پژوهشکده
رایاسامانه‌های امن
پارسا

SADAF Hardware Security Module

ماژول امنیت سخت‌افزاری صدف

ریشه اعتماد در تراکنش‌های دیجیتال

شهریور ۱۴۰۳

پژوهشکده پارسا

رمزنگاری به عنوان رایج‌ترین روش برای اشتراک امن اطلاعات

- استفاده از روش‌های ریاضی برای تولید پیام رمز شده به کمک کلید مبتنی بر یک الگوریتم رمز است.
- در کاربردهای واقعی، تسهیم راز یک ضرورت است. لذا الگوریتم باید آشکار باشد و تنها مورد مخفی کلید است.
- مدیریت کلید پاشنه آشیل رمزنگاری است.

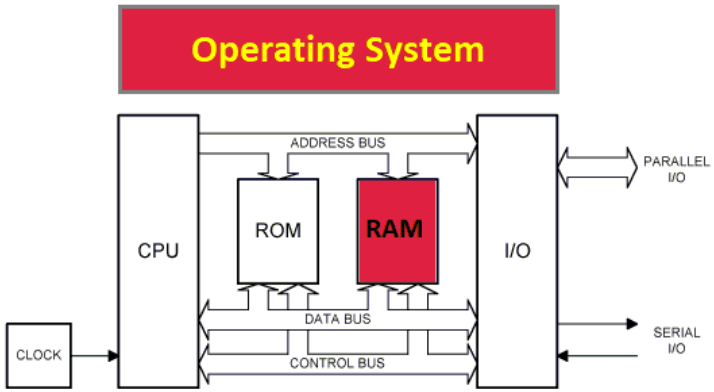
مدیریت کلید، پاشنه آشیل رمزنگاری

- تنها فاکتور مخفی در رمزنگاری کلید است و امنیت کلید بسیار مهم است.
- چرخه عمر کلید
  - تولید کلید
  - انتقال کلید
  - استفاده از کلید
  - نابودی کلید

ریشه اعتماد (Root-of-Trust) در فناوری رمزنگاری، مرجع مدیریت کلید است سیستم به امنیت آن اعتماد می‌کنند.

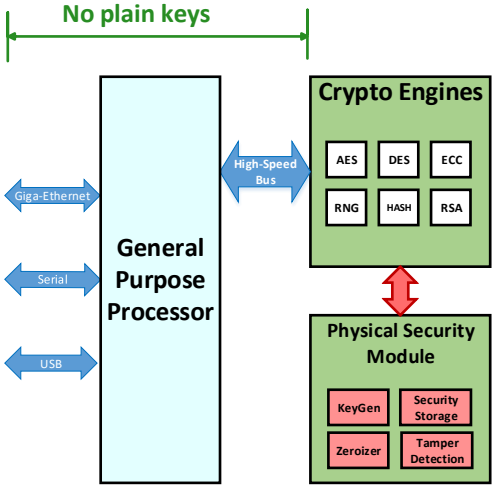
پیاده‌سازی ریشه اعتماد مبتنی بر سیستم نرم‌افزاری

- در این روش، روال‌های کار با کلید در محیط نرم‌افزار پیاده‌سازی می‌شوند و روی یک پردازنده یا میکروکنترلر اجرا می‌شوند.
- از نظر کارکرد تمام ویژگی‌های موردنیاز قابل دستیابی است.
- از نظر کارایی با استفاده از پردازنده‌های مدرن سطح نسبتاً بالایی از کارایی قابل دستیابی است.
- از نظر امنیتی الزامات پایه قابل دستیابی نیست.

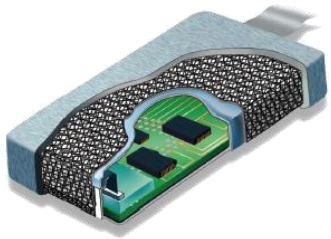


مشکل اصلی: کلید به صورت خام در حافظه اصلی سیستم ظاهر می‌شود که عملاً راه حلی ندارد.

ساخت ریشه اعتماد با استفاده از سخت‌افزار



- پیاده‌سازی ریشه اعتماد مبتنی بر سخت‌افزار
  - هرگز کلیدهای خارج از سخت‌افزار به صورت خام ظاهر نمی‌شوند.
  - کلیه عملیات رمزنگاری در داخل سخت‌افزار انجام می‌شود.
  - کلیه کلیدهای داخل سخت‌افزار با یک شاه‌کلید محافظت می‌شوند و ماژول امنیت فیزیکی از شاه‌کلید محافظت می‌کند.



در استاندارد امنیتی FIPS-L2+ بدون پیاده‌سازی سخت‌افزاری نیازمندی‌های لازم برای ریشه اعتماد برآورده نمی‌شود.

مفهوم Root-of-Trust

- ریشه اعتماد در فناوری رمزنگاری، مرجعی برای مدیریت کلید است که تمام عملیات یک سیستم امن به آن اعتماد می‌کنند.
- ریشه اعتماد باید با استفاده از بهترین فناوری ممکن، چرخه عمر مطمئنی را برای کلیدهای سیستم ایجاد نماید.

ماژول امنیت سخت‌افزاری به عنوان Root-of-Trust

- ماژول امنیت سخت‌افزاری یا Hardware Security Module (HSM)
- یک سیستم سخت‌افزاری قابل اطمینان و حفاظت شده با تکنیک‌های امنیت

سخت‌افزار/نرم‌افزار است که هدف اصلی آن مدیریت کلید در طول چرخه عمل آن است.

- تولید کلید امن
- بکارگیری امن کلید
- امحاء کلید

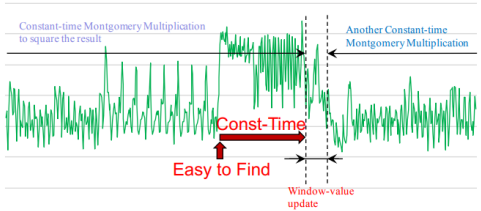
- مجهز به یک مجموعه هسته‌های رمزنگاری با کارایی بسیار بالاست.
- کاربردها:
  - مخابرات امن
  - بانکداری و پرداخت الکترونیکی
  - مدارک الکترونیکی و امضای دیجیتال
  - کارتهای شناسایی ملی و پاسپورت
  - وب‌سایت‌های امن
  - کاربردهای پزشکی
  - ... هر کاربرد مبتنی بر رمزنگاری

کاربردهای ماژول امنیت سخت‌افزاری

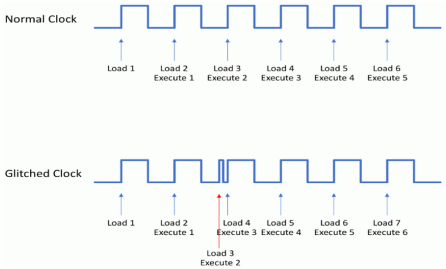
حفاظت از اطلاعات اساسی و کلیدها در

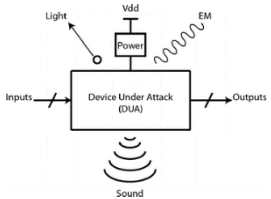
- مخابرات امن
- بانکداری و پرداخت الکترونیکی
- مدارک الکترونیکی و امضای دیجیتال
- سامانه‌های مبتنی بر کارتهای هوشمند
- کارتهای شناسایی ملی و پاسپورت
- وب‌سایت‌های امن
- کاربردهای پزشکی
- ... هر کاربرد مبتنی بر رمزنگاری

پیچیدگی‌های ساخت ماژول امنیت سخت‌افزاری




```
6       for (i=0;i<w;i++) {
7       BN_mod_mul(v,v,v,m);
8           wval<<=1;
9           wval+=BN_is_bit_set(d,b);
10          b--;
11      }
```





- رعایت اصول امنیت سخت‌افزار در طراحی HSM و PSM
  - حفاظت در برابر حملات کانال جانبی، حملات تزریق خطا، حملات مبتنی بر معماری و ...
  - حذف سیستم عامل: حفاظت در برابر بدافزارها، حفاظت در برابر حملات هکری
  - حفاظت دقیق از کل فایل‌های طراحی سخت‌افزار
- تولید اعداد تصادفی با کیفیت بسیار بالا با Hardware PUF
- نیاز به قابلیت اطمینان و تحمل‌پذیری خطای بالا
- توسعه حجم بسیار بالایی از نرم‌افزار سطح سیستمی، ابزارهای ارتباطی، پروتکل‌های امنیتی، سخت‌سازی سیستم عامل، کنترل I/O
- نیاز به کارایی بالا در کاربردهای واقعی

پژوهشکده رایا سامانه‌های امن پارسا

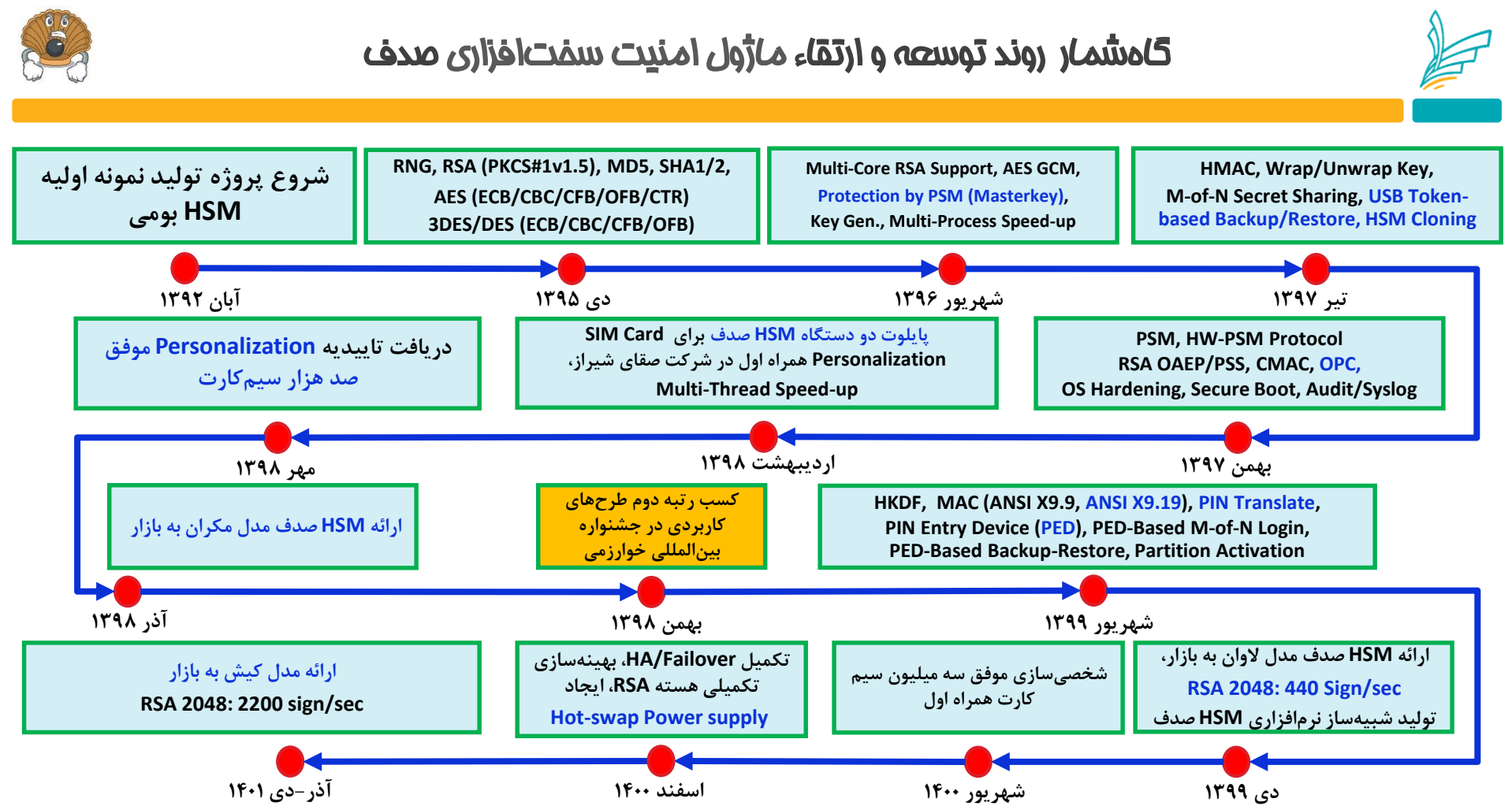
- پژوهشکده پارسا از نگاه مالی یک شرکت با مسئولیت محدود و از نگاه وزارت علوم یک پژوهشکده بخش خصوصی است.
- پژوهشکده در سال ۱۳۹۶ تأسیس شده است.
- ساختار فنی آن شامل سه آزمایشگاه پایه است:
  - آزمایشگاه امنیت سخت‌افزاری
  - آزمایشگاه امنیت داده
  - آزمایشگاه امنیت شبکه‌های سلولی

پژوهشکده
رایاسامانه‌های امن
پارسا

معرفی HSM صدف

- صدف یک HSM منطبق بر سطح سوم استاندارد FIPS 140-2 است.
- صدف از یک سخت‌افزار خاص منظوره به عنوان بستر امن اجرای عملیات تصدیق اصالت، رمزنگاری و مدیریت کلید کاربران HSM استفاده می‌کند.
- هیچ کدام از داده‌های حساس هرگز در خارج از مرز امن رمزنگاری به صورت خام ظاهر نمی‌شوند.

گام‌شمار روند توسعه و ارتقاء ماژول امنیت سخت‌افزاری صدف



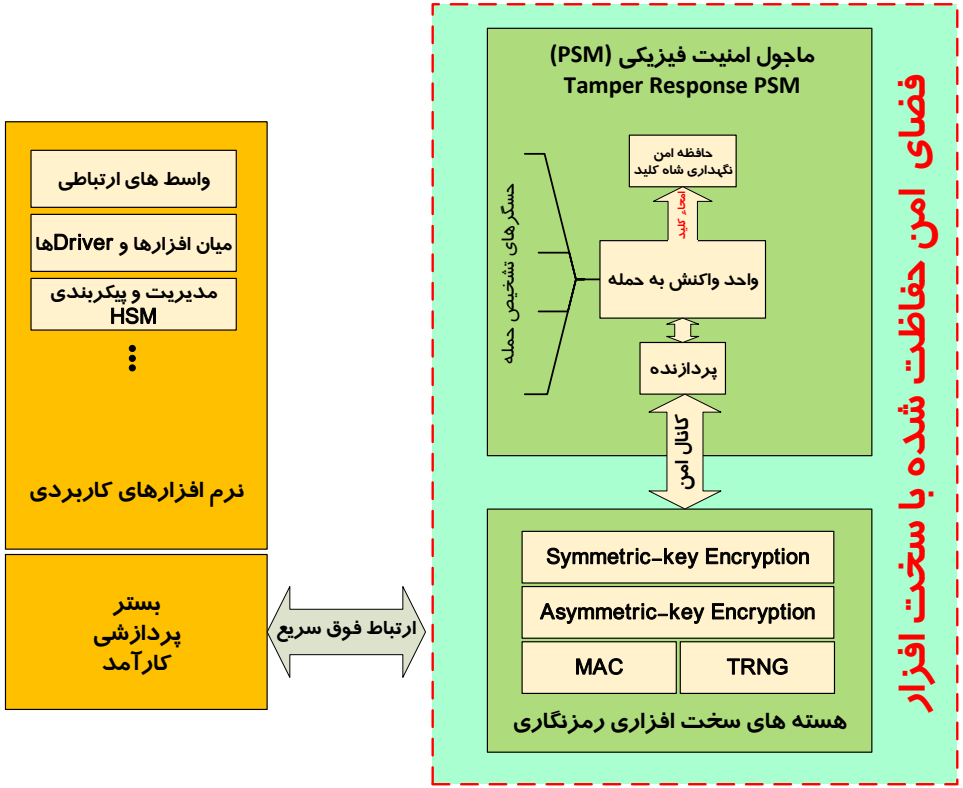
پایلوت‌های موفق برپایه HSM صدف

- صنایع قطعات الکترونیک (صقا) شیراز
  - استفاده از HSM صدف در خط تولید و شخصی‌سازی بیش از ۷ میلیون سیمکارت
- مرکز ریشه صدور گواهی دیجیتال (مرکز توسعه تجارت الکترونیک وزارت صمت)
  - مورد استفاده در TSA (Time Stamp Authority)
- مرکز میانی صدور گواهی دیجیتال بخش خصوصی ParsSign
  - پشتبیانی از امضای دیجیتال شرکت هویتا
- سامانه امضای دیجیتال شرکت پندار کوشک ایمن
  - پشتبیانی از امضای دیجیتال شرکت پندار کوشک ایمن
- منتخب بکارگیری در مرکز صدور گواهی دیجیتال بانک مرکزی با همکاری شرکت خدمات انفورماتیک ایران
  - استفاده از صدف در سامانه نماد

مروری بر امکانات کاربردی HSM

Successful Integration	امنیت شبکه	امنیت پایگاه داده	Web/App Server	مرکز گواهی دیجیتال (CA)	Mobile Operator	Utilities
	VPN (OpenVPN) WAF (Amnafzar WAF) DNS Security (Bind DNSSEC) E-Mail Client (Thunderbird)	Oracle TDE PostgreSQL TDE	Apache NginX Tomcat Weblogic IIS JBOSS	هویتا (ParsTrust) پندارکوشک ایمن (PKI) WinServer2012-CA EJBCA EasyRSA	سامانه شخصی‌سازی سیم کارت همراه اول (صا ایران، صقا) سامانه Advanced OTA همراه اول (حصین)	Cryptoki Manager OpenSC PKCS11-Tool HashiCorp-Vault
User Interface Utility Tools	واسط‌های کاربری گرافیکی، تعاملی، و خط فرمان ابزارهای تست خودکار امنیت، عملکرد، کارایی (تست NIST، GoogleTest، شرایط مرزی، خودآزمون)	واسط مدیریت	برنامه نصاب گرافیکی	برنامه تست بار (Load Test)	شبیه‌ساز نرم‌افزاری	
Programming Interface	PKCS#11 (Windows, Linux)	OpenSSL Engine	Optimized IAIK PKCS11 Java Wrapper PKCS11Interop .Net Wrapper	JCA/JCE (SUN PKCS11 Provider) Microsoft CNG (KSP)		
Clustering and HA	HSM Cloning	Partition Backup on USB Token	HA and Failover HSM Clustering/Load Balancing			

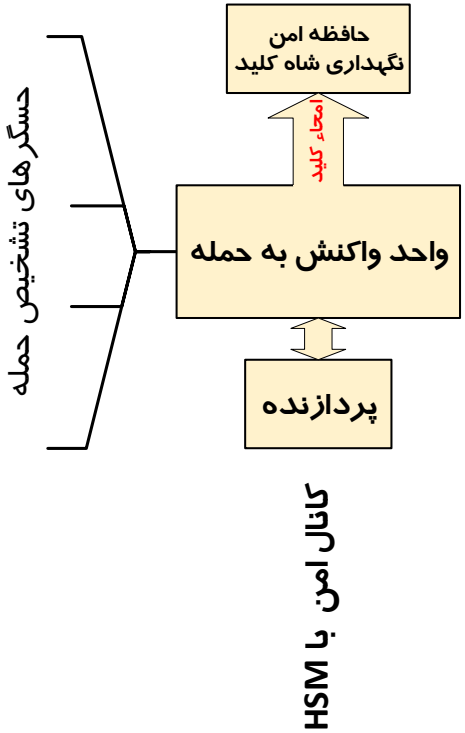
ساختار کلی HSM صدف



- در ساختار HSM صدف:
  - کلید هرگز خارج از مرز امن رمزنگاری به صورت خام ظاهر نمی‌شود.
  - کلیه ارتباطات بین ماژول‌ها به صورت رمز شده و مبتنی بر پروتکل‌های رمزنگاری دقیق انجام می‌شود.
  - ارتباطات با دنیای بیرون از مسیر درگاه‌ها و پروتکل‌های استاندارد است.
  - شاه‌کلید سیستم توسط ماژول حفاظت فیزیکی (PSM) با مکانیسم‌های دقیق حفاظت می‌شود.

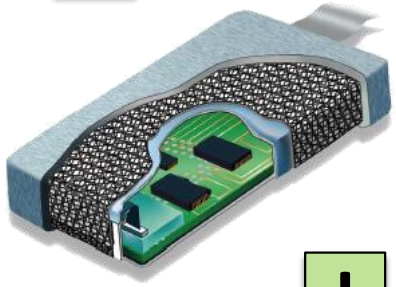
کنترل دسترسی فیزیکی به PSM

- وظیفه اصلی این ماژول، برآورده کردن نیازمندی پنجم از استاندارد FIPS 140-2 با عنوان Physical Security است. در صورت تشخیص هر نوع دستکاری، اقدام به امحاء شاه‌کلید می‌کند.
- دسترسی فیزیکی به PSM با مش و حسگر کنترل می‌شود.
  - حسگرهای نور، ولتاژ، دما، سوییچ، فرکانس و ...
  - حسگر مش حفاظتی
  - رزین پوشاننده
- صفرسازی شاه کلید بر روی SRAM
  - بازنویسی داده تصادفی و ثابت در SRAM
  - قطع برق SRAM
  - پاک کردن کلیدها
  - فعال کردن سیگنال Temper LED خروجی کیس



ساختار ماجول حفاظت فیزیکی

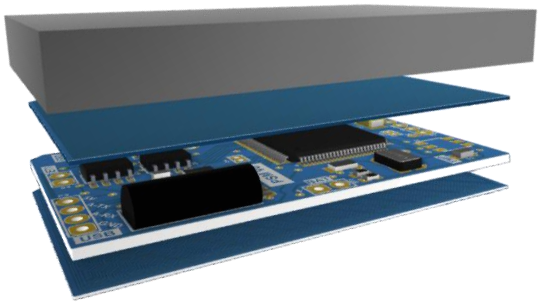
+



+

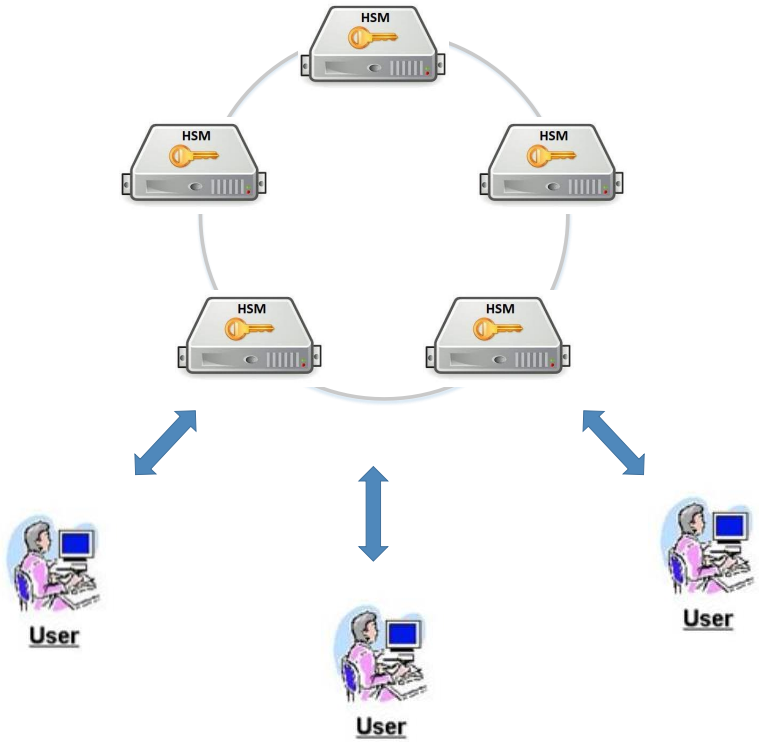
رزین

=



- این بخش مجهز به یک باتری خاص است که:
  - از محتوای کلید اصلی در حالت خاموش محافظت می‌کند.
  - سیستم تشخیص دستکاری در حالت خاموش فعال می‌ماند.

قابلیت HA در ماژول امنیت سخت‌افزاری صدف

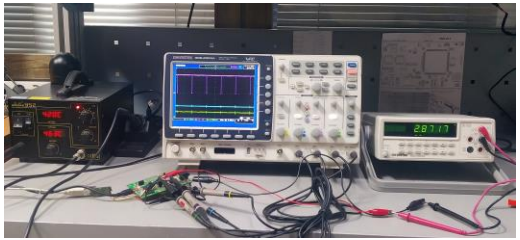


- مزایای قابلیت HA در صدف:
  - قابلیت HA صدف سطح بسیار بالایی از دسترس‌پذیری را در اختیار کاربران قرار می‌دهد.
    - مکانیسم توزیع بار در این معماری امکان تجمیع کارایی HSMها را به صورت کارآمد فراهم می‌کند.
    - مکانیسم Active-Active failover امکان تداوم سرویس‌دهی با وجود رخداد خرابی در سیستم را فراهم می‌کند.
    - سازگارسازی HSM جدید در شبکه HA با کل HSMهای موجود در HA به صورت خودکار و دستی قابل انجام است.
  - جزییات عملیات کاملاً از دید کاربر نهایی پنهان است.
  - کلیه عملیات با پروتکل‌های امنیتی دقیق حفاظت می‌شود.

تجهیز امنیتی Pin Entry Device (PED) برای سطح سوم FIPS

- دستگاه PED یک دستگاه مستقل است که از طریق شبکه با HSM ارتباط برقرار می‌کند.
- وجود PED یک الزام برای FIPS 140-2 Level 3 است.
- کاربردهای PED
  - مدیریت و تصدیق اصالت از راه دور
  - پشتیبان‌گیری و بازیابی کلیدهای HSM با استفاده از توکن‌ها
  - تصدیق اصالت مبتنی بر تسهیم راز M-of-N با استفاده از توکن‌ها

روال تست سیستم قبل از تحویل به مشتری



تست تجهیزات: تأمین قطعات، بررسی اصالت قطعات، تست اولیه قطعات.

تست سخت‌افزار :تست اولیه سخت‌افزار مونتاژ شده، تست سخت‌افزار PSM.

تست اولیه :نصب نرم‌افزار، شخصی‌سازی، تست واسط بین PSM و HSM، تست سامانه تشخیص حمله.

تست پایه نرم‌افزار :تنظیمات نرم‌افزار، تست اولیه مؤلفه‌های نرم‌افزاری، تست اسکریپت‌ها.

تست هسته‌های رمزنگاری :تست عدد تصادفی، تست توابع رمزنگاری.

تست سازگاری :تست HSM با سیستم‌های عامل مختلف.

تست PED: تست تجهیز PED در شرایط مختلف، تست با توکن، تست توابع مرتبط با توکن.

تست قابلیت اطمینان :تست سیستم با انواع بار سنگین و متنوع با زمان طولانی، تست پشتیبان‌گیری و بازیابی کلیدها .

تست قابلیت دسترسی :تست High-Availability با اعمال خرابی در شرایط مختلف

شبیه‌ساز نرم‌افزاری HSM صدف

- یک ماشین مجازی که از نظر کاربری و مدیریت مشابه دستگاه HSM سخت‌افزاری است.
- مشتریان با استفاده از واسط شبکه از ماشین مجازی خدمات مشابه با یک HSM دریافت می‌کنند.
  - آموزش پرسنل
  - توسعه واسط‌ها
  - تست سازگاری
- شبیه‌ساز از نظر سطح امنیت معادل SSM است.
- کارایی آن وابسته با کارایی ماشین میزبان است ولی معمولاً خیلی پایین‌تر از HSM است.

مشخصات فنی – بخش اول

تصدیق اصالت	FIPS Level 2 • Secure Password-based Authentication FIPS Level 3: • Secure USB Token-based Authentication (PED-based Trusted Path, Two-Factor Authentication, M-of-N Login)
Logging/Audit	Syslog
پروتکل ارتباطی	TLSv1.2
API	PKCS#11, Java JCA/JCE, OpenSSL Engine, Microsoft CNG (KSP)
سیستم عامل	Linux/Unix, Windows

High Availability (HA) Active-Active Failover Loadbalancing	پشتیبانی می‌شود.
Network Time Protocol (NTP)	پشتیبانی می‌شود.
Network Management	• Network Access Control Rules • Configuration of TCP/IP options, including Keep Alive and Timeout.
پشتیبانی از برنامه‌های کاربردی	+ Web/Application Server (HTTPS/SSL/TLS) • Weblogic • Tomcat • NGINX • Apache • IIS + Database Security, Transparent Data Encryption • Oracle • PostgreSQL + Network Security • OpenVPN • Bind DNS Server (DNSSec) + Application Security • HashiCorp-Vault • PKI: Windows Certificate Server/Authority • SIM card Personalization • Secure Email: Mozilla Thunderbird

مرز حفاظت سخت‌افزاری	+ پیاده‌سازی و اجرای کلیه عملیات حساس در داخل سخت‌افزار FPGA: • تولید، ذخیره‌سازی، پشتیبان‌گیری و بازیابی کلیدها • عملیات رمزنگاری • تصدیق اصالت کاربران + محافظت از داده‌های حساس (کلیدهای رمزنگاری و تصدیق اصالت) در برابر: • مولفه‌های نرم‌افزاری HSM شامل سیستم عامل، برنامه‌های کاربردی، درایورها • مولفه‌های سخت‌افزاری عام‌منظوره HSM شامل CPU، حافظه‌های موقتی و دائمی
سطح امنیتی	قابل پیکربندی در دو سطح: • FIPS 140-2 Level 2 • FIPS 140-2 Level 3

تولید عدد تصادفی	Hardware-based True Noise Source NIST SP 800-90A compliant CTR-DRBG
پیاده‌سازی الگوریتم‌های رمزنگاری یا پروتکل‌های امنیتی بومی/اختصاصی روی سخت‌افزار FPGA	پشتیبانی می‌شود.
کاربران/نقش‌ها	+ Multiple Administrators per HSM Device + Separate Administrator account for Audit operations + Two distinct Users per HSM Partition: • Security Officer • Normal User

مشخصات فنی – بخش پنجم

Algorithm	MAKRAN	LAVAN	KISH	کارایی (TPS)
RSA 1024	1000	4500	4500	RSA Sign/Sec
RSA 2048	250	900	2200	
RSA 4096	40	170	350	
AES 256	2500	8000	8000	Symmetric Enc/Sec
TDES	2500	8000	8000	

ارزیابی قابلیت اطمینان ماژول امنیت سخت‌افزاری صدف

- استفاده از بهترین برندها با بالاترین سطح کیفی برای تجهیزات سیستم.
- تکرار روند طراحی برای رسیدن به بالاترین سطح قابلیت اطمینان
- انجام انواع تست‌های طولانی‌مدت و سنگین برای ارزیابی میزان قابلیت اطمینان
  - بیش از ٤ سال تست قابلیت اطمینان تجهیزات اساسی مانند **باتری** و **فن**
  - ده‌ها هزار ساعت تست بار سنگین در شرایط واقعی روی مدل‌های مختلف
- ارتباط مداوم با مشتریان
  - دریافت بازخورد از بیش از ۲۰ مشتری در طول حدود ٤ سال
  - رصد دائمی شرایط HSMهای تحویلی با هدف اطلاع از گلوگاه‌های قابلیت اطمینان

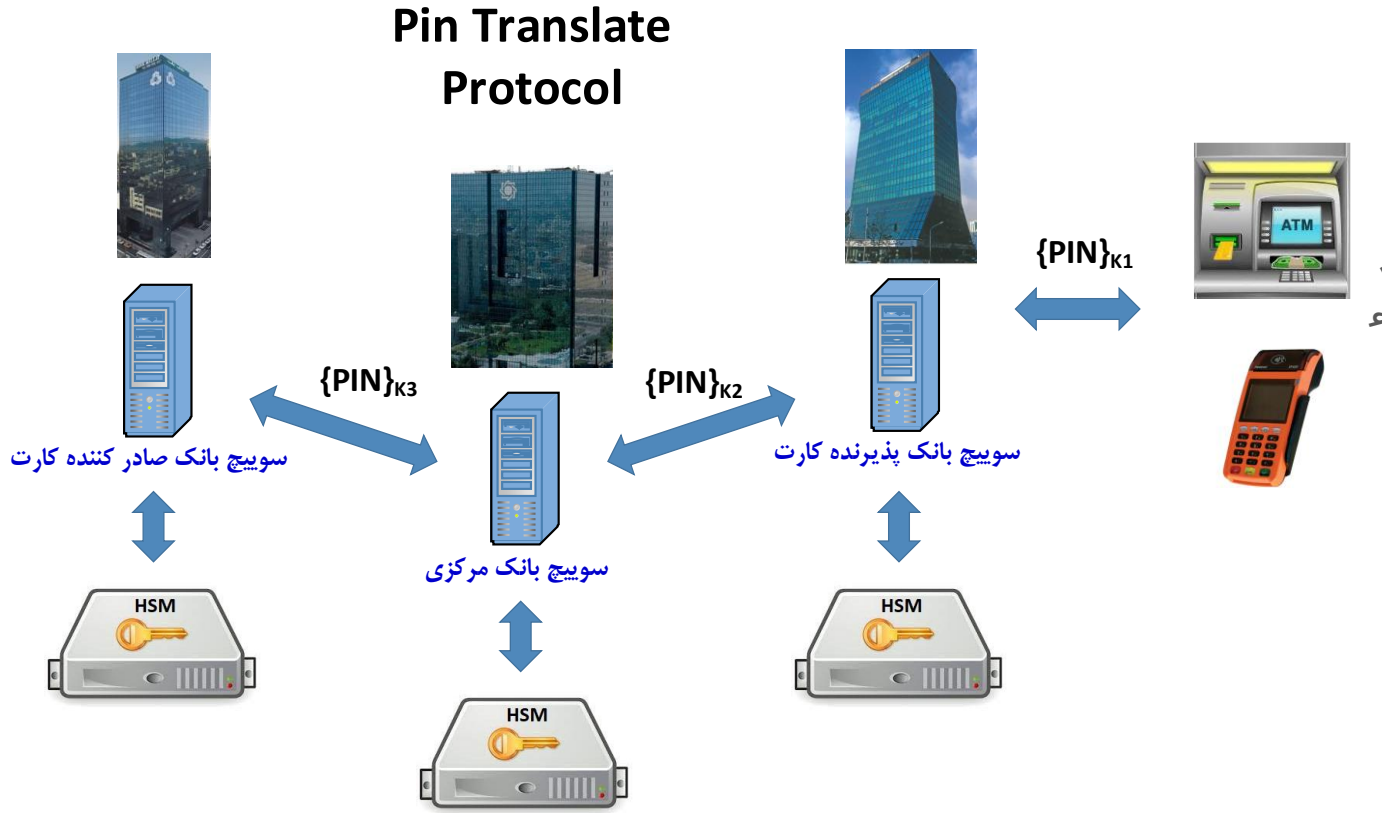
مطالعه تطبیقی با محصولات خارجی

Feature		SafeNet Luna			Utimaco			Sadaf		
		LS700	S750	S790	Se52	Se500	Se1500	Makran	Lavan	Kish
FIPS Level		FIPS 140-2 Level 3	FIPS 140-2 Level 3	FIPS 140-2 Level 3	FIPS 140-2 Level 3	FIPS 140-2 Level 3	FIPS 140-2 Level 3	FIPS 140-2 Level 3	FIPS 140-2 Level 3	FIPS 140-2 Level 3
Symmetric Key	DES, 3DES	✓	✓	✓	✓	✓	✓	✓	✓	✓
	AES	✓	✓	✓	✓	✓	✓	✓	✓	✓
Asymmetric Key	RSA	✓	✓	✓	✓	✓	✓	✓	✓	✓
	ECC	✓	✓	✓	✓	✓	✓	×	Final test	Final test
HASH		✓	✓	✓	✓	✓	✓	✓	✓	✓
MAC		✓	✓	✓	✓	✓	✓	✓	✓	✓
HW-based TRNG		✓	✓	✓	✓	✓	✓	✓	✓	✓
Simulator		✓	✓	✓	✓	✓	✓	✓	✓	✓
HA/FO		✓	✓	✓	✓	✓	✓	✓	✓	✓
RSA-2048		1,000	5,000	10000	75	580	780	250	900	2200
ECC P256		2,000	10,000	22,000	880	1040	1400	Estimate: 500	Estimate: 2000	Estimate: 3500
AES		2,000	10,000	17,000	?	?	?	2500	8000	8000
Education		×	×	×	×	×	×	✓	✓	✓
Technical Support		×	×	×	×	×	×	✓	✓	✓
Guarantee		×	×	×	×	×	×	3 Years	3 Years	3 Years

افتخارات و گواهی ها

- اخذ گواهی FIPS140-2 Level3 از آزمایشگاه مرکز تحقیقات صنایع انفورماتیک (مورد تایید مرکز افتا و مرکز ریشه) در سال ۱۴۰۲
- تایید فنی توسط شرکت متیران
- کسب رتبه دوم جشنواره بین المللی خوارزمی
- تایید فنی توسط آپای دانشگاه شریف
- مراحل فنی اخذ تأییدیه FIPS از افتا با موفقیت طی شده و صدور گواهی افتا در جریان است.

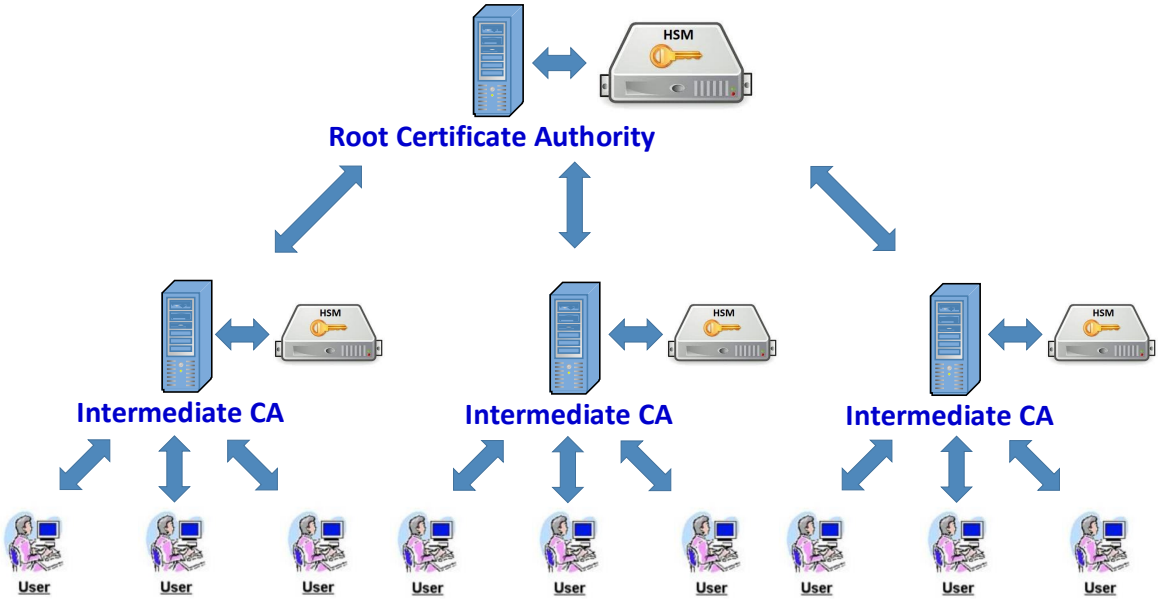
جایگاه HSM در شبکه پرداخت بین بانکی



- کلیه توابع لازم برای این کارکرد در HSM صدف پشتیبانی می‌شود.
- استفاده از HSM صدف در این زیرساخت، باعث ارتقاء امنیتی می‌شود.
- مثال:
  - عدم دسترسی به PINها

ارتقاء امنیت سامانه امضای دیجیتال سازمانی

- کلیه توابع لازم برای این کارکرد در HSM صدف پشتیبانی می‌شود.
- HSM صدف در مرکز ریشه صدور گواهی دیجیتال وزارت صمت مورد استفاده است
- HSM صدف برای سامانه امضای الکترونیکی داخلی در وزارت علوم هم مورد استفاده است.



ویژگی‌های ضروری برای تراکنش‌های بانکی و بیمه در کشور

- این نیازمندی‌ها از حدود ۲ سال قبل احصاء گردید:
  - همکاری و جلسات فنی با شرکت‌های خدمات انفورماتیک، شاپرک، پندار کوشک ایمن، بررسی محصولات مشابه، مطالعه دقیق استانداردهای تبادلات بانکی

- لیست نیازمندی‌های پایه پشتیبانی شده توسط HSM صدف
  - قابلیت اطمینان بالا (High Availability و Failover)
  - پشتیبانی از استانداردهای پرداخت
  - خوشه‌بندی و توزیع بار کارآمد
  - پشتیبانی از الگوریتم‌های رمزنگاری سامانه‌های پرداخت
  - کارایی بالا در محاسبات رمزنگاری
  - مدیریت و مانیتورینگ انعطاف‌پذیر

- در حال حاضر همه این ویژگی‌ها به HSM صدف اضافه گردیده است.
- شرایط تجاری HSM صدف در شبکه بانکی:
  - HSM صدف در چهار بانک نصب و راه‌اندازی شده است.
  - مذاکره با یک بانک دیگر جهت خرید HSM در حال انجام است.
  - بیش از دو سال همکاری با شرکت خدمات انفورماتیک جهت مجتمع‌سازی صدف در سامانه‌های شرکت خدمات

چرا HSM پارسا؟

- کارکرد، کارایی و امنیت قابل اثبات
- پشتیبانی و خدمات پس از فروش
- ضمانت قطعات و سرویس‌ها
- مستندات دقیق و آموزش کامل