تاباندن پالس لیزر روی بخش خاصی از تراشه برای تغییر بیت‌ها یا ایجاد خطای محاسباتی.

حمله	نوع	توضیح
حمله نوری (Light Attack)	فعال	تاباندن نور شدید به تراشه (پس از برداشتن بسته‌بندی) برای تغییر رفتار ترانزیستورها یا ایجاد خطا.
تحلیل توان مصرفی (SPA/DPA)	غیرفعال	اندازه‌گیری جریان مصرفی تراشه و استخراج کلیدهای رمزنگاری از روی الگوی مصرف توان.
تحلیل الکترومغناطیسی (EMA/EM Analysis)	غیرفعال	اندازه‌گیری میدان‌های الکترومغناطیسی منتشرشده از تراشه برای استنتاج داده‌ها یا کلیدهای محرمانه.
تزریق خطا (Fault Injection)	فعال	ایجاد خطای عمدی در محاسبات (با ولتاژ، کلاک، لیزر، EMو ...) برای استخراج اطلاعات محرمانه یا دور زدن کنترل‌های امنیتی.
Probe کردن گذرگاه‌های داخلی (Bus Probing)	غیرفعال	اتصال پروب‌های بسیار ظریف به خطوط داخلی تراشه برای مشاهده داده‌ها، آدرس‌ها یا کلیدهای در حال انتقال.

در واقع هر جا که یک راز دیجیتال (Secret) وجود داشته باشد، احتمالاً به Secure Element نیاز است.

در نسل فناوری ۴۰ نانومتر میکس سیگنال، چنین تراشه‌ای معمولاً مساحتی در حدود 7 تا 10 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. مشخّصات کلّی تراشه هدف این طرح به شرح زیر است.

پارامتر	مقدار نهایی پیشنهادیRFP
Product	Secure Identity & Smart Card SoC
Technology	40nm Mixed-Signal CMOS
Primary applications	eID / National ID / ePassport / Digital Signature
Secondary applications	Multi-application card / token / IoT SE
CPU	32-bit Secure CPU, target ≥50MHz
Flash	1MB target
ROM	64KB
SRAM	≥32KB total
OTP/eFuse	≥256B
Contact	ISO/IEC 7816-3 T=0/T=1
Contactless	ISO/IEC 14443 A/B
SPI	Slave ≥2Mbps
RSA	up to 4096bit
ECC	ECDSA/EdDSA up to P-521 / Ed448؛ تبادل کلید ECDH/X25519/X448
Symmetric	AES-128/192/256 + legacy 3DES
Hash	SHA-2/3 + SHAKE
TRNG	AIS31 target

پارامتر	مقدار نهایی پیشنهادیRFP
PQC	ML-KEM/ML-DSA architecture; acceleration preferred
Tamper	Voltage/temperature/clock/light/glitch + active shield
PUF	Yes
Security assurance	CC EAL5+ readiness
Die area	Preferred ≤7mm²; target ≤8mm²; max 10mm² with justification
Temperature	-25°C to +85°C minimum target
Packages	Micro-module + QFN
First silicon	Target ~21 months
Team	~33 peak engineers

۲- ضرورت منشاء نیاز

زیرساخت اسناد هویتی الکترونیکی، گذرنامه، کارت ملی، کارتهای چندمنظوره و سامانه‌های امضای دیجیتال به یک ریشه اعتماد سختافزاری مستقل، قابل تولید و قابل ارزیابی نیاز دارد. وابستگی کامل به Secure Elementهای خارجی، علاوه بر موضوع مالکیت فناوری، میتواند مدیریت زنجیره تأمین، شخصی سازی، تأمین کلیدهای ریشه، کنترل چرخه عمر و امکان ارزیابی مستقل امنیت را محدود کند.

سند مرجع تصریح میکند که محصول برای شناسایی، تصدیق هویت و امضای دیجیتال، با تمرکز اولیه بر کارت از منظر صنعتی، هدف این طرح ایجاد یک محصول silicon قابل تولید، قابل شخصیسازی و قابل استفاده در خانوادهای از محصولات اسناد هویتی است؛ به نحوی که سختافزار، firmware، کتابخانه‌های رمزنگاری، سیستم عامل امن و ابزارهای توسعه/شخصی سازی به صورت یک زنجیره محصولی تحت کنترل کارفرما قرار گیرد.

طراحی و بومی‌سازی SE یک موضوع راهبردی (Strategic Technology) است، نه صرفاً یک پروژه نیمه‌هادی. زیرا:

- Root of Trust: ریشه اعتماد کل اقتصاد دیجیتال است. امروزه تقریباً تمام زیرساخت‌های دیجیتال بر یک Root of Trust سخت‌افزاری متکی هستند. اگر کشوری نتواند Root of Trust خود را طراحی کند، در عمل باید به Root of Trust کشور دیگری اعتماد کند. این یعنی اعتماد به: تراشه، معماری، کلیدها، فرآیند تولید، و ابزارهای شخصی‌سازی (Personalization). در نتیجه، استقلال امنیتی نخواهد داشت.
- وابستگی در زنجیره تأمین (Supply Chain)؛ وقتی تنها چند شرکت خارجی Secure Element تولید می‌کنند، با تحریم، توقف صادرات، کاهش ظرفیت تولید، یا بحران ژئوپلیتیکی، تولید تمام محصولات وابسته متوقف می شود. برخی از این محصولات عبارتند از: POS، کارت بانکی، کارت ملی، گذرنامه، eSIM، خودرو، کنتور هوشمند، و تجهیزات پزشکی. بنابراین Secure Element یک Single Point of Failure در زنجیره تأمین می‌شود.
- امنیت ملی: امروزه تقریباً تمام تجهیزات حساس دارای Root of Trust هستند. برای مثال: تجهیزات مخابراتی، ماهواره، رادیوهای نظامی، تجهیزات رمز، سامانه‌های فرماندهی، پهپاد، و تجهیزات فضایی، همگی متّکی بر RoT هستند. اگر Root of Trust خارجی باشد، حتی اگر هیچ Backdoor وجود نداشته باشد (که **بدیهی است که تمام SEهای خارجی backdoor دارند**)، دولت

استفاده‌کننده مجبور است به طراحی، فرآیند ساخت، آزمون و مدیریت کلیدهای آن اعتماد کند. برای هیچ کشور بواقع مستقل یا مقتدری، این وابستگی در سامانه‌های حساس قابل قبول نیست.

- اقتصاد دیجیتال: بدون Secure Element داخلی، بسیاری از صنایع وابسته می شوند. از جمله صنایعی که برای استقلال بنیادین خود به SE نیازمند هستند می‌توان به بانکداری، پرداخت، eSIM، IoT، خودرو، دولت الکترونیک، SIM card، و ... اشاره کرد. بنابراین بدون SE بومی بخش بزرگی از ارزش افزوده به خارج منتقل می‌شود.
- استقلال فناوری: Secure Element صرفاً یک تراشه نیست. بلکه مجموعه‌ای از فناوری‌هاست: معماری امنیتی، رمزنگاری سخت‌افزاری، طراحی مقاوم در برابر حملات جانبی، TRNG، Secure Boot، مدیریت کلید، اخذ گواهی‌های امنیتی. وقتی کشوری این فناوری را توسعه دهد، همان دانش در بسیاری از پروژه‌های دیگر نیز قابل استفاده خواهد بود.
- اهمیت برای صنعت دفاعی: تقریباً همه سامانه‌های مدرن دفاعی به نوعی Root of Trust نیاز دارند. به عنوان مثال می‌توان به سامانه‌های زیر اشاره کرد: لینک‌های داده امن، رادیوهای تاکتیکی، پهپادها، تجهیزات جنگ الکترونیک، سامانه‌های فضایی، سامانه‌های شناسایی دوست از دشمن (IFF)، و تجهیزات کنترل دسترسی. بنابراین فناوری Secure Element می‌تواند یک فناوری پایه برای بسیاری از سامانه‌های دفاعی باشد.
- تاب‌آوری (Resilience): اگر یک کشور مالک IP امنیتی خود باشد، می‌تواند Foundry را تغییر دهد، می‌تواند Node فناوری را تغییر دهد، می‌تواند بسته‌بندی را تغییر دهد، و می‌تواند تأمین‌کننده را تغییر دهد. در حالی که اگر فقط مصرف‌کننده یک تراشه خارجی باشد، این انعطاف را ندارد.

Security Subsystem IP Platform مهم‌تر از یک تراشه است چون اگر ما مثلاً فقط یک تراشه برای POS طراحی کنیم، بازار آن محدود است. اما اگر یک Security Subsystem IP Platform توسعه دهید، همان فناوری می‌تواند در ده‌ها نوع تراشه استفاده شود. در این حالت فقط یکبار توسعه انجام می‌شود. لیکن بارها مورد استفاده قرار می‌گیرد، هزینه توسعه سر شکن می شود، گواهی‌های امنیتی قابل استفاده مجدد هستند، نگهداری ساده‌تر می شود، یک IP Platform می‌تواند صدها بار لایسنس شود و در ده‌ها خانواده SoC استفاده شود یا به شرکت‌های مختلف فروخته شود یا به نسل‌های مختلف فناوری (nm۴۰، nm۲۲، nm۱۲ و...) منتقل شود. به همین دلیل ارزش اقتصادی IP معمولاً از یک محصول منفرد بیشتر است.

شرکت	مهم‌ترین محصولات	بازارهای اصلی	جایگاه

Infineon Technologies	SLE78 ،SLC38 ، OPTIGA	ePassportبانک، ، IoT ،TPMخودرو،	رهبر بازار امنیت سخت‌افزاری
NXP Semiconductors	SmartMX ،EdgeLock SE050 ،SN100	بانک، موبایل، خودرو، NFC	NFC رهبر پرداخت و
STMicroelectronics	ST31 ،ST33 ،ST54	، موبایل، eSIM ،POS IoT	یکی از سه بازیگر اصلی
Thales	eSIM Secure IC ،eSE	مخابرات، دولت، پرداخت	eSIM رهبر و خدمات امنیتی
Microchip Technology	ATECC608 ،TA100	، خودرو، صنعتIoT	Secure رهبر سبک Element
Samsung Electronics	S3K eSE	موبایل	عمدتاً مصرف داخلی
Renesas Electronics	Automotive Security IC	خودرو	قوی در خودرو
IDEMIA	eSIM Platform	دولت، مخابرات	بیشتر یکپارچه‌ساز و ارائه‌دهنده راهکار
Giesecke+Devrient	eSIM ،Banking SE	بانک، دولت، مخابرات	رهبر شخصی‌سازی و کارت‌های هوشمند

۳- هدف و الزامات فنّی فراخوان

CPU امن ۳۲ بیتی (در طراحی پردازنده امن الزام اصلی این است که محرمانگی، تمامیت، جداسازی دامنه‌های امنیتی و مقاومت در برابر حملات فیزیکی و نرم‌افزاری در معماری پردازنده و مسیر حافظه به‌صورت یکپارچه پیاده‌سازی شود. پردازنده باید یک ریشه اعتماد سخت‌افزاری برای بوت امن، احراز اصالت کد و مدیریت کلید داشته باشد و از secure boot ، به‌روزرسانی امن، قفل‌کردن حالت debug و کنترل دقیق دسترسی پشتیبانی کند. در سطح معماری، MPUبرای محدودسازی دسترسی نواحی حافظه، SAU یا مکانیزم معادل برای جداسازی Secureو Non-secure world، و کنترل‌های privilege باید وجود داشته باشند. برای کارت هوشمند، پشتیبانی از وقفه‌های امن، جلوگیری از نشت اطلاعات از رجیسترها و باس‌ها، پاک‌سازی امن داده‌های حساس، مدیریت خطا و ثبت رویدادهای امنیتی نیز ضروری است. افزون بر این، معماری باید در برابر fault injection، glitch، probing، حملات زمان‌بندی، تحلیل توان و الکترومغناطیس و حملات cache یا speculative execution مقاوم باشد؛ بنابراین طراحیconstant-time ، کنترل دسترسی بدون نشت، masking و متعادل‌سازی مسیرهای توان در بخش‌های حساس اهمیت دارد.

علاوه بر پردازنده؛ بخش حافظه امن شامل ROM، SRAM، NVM، مورد نیاز است.

مجموعه ای از ماجول های امنیتی شـــامل AES، RSA، ECC، SHA، TRNG، Key Manager، Tamper Detection (از جمله تشخیص حملات فیزیکی نظیر probing با بکارگیری active shield و د ستکاری ولتاژ و دما و امواج EM با قراردادن سنسور های مناسب) مورد نیاز است.

طراحی سخت افزار باید با در نظر گرفتن ملاحظات ایجاد مقاومت به حملات تحلیل توان تفاضلی و تزریق خطا باشد، از جمله بکارگیری تکنیک های پوشش دهی (masking) با پنهان سازی (hiding) و طراحی قابلیت اخذ گواهی‌های امنیتی و اکو سیستم نرم‌افزاری (مانند Java Card و GlobalPlatform) را دارا باشد. سیستم‌عامل کارت باید حداقل با مشـخصـات GlobalPlatform Card Specification v2.3.1 و در صـورت پشـتیبانی از اپلت‌های جاوا، با Java Card v3.1 سازگار باشد.

۳-۱- هدف

هدف، طراحی، ساخت نمونه اولیه،bring-up ، آزمون و مستند سازی یک Secure Element SoC بومی در فناوری 40nm Mixed-Signal CMOS اسـت که بتواند در میکرومدول‌های تماسـی، بدون تماس و dual-interface برای اسناد هویتی و کارت‌های هوشمند مورد استفاده قرار گیرد.

هدف	معیار کلی
کاربرد اصلی	eID / کارت ملّی هوشمند، ePassport، Digital Signature
کاربرد ثانویه	Multi-application smart card، security token، IoT embedded SE
فرآیند ساخت	40nm Mixed-Signal Si CMOS
امنیت هدف	CC EAL5+ readiness
رابط تماسی	ISO/IEC 7816-3، T=0 و T=1
رابط بدون تماس	ISO/IEC 14443 A/B (لایه ۱ تا ۳) + ISO/IEC 14443-4 (T=CL) + ISO/IEC 7816-4 APDU over contactless
رابط داخلی/توسعه	SPI slave حداقل 2Mbps
حافظه Flash	هدف 1MB؛ حداقل 512KB قابل قبول با توجیه معماری
SRAM	حداقل 32KB، شامل فضای کار رمزنگاری
OTP/eFuse	حداقل 256B؛ ترجیحاً 512B–1KB
Die area	Target حدود 6–8mm²؛ Preferred ≤7mm²؛ سقف 9mm² با توجیه فنی
دما	حداقل -25°C تا +85°C برای محدوده صنعتی/کارت

هدف	معیار کلی
بسته‌بندی	Micro-moduleو QFN engineering package

۳-۲- الزامات فنی محصول

۳-۲-۱- معماری کلی

تراشه باید به صورت یک SoC امن با Trust Boundary مشخص طراحی شود. کلیه مسیرهای دسترسی به کلیدها، حافظه‌های حساس و واحدهای رمزنگاری باید تحت کنترل Security Controller و سیاست lifecycle باشند.

زیرسیستم	الزام
Secure CPU	پردازنده باید دارای تحویل کامل کدهای RTL سنتزپذیر و تست‌بنچ‌های اعتبارسنجی در سطح سورس نظیر (Source-Level Verilog/SystemVerilog) باشد؛ ترجیحاً مبتنی بر معماری‌های ۳۲ بیتی استاندارد باز نظیر RISC-V Secure Profile یا معماری‌های تجاری معتبر با حق کامل سنتز و ممیزی امنیتی
Execution	In-order، deterministic؛ بدون speculative execution غیرضروری
MPU/Memory Protection	الزامی
Privilege levels	حداقل دو سطح privilege برای OS و application
Secure Boot	Boot ROM غیرقابل تغییر + authenticated firmware
Lifecycle	Manufacturing/Personalization/Test/Operational/RMA/Decommissioned
Watchdog	Secure watchdog با clock مستقل
Tamper controller	مرکزی و policy-driven
Security clock	مستقل از clock عادی CPU تا حد امکان
Debug	Lifecycle-controlled؛ در production دسترسی غیرمجاز ممنوع

۳- ۲- ۲- CPU

با توجّه به نسـل فناوری 40nm و با توجه به ماهیت workload کارت هوشـمند، مجری به یک CPU خاص مقید نخواهد بود؛ معیار اصلی امنیت، مصرف، area، timing closure، toolchain و قابلیت تحویل کامل IP است.

پارامتر	Requirement
Word size	32-bit
Clock target	30–60MHz؛ هدف طراحی 50MHz یا بیشتر
Pipeline	3–5 stage، بر اساس PPA و امنیت
MMU	الزامی نیست
MPU	Mandatory
FPU/Vector	Not required
Cache	در صورت نیاز؛ کوچک و ترجیحاً از نوع non-speculative
Debug	Secure/lifecycle controlled
Boot mode	Immutable Boot ROM

۳- ۲- ۳- Memory

حداقل 768 KB Secure Flash، حداقل 24 KB User RAM و OTP حداقل 256 B و Flash حداقل endurance برابر 500,000 چرخه و retention برابر 25 سال الزامی است.

حافظه	Requirement پیشنهادی
Secure Embedded Flash	768KB minimum؛1MB target
Boot ROM	64KB target
User SRAM	24KB minimum
Crypto RAM	8KB minimum، با امکان استفاده مشترک کنترل‌شده
Total SRAM	32KB minimum
OTP/eFuse	≥256B
Secure NVM	≥16KB برای lifecycle، counters، monotonic values و metadata
Flash endurance	≥500,000 P/E cycles target
Data retention	≥25 years target
Page erase	subject to selected macro/process، ≤0.5ms target
Byte program	subject to selected macro/process، ≤7µs target

۳- ۲- ۴- Memory Security

Address and data scrambling برای حافظه‌های حساس.

Bus/data-path protection برای مسیرهای حاوی داده حساس.

Encryption/integrity protection برای persistent security objects در صورت نیاز معماری.

Memory access firewall و privilege checking.

Secure erase / zeroization.

Anti-tearing و atomic update برای داده‌های حیاتی.

جلوگیری از دسترسی CPU/application به raw private-key material.

۳- ۲- ۵- Contact Interface

رابط تماسی باید مطابق ISO/IEC 7816-3 طراحی شود و T=0 و T=1 را پشتیبانی کند. سرعت تا TA1=0x97 در 5MHz.

پارامتر	Requirement
Protocol	T=1،T=0
Clock	مطابق profile کارت و ISO/IEC 7816-3
ATR	Mandatory
PPS	Mandatory
ETU timing	Mandatory
Electrical classes	کلاس‌های C/B/A در محدوده 1.62–5.5V، subject to pad/process validation
ESD	HBM ≥4kV و CDM ≥500V به عنوان target طراحی

۳- ۲- ۶- Contactless Interface

رابط بدون تماس باید برای ISO/IEC 14443 Type A و Type B طراحی شود. airspeed از 106 تا 848kbps و VHBR حداقل 1.7Mbps باشد و تأمین توان از آنتن ID-1 با 1 PICC Classes و 2 باشد.

پارامتر	Requirement
Standard	ISO/IEC 14443 Type A/B
Bit rate	106/212/424/848kbps
VHBR	≥1.7Mbps target
Power	Energy harvesting from antenna
AFE	Rectifier + regulator + load modulation + demodulation + clock extraction
Antenna	خارج از die ؛ Design Guide باید تحویل شود
Contactless operating modes	interoperability Reader/writer و card emulation profile هدف

۳- ۲- ۷- SPI

SPI slave حداقل 2Mbps باید فراهم شود SPI slave در چارچوب GlobalPlatform با حداقل 2Mbps باشد.

دسترسی SPI باید lifecycle-controlled باشد و در production صرفاً عملیات مجاز را بپذیرد.

۳- ۲- ۸- Timers, Watchdog and Interrupts

بلوک	Requirement
General timers	≥2
Watchdog	Independent/security watchdog
ETU timer	Dedicated
Contactless timing	Dedicated/programmable
Interrupt controller	Secure, prioritized
Low-power timer	Preferred
Monotonic counter	Mandatory for security/anti-rollback use cases

۳- ۲- ۹- Cryptographic Subsystem

مجموعه گسترده‌ای از شتاب‌دهنده‌های رمزنگاری باشد تعبیه شود: RSA :تا4096bit ، ECC تا 521bit و Curve25519/448، PQC شامل Kyber و Dilithium، AES/3DES، SHA-1/SHA-2/SHA-3 ، TRNG و PRNG.

Primitive	Requirement
RSA	Key length up to 4096bit
RSA CRT	Mandatory
RSA-2048 signing	≤100ms target
RSA-4096 signing	≤550ms target
ECC	ECDSA/ECDH/EdDSA
Weierstrass	NIST + brainpool up to P-521
Montgomery	X25519/X448
Edwards	Ed25519/Ed448 where applicable
ECC-256 sign	≤20ms target
ECC-521 sign	≤60ms target
AES	128/192/256
Modes	ECB/CBC/CTR/CCM/GCM
3DES	3-key legacy support where required

Requirement	Primitive
SHA-1, SHA-224/256/384/512, SHA-3, SHAKE	**SHA**
Hash Based Message Authentication Code	**HMAC**
AIS31-compliant target	**TRNG**
Cryptographic DRBG; AIS20-compatible architecture	**DRBG/PRNG**

۳- ۲- ۱۰- Post-Quantum Cryptography

با توجه به الزامات مهاجرت به استانداردهای نوین امنیتی، معماری سخت‌افزار/نرم‌افزار تراشه باید آمادگی کامل برای پشتیبانی از الگوریتم‌های استاندارد NIST بر پایه شبکه (Lattice-based) شامل ML-KEM (FIPS 203 /و Kyber) و ML-DSA / Dilithium) FIPS 204 را دارا باشد. مجری باید در ماتریس انطباق (Compliance Matrix) نحوه پشتیبانی، سطح بلوغ و بودجه حافظه/زمان اجرا را به تفکیک مشخص نماید.

الگوریتم	First silicon policy
خانواده ML-KEM/Kyber	الزامی در سطح معماری؛ شتاب‌دهنده سخت‌افزاری ترجیحا
خانواده ML-DSA/Dilithium	الزامی در سطح معماری؛ شتاب‌دهنده سخت‌افزاری ترجیحا
حافظه PQC RAM	رم کاری اختصاصی متناسب با بنچمارک پیاده‌سازی (حداقل 16 KB با قابلیت ارتقا به 32 KB)
رابط PQC API	لایه انتزاع سخت‌افزاری (HAL) پایدار و ایمن
مهاجرت Migration	امکان بازنگری الگوریتم بدون تغییر در ریشه اعتماد (RoT)

۳- ۲- ۱۱- واحد مولد اعداد تصادفی

زیرسیستم تولید اعداد تصادفی تراشه باید به عنوان یک مولد تصادفی واقعی ترکیبی (Hybrid TRNG/DRBG) با درجه انطباق استانداردهای امنیتی طراحی شده و شامل الزامات زیر باشد:

بند فنی	شرح نیازمندی و مشخصات عملکردی
منبع آنتروپی فیزیکی (Noise Source)	بهره‌گیری از منبع آنتروپی فیزیکی آنالوگ/دیجیتال واقعی (مانند RO Jitter یا Metastability) مقاوم در برابر حملات تزریق فرکانس و پایش ولتاژ، با نرخ آنتروپی دست‌کم $H_{min} \geq 0.997$ به ازای هر بیت.
آزمون‌های سلامت زمان راه‌اندازی (Startup Tests)	اجرای خودکار آزمون‌های سلامت استاندارد (تایید آماری آنتروپی و صحت عملکرد سنسورها مطابق NIST SP 800-90B / AIS 31) پیش از بارگذاری ریشه اعتماد و صدور هرگونه بیت خروجی.

بند فنی	شرح نیازمندی و مشخصات عملکردی
آزمون‌های سلامت پیوسته (Online Tests)	پایش بلادرنگ و برخط داده‌های خام آنتروپی حین کارکرد عادی تراشه (شامل آزمون‌های Repetition Count و Adaptive Proportion) جهت کشف فوری هرگونه دستکاری فیزیکی یا خرابی سخت‌افزاری.
بهسازی آنتروپی (Conditioning Unit)	استفاده از مدارات بهسازی سخت‌افزاری معین (مانند فشرده‌سازهای غیرخطی بر پایه هش یا توابع مشتق‌گیر مبتنی بر استاندارد) جهت حذف بایاس DC و رساندن داده‌ها به توزیع یکنواخت کامل.
مولد تصادفی قطعی رمزنگاری (Crypto DRBG)	موتور قطعی مبتنی بر استانداردهای NIST SP 800-90A (نظیر CTR_DRBG بر پایه AES-256 یا Hash_DRBG) با امکان بازبذردهی دوره‌ای خودکار (Reseeding) از منبع آنتروپی.
مدیریت خطای بحرانی (Mute & Fail-Safe)	ورود بلادرنگ به وضعیت خطای سخت‌افزاری (Hardware Trap/Halt) در صورت رد شدن آزمون‌های سلامت، و مسدودسازی قطعی خروجی به منظور جلوگیری از نشت آنتروپی غیرمعتبر به پردازنده و بافرها.
پیکربندی و خودآزمایی	تعبیه رابط‌های کنترلی ایزوله برای اجرای خودآزمایی‌های دوره‌ای (On-demand Self-Test) و تزریق داده آزمون (Test Vector Injection)

۳- ۲- ۱۲- Secure Boot and Firmware

تراشه باید مجهز به حافظه Boot ROM ماسک‌شده و غیرقابل تغییر (Immutable) به عنوان اولین حلقه از زنجیره اعتماد سخت‌افزاری (Hardware Root of Trust) باشد. فرآیند بوت امن (Secure Bootloader) باید عملیات احراز اصالت (Authentication)، بررسی تمامیت (Integrity) و اعتبارسنجی نسخه و ممانعت از بازگشت به نسخه‌های آسیب‌پذیر پیشین (Anti-Rollback بر پایه eFuse / شمارنده‌های یکنواخت) را پیش از واگذاری کنترل به فریم‌ور اصلی اجرا نماید. فرآیند به‌روزرسانی فریم‌ور باید دارای رفتار تراکنشی اتمیک (Atomic Update) و مقاوم در برابر قطع ناگهانی تغذیه (Power-loss Resilient) باشد.

Firmware component	Required
Immutable Boot ROM	Yes
Secure Bootloader	Yes
Secure OS	Yes
Crypto HAL	Yes
Flash/NVM driver	Yes
7816 driver/stack	Yes
14443 driver/stack	Yes
APDU dispatcher	Yes

Firmware component	Required
Secure filesystem	Yes
Key-management service	Yes
PQC library/API	Yes
Diagnostics	Yes
Personalization firmware	Yes

۳- ۲- ۱۳- Card Operating System

محصول باید به همراه یک Card Operating System قابل اجرا ارائه شود. OS می‌تواند Native باشد، ولی معماری باید امکان اجرای Java Card یا محیط سازگار باapplication های smart-card را فراهم کند.

.Application isolation

.Security Domain / trusted application model

.PIN/PUK management

.Secure filesystem

.APDU engine

.Cryptographic services

.Secure messaging

.Lifecycle control

.Secure update

.Audit/security event management

۳- ۲- ۱۴- ePassport / eID Functions

اجرای PACE+EAC مطابق BSI TR-03110 با زمان هدف کمتر از 2 ثانیه برایchip + software library ضـروری اسـت. کلیه پروتکل‌های ePassport باید مطابق ICAO Doc 9303 (ویرایش ۸) و BSI TR-03110 (نسخه ۳) پیاده‌سازی شوند.

Function	Requirement
PACE	Mandatory
EAC	Mandatory for ePassport profile
Chip Authentication	Mandatory where profile requires
Terminal Authentication	Mandatory where profile requires
Secure Messaging	Mandatory

DG/EF access control	Mandatory
Digital Signature	Mandatory service
Authentication	Mandatory
PACE+EAC benchmark	≤2s target under defined test configuration

۳-۲-۱۵- Security Architecture

امنیت باید در چهار لایه ســخت‌افزار، معماری حافظه/داده، firmware/OS و physical implementation تعریف شــود. reverse engineering، test-mode irreversibility، tamper، scrambling، side-channel ، fault injection، timing و physical attacks هدف است.

موضوع	Requirement
Test mode	در production برگشت‌ناپذیر یا cryptographically locked
Tamper	Central tamper controller
Voltage	Low/high voltage sensors
Temperature	Low/high temperature sensors
Clock	Low/high frequency + glitch detection
Light	Light sensor
Shield	Active shield
Unique ID	Mandatory
PUF	Mandatory target; enrollment/reconstruction must be characterized
Side channel	SPA/DPA/CPA/EMA/timing countermeasures
Fault injection	Laser/EM/glitch/DFA countermeasures
Physical	FIB/probing threat model and countermeasures

۳-۲-۱۶- PUF and Device Identity

PUF باید به عنوان ریشه تولید/بازیابی device-unique secret قابل استفاده باشد، ولی raw PUF response نباید مستقیماً در firmware قابل خواندن باشد. معماری باید شامل enrollment، helper data protection ، reconstruction، error correction و lifecycle policy باشد.

Unique Chip ID باید immutable یا lifecycle-protected باشــد و در personalization و traceability قابل استفاده باشد.

۳-۲-۱۷- Tamper Response

Event	Minimum response

Over/under voltage	Abort + secure state
Over/under temperature	Abort/limited operation + secure event
Clock anomaly	Abort/security reset
Glitch	Abort/security reset
Light	Security event + configurable response
Shield breach	Immediate security response
Repeated fault	Escalation policy
Critical key compromise indication	Zeroization of volatile key material

۳- ۲- ۱۸- الزامات امنیت فیزیکی و لی‌اوت تراشه

طراحی فیزیکی تراشه باید کلیه مکانیزم‌های سخت‌سازی لازم را جهت مقابله با حملات فیزیکی تهاجمی (Invasive)، نیمه‌تهاجمی (Semi-Invasive) و غیرتهاجمی (Non-Invasive) نظیر پروبینگ میکروسکوپی (Micro-probing)، دستکاری با لیزرFIB، بازگشایی لایه‌ها (Delayering) و نشت اطلاعات از طریق کانال جانبی (Side-Channel) پیاده‌سازی نماید.

بند فنی	حوزه طراحی فیزیکی	شرح الزامات و مشخصات فنی لی‌اوت
ایزولاسیون مسیرهای حساس (Sensitive Routing Isolation)	Routing / Interconnect	استفاده از روش‌های Shielded Routing (سیم‌بندی بین خطوط تغذیه) برای سیگنال‌های حامل کلید، داده‌های رمزشده، پالس‌های ساعت امن و باس‌های داده؛ عدم عبور سیگنال‌های حساس از بالاترین لایه‌های فلزی چیپ.
کنترل نویز بستر و حلقه‌های محافظ (Rings Guard & Substrate Noise)	Floorplanning / Silicon	تفکیک کامل نواحی آنالوگ/RF، بلوک‌های رمزنگاری و مدارات دیجیتال با استفاده از Isolation Triple-Well و حلقه‌های محافظ پیوسته (Guard Rings) دور تا دور بلوک‌های حساس به‌منظور جلوگیری از انتشار نویز سوبسترا و اثرات Latch-up تحت تابش لیزر.
سپر فعال و مش ضد دستکاری (Active Shield / Tamper Mesh)	Top Metal Layer	پوشش کامل سطوح حیاتی تراشه (CPU، NVM، Key RAM، Crypto) با مش فعال چندلایه با الگوریتم پویا (Dynamic/Random Bit Pattern Mesh) در بالاترین لایه‌های فلز، به‌گونه‌ای که هرگونه برش فیزیکی، اتصال کوتاه یا دستکاری میکروسکوپی سریعاً منجر به فعال‌سازی Alarm و ریست سخت‌افزاری گردد.
ایزولاسیون فیزیکی حافظه کلید (Key RAM Isolation)	Physical Placement	جانمایی بلوک Key RAM در عمیق‌ترین و محافظت‌شده‌ترین بخش مرکزی چیپ، با قابلیت پاک‌سازی آنی و قطعی مقادیر (Zeroization) در اثر وقوع هرگونه رخداد Tamper فیزیکی.
کمینه‌سازی نشت در مسیر داده (Crypto	Cell Level / Logic	استفاده از منطق‌های متقارن و Dual Rail logic در مسیرهای محاسباتی حساس و متقارن‌سازی کامل طول و خازن مسیرهای رفت

بند فنی	حوزه طراحی فیزیکی	شرح الزامات و مشخصات فنی لی‌اوت
Datapath (Hardening		و برگشت داده (Matched Routing) جهت به حداقل رساندن نشت اطلاعات الکترومغناطیسی و توانی (DPA/EMA).
حفاظت از شبکه‌های پالس ساعت و ریست Reset & Clock) (Hardening	Clock Tree Synthesis (CTS)	توزیع پالس ساعت به صورت ایزوله، استفاده از منابع کلاک نامتقارن/داخلی امن، و تعبیه فیلترهای ضد Glitch در خطوط Reset و Clock با قابلیت تشخیص دستکاری فرکانس/لبه‌های ناهنجار.
تفکیک دامنه‌های تغذیه Power Domain) (Separation	Power Grid Design	جداسازی دامنه‌های تغذیه بلوک‌های رمزنگاری (Crypto Island)، هسته پردازنده، حافظه‌های امن و رادیو/رابط‌های ارتباطی از طریق رگولاتورهای داخلی (LDO) اختصاصی و خازن‌های دکوپلینگ مجتمع (Decap Cells) جهت تضعیف نویزهای قابل تحلیل روی پین‌های خارجی.
ایزولاسیون دسترسی‌های آزمون تولید (/ DFT JTAG / Scan (Isolation	Testability & DFT	قفل‌گذاری و غیرفعال‌سازی دائم یا احراز هویت قوی پورت‌های تست (JTAG/Scan Chains) در فازهای پس از تولید، ممانعت از بازخوانی محتوای ثبات‌های امنیتی حین تست اسکن، و عدم وجود هرگونه مسیر تولیدی (Backdoor) برای دور زدن سیستم کنترل چرخه حیات (Lifecycle Controller).

۳- ۲- ۱۹- Reliability and Electrical

محدوده دمایی مرجع -25°C تا +85°C و تغذیه contact در کلاس‌های C/B/A با محدوده 1.62 تا 5.5V است.

مجری باید library/process corners، PVT، ESD، latch-up، IR drop، EM، thermal، power integrity و reliability را در sign-off لحاظ کند.

۴- پروفایل محافظتی و اهداف امنیتی

هدف امنیتی محصـــول، حفاظت از credentialهای هویتی، کلیدهای خصـــوصـــی، داده‌های شـــخصـــی، application code، stateهای امنیتی و عملیات امضای دیجیتال در برابر مهاجم نرم‌افزاری و فیزیکی با قابلیت بالا است.

۴-۱- دارایی‌های امنیتی

- Private keys
- Authentication credentials
- PUF-derived secrets
- Boot keys
- Firmware integrity
- Card OS
- Application code
- Personal identity data
- PIN/PUK state
- Secure messaging keys
- PQC private keys
- Lifecycle state
- Audit/security state

۴-۲- مهاجمین مورد نظر

- Terminal مخرب
- Application مخرب
- کاربر دارای دسترسی فیزیکی
- مهاجم آزمایشگاهی
- Side-channel attacker
- Fault-injection attacker
- Reverse-engineering attacker
- Probing/FIB attacker
- Malicious manufacturing actor
- Unauthorized personalization operator

۴-۳- Security Functional Requirements

حوزه SFR	الزام
Identification & authentication	Secure device/application/administrator authentication
Access control	Object/file/application access control
Cryptographic operations	Isolated hardware-backed crypto
Key management	Generation, storage, use and destruction under policy
Secure boot	Authenticated chain of trust
Secure update	Authenticated, anti-rollback, atomic
Audit	Security-event logging where applicable
Self-test	Startup and conditional crypto self-tests
Tamper	Detection and response
Data protection	Confidentiality + integrity
Randomness	Approved entropy and DRBG architecture
Lifecycle	Monotonic controlled states

۴-۴- Security Assurance Target

هدف طراحی و فرآیند توسعه باید آماده‌سازی برای مطابقت با Common Criteria در سطح EAL5+ باشد.

پیشنهاد RFP: مجری باید از ابتدای پروژه شواهد و artifacts لازم برای CC EAL5+ را تولید کند، ولی اخذ گواهی رسمی مدّنظر نیست.

مجری باید حداقل مستندات و شواهد زیر را تهیه کند:

- Security Target
- TOE Description
- Security Architecture
- TSS
- Assumptions
- Threats
- OSP
- SFR Mapping
- Assurance Evidence Plan

در صورت برون‌سپاری ساخت، مجری باید روش‌های کشف/کاهش خطر hardware Trojan و تغییرات غیرمجاز را پیشنهاد و در فرآیند verification و acceptance لحاظ کند.

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 checklistو 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.

فاز	محتوا	خروجی اصلی
F0	Kick-off و requirement baseline	SRS + Compliance Matrix
F1	Architecture	System/Security/Memory/Clock/Power architecture
F2	Security engineering	Threat Model + Security Target draft
F3	RTL + IP integration	RTL freeze candidates
F4	Firmware/OS	Boot ROM/OS/drivers/libraries
F5	Verification	Regression + coverage + formal
F6	Physical design	Netlist/GDSII/sign-off
F7	Tape-out	Final GDSII + foundry package
F8	Fabrication	Wafer
F9	Packaging/ATE	Packaged samples + tester
F10	Bring-up	First silicon report
F11	Security characterization	SCA/FI/tamper/penetration report
F12	Final acceptance	Release package

Verification باید از Architecture Phase شروع شود و به post-silicon ختم شود. هیچ بلوک امنیتی بحرانی نباید فقط با simulation عملکردی پذیرفته شود.

سطح	موارد
Unit RTL	Directed/random/assertion

موارد	سطح
Crypto, memory, security controller, interfaces	**Subsystem**
Boot/APDU/lifecycle/interrupt/reset/power	**SoC**
Unit/integration/fuzzing	**Software**
Security FSM, access control, reset/zeroization, key isolation	**Formal**
End-to-end functional demonstration	**FPGA**
Threat-driven verification	**Pre-silicon security**
SCA, FI, fault/tamper, electrical, performance	**Post-silicon**

۶- خروجی‌ها و موارد تحویلی مورد انتظار

۶-۱- اسناد مهندسی

System Requirement Specification
Compliance Matrix
System Architecture
Security Architecture
Threat Model
Security Target draft
Memory Map
Register Map
Clock/Reset/Power architecture
Interface specifications
Micro-architecture specifications
Verification Plan
DFT Plan
Physical Design Guidelines

۶-۲- RTL و Design Database

Complete RTL/HDL
Synthesis scripts
Constraints
IP manifests
Configuration files
Lint reports
CDC/RDC reports
Netlists
LEF/DEF
GDSII
DRC/LVS/ERC reports
STA reports
IR/EM reports
Power reports
Complete set of tape-out ready files

۶-۳- Software

Boot ROM source/binary
Bootloader
Secure OS
Drivers
Crypto library
SIM/eID middleware
APDU stack
Secure filesystem
Personalization software
Flash loader

PQC library
Host SDK
Compiler/toolchain integration
Debugger/emulator support

Test and Security - ۴-۶

UVM testbench
Test vectors
Coverage database
Formal proofs/reports
FPGA image
ATE program
Production test specification
Security test plan
SCA report
Fault injection report
Tamper characterization
Vulnerability analysis
Errata

خروجی نهایی باید در قالب Micro-Module برای کاربردهای تما سی و بدون تماس و همچنین QFN برای دسترسی به همه پایه‌ها ارائه شود. ابعاد die باید با استاندارد ISO/IEC 7816-2 (ابعاد ماژول کارت هوشمند) و الزامات wire bonding فاندری سازگار باشد. ابعاد die حداکثر 5mm برای قالب micro-module استاندارد می‌تواند باشد.

با توجه به این RFP و جزئیات امنیتی و PQC، در فناوری 40nm Mixed-Signal پیشنهاد می‌شود area به صورت target ≤8mm² و preferred ≤7mm² تعریف شود؛ سقف 9mm² فقط با توجیه فنی پذیرفته می‌شود. این برآورد، یک تخمین مهندسی است و در Architecture/Floorplan با macroهای واقعی فرآیند بازبینی خواهد شد.

بلوک	مساحت برآوردی (mm²)	توضیح
CPU + interconnect + MPU	0.15–0.30	بسته به CPU/IP
Secure controller/lifecycle/boot	0.15–0.30	Security FSM, lifecycle
AES/SHA/HMAC/CRC	0.20–0.40	Macro/RTL dependent
RSA/ECC accelerator	0.35–0.75	تا RSA-4096/P-521
PQC accelerator	0.40–1.20	بسیار وابسته به RAM و architecture
TRNG/DRBG/PUF/tamper	0.20–0.45	Mixed-signal/security
ROM	0.05–0.12	64KB

بلوک	مساحت برآوردی (mm^2)	توضیح
SRAM	0.10–0.25	32KB + crypto RAM
Flash/NVM	1.0–2.0	Process macro dependent
Contactless AFE	0.50–1.20	Rectifier/regulator/modulation/demodulation
7816/SPI/digital I/O	0.10–0.25	بدون pad ring
Clock/reset/power monitor	0.10–0.25	Security clock included
DFT/MBIST	0.05–0.15	Test infrastructure
Routing/guard/shield/isolation	0.50–1.00	Security layout overhead
Pad ring/ESD	0.50–1.20	به تعداد و اندازه pads وابسته
جمع مهندسی	≈4.4–9.6	بازه اولیه

پارامتر	هدف اولیه
CPU clock	50MHz target
Contactless	پشتیبانی از 106–848kbps و ≥1.7Mbps (Target 3.2Mbps for future-proofing)
RSA-2048 CRT sign	≤100ms
RSA-4096 CRT sign	≤550ms
ECDSA P-256 sign	≤20ms
ECDSA P-521 sign	≤60ms
PACE+EAC	≤2s end-to-end target
Standby	حداقل ممکن و مطابق card profile
Peak contactless power	مطابق ISO/IEC 14443/PICC class target
Contact mode	مطابق ISO/IEC 7816-3 electrical/current limits

۷- زمان‌بندی اجرای طرح

با توجه به اینکه scope شامل silicon، contactless AFE، crypto، firmware و Card OS است، زمان‌بندی پیشنهادی برای first silicon حدود ۲۱ الی ۲۲ ماه تا تحویل نمونه اولیه است. لازم به ذکر است که زمانبدی که در اینجا پیشنهاد می‌شود، الزامی نبوده و مجری می‌تواند زمانبندی خود را ارائه نماید.

فاز	مدت (ماه)	مدت تجمعی (ماه)
نیازمندی و architecture	1.5	1.5
Security architecture / Threat model	1.5	3
IP integration وRTL	4.5	7.5
Firmware/OS/crypto software	6 (موازی)	9
Verification	6 (موازی)	10.5
Physical design	3	13.5
Sign-off + tape-out	1	14.5
Fabrication	4–5	19
Packaging + ATE	1	20
Bring-up/characterization	1.5–2	21–22

۸- ترکیب پیشنهادی گروه اجرایی طرح

لازم به ذکر است که ترکیب گروه اجرایی که در اینجا پیشنهاد می شود، الزامی نبوده و مجری می‌تواند ترکیب گروه خود را ارائه نماید.

تخصص	تعداد	مسئولیت
Project Manager	1	مدیریت پروژه، schedule، ریسک، interface با کارفرما
System/SoC Architect	1	معماری کل تراشه
Security Architect	2	security architecture، Security Target،Threat model
CPU/RTL Engineers	2	control logic، MPU، bus،CPU
Crypto RTL Engineers	3	RSA/ECC/AES/SHA/PQC
Memory/Security RTL	2	tamper، lifecycle، key vault،memory controller
Mixed-Signal/AFE	2	power، sensors، oscillator،contactless AFE
Firmware/Secure OS	3	secure services، drivers، OS،Boot
Card OS/SIM/eID Software	3	applications، PACE/EAC، filesystem،APDU
Verification/UVM	4	SoC/subsystem verification
Formal/Security Verification	2	SCA/FI pre-silicon،formal
Physical Design	3	IR/EM، DRC/LVS، STA،PD
DFT/ATE	2	production test، ATE، MBIST،scan
Post-silicon/Security Test	2	security testing، characterization،bring-up
QA/Documentation	1	configuration/document control
جمع	33	پیک تیم؛ قابل کاهش باreuse IP

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 ...)، پولی و بانکی (کیف پول سخت‌افزاری، پرداخت و ...) و سایر حوزه‌های نیازمند تراشه SE، 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
بانک مرکز ج.ا ایران 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 کدهایHDL ، بلوک‌هایIP ، 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.