ماژول امنیت سخت‌افزاری (HSM) صدف

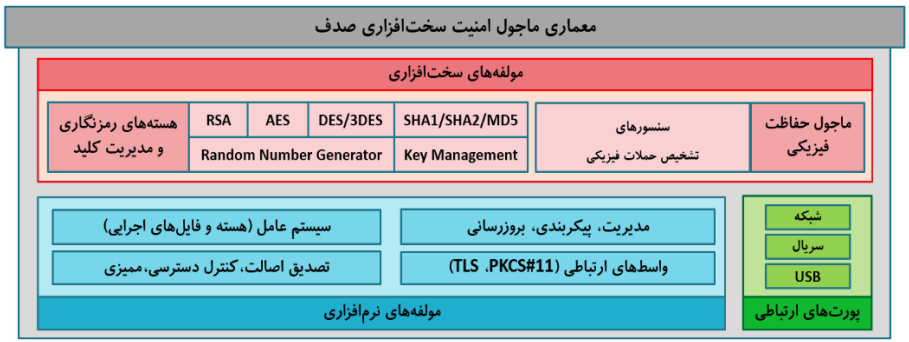
پژوهشکده رایاسامانه‌های پارسا

معرفی کلی

مهم‌ترین چالش امنیتی در سامانه‌هایی که برای حفاظت از اطلاعات حساس خود از روش‌های رمزنگاری استفاده می‌کنند، حفاظت از کلیدهای رمزنگاری به کار رفته در این روش‌هاست. در حال حاضر ایمن‌ترین راه برای حفاظت از یک کلید، ذخیره‌سازی و بکارگیری آن در داخل یک سخت‌افزار حفاظت شده با عنوان ماژول امنیت سخت‌افزاری (Hardware Security Module – HSM) است. در طول ۹ سال گذشته و با حمایت شرکت ارتباطات سیار ایران (همراه اول)، ماژول امنیت سخت‌افزاری صدف مبتنی بر دانش بومی و منطبق بر آخرین استانداردهای صنعتی این حوزه در مرکز پژوهشی پارسا طرحی و تولید شده است. در پیاده‌سازی صدف، پیشرفته‌ترین مکانیزم‌های رمزنگاری و حفاظت از کلید به کار رفته است و این محصول می‌تواند افق‌های نوینی از امنیت اطلاعات و ارتباطات را برای سامانه‌های حیاتی کشور نظیر اپراتورهای تلفن همراه، بانک‌ها، و سایر سازمان‌های اطلاعاتی و امنیتی بگشاید.

ویژگی‌های فنی

- پشتیبانی از استاندارد FIPS 1402– Level3.
- بکارگیری روش‌های پیشرفته حفاظت فیزیکی فعال (Tamper Response).
- تضمین اصالت کلیه مولفه‌های نرم‌افزاری با رمزگذاری و امضای نرم‌افزارها با کلیدهای سخت‌افزاری.
- استفاده از مکانیسم‌های کارآمد و بروز برای پشتیبانی از انواع الگوریتم‌های رمزنگاری مدرن
- دستیابی به کارایی بالا با انتخاب بستر مناسب و فراهم کردن امکان اجرای موازی و همزمان چندین عملیات رمزنگاری مستقل، مقیاس‌پذیر با توزیع بار بر روی چند صدف از طریق واسط شبکه به همراه قابلیت HA/Failover.
- مشاوره، آموزش، سفارشی‌سازی و کلیه خدمات پشتیبانی/فنی پس از فروش.



آدرس: تهران، طرشت، نبش بلوار شهید صالحی و بلوار شهید اکبری، برج فناوری شریف، واحد ۱۰۸ - تلفن: ۶۵۰۱۳۰۳۲ وبگاه: www.parsasharif.ir - رایانامه: info@parsasharif.ir

مشخصات فنی ماژول امنیت سخت‌افزاری صدف	
سطح امنیتی	قابل پیکربندی در دو سطح: • FIPS 140-2 Level 2 • FIPS 140-2 Level 3
حفاظت فیزیکی	تشخیص دستکاری فیزیکی (Tamper Evidence) و پاسخ به آن (Tamper Response) بر اساس FIPS 140-2 Level 4
رمزنگاری نامتقارن	RSA (1024, 2048, 4096) • Padding: PKCS#1v1.5, PKCS#1v2.2 (OAEP, PSS) ECDSA • SECP256R1, SEC256K1, SECP384R1 • BrainpoolP256R1, BrainpoolP384R1, BrainpoolP512R1, BrainpoolP512T1
رمزنگاری متقارن	AES (128, 192, 256), DES, 3DES (112,168) • Modes: ECB, CBC, OFB, CFB, CTR, GCM
Hash Functions	MD5, SHA-1, SHA-2 (224, 256, 384, 512)
MAC Algorithms	HMAC (MD5, SHA-1, SHA-2) CMAC (AES, 3DES) MAC [ANSI X9.9] (AES, DES, 3DES) MAC [ANSI X9.19] (AES, 3DES)
Wrap/Unwrap Algorithms	Symmetric Wrap/Unwrap (NIST SP 800-38F) Symmetric Wrap/Unwrap (AES/DES/3DES) Asymmetric Wrap/Unwrap (RSA, PKCS#8)
پشتیبان‌گیری/بازیابی	Cloning (HSM to HSM) Manual Synchronization (among multiple HSMs) Partition Backup (HSM to USB Tokens) M-of-N Secret sharing (HSM to USB Tokens)
تولید عدد تصادفی	Hardware-based True Noise Source NIST SP 800-90A compliant CTR-DRBG
پیاده‌سازی سخت افزاری الگوریتم‌های رمزنگاری و پروتکل‌های امنیتی بومی/اختصاصی	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
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)

ویژگی‌های راهبردی HSM صدف نسبت به محصولات خارجی

- دسترسی دشوار به HSMهای خارجی و پشتیبانی نامناسب از آن‌ها به دلیل تحریم‌های اقتصادی و فقدان نمایندگی معتبر فروش در داخل کشور
- بی اطلاعی از معماری امنیتی HSMهای خارجی و نگرانی جدی در مورد احتمال آلودگی آن‌ها به انواع بدافزارهای نرم‌افزاری و سخت‌افزاری و در نتیجه سرقت اطلاعات حساس
- تضمین امنیت کلیدهای رمزنگاری در زیرساخت‌ها و سامانه‌های شرکت ارتباطات سیار ایران، و سایر سامانه‌های اطلاعاتی حساس کشور نظیر بانک‌ها، مراکز صدور گواهی دیجیتال، مراکز صدور انواع کارت هوشمند
- امکان سفارشی‌سازی محصول برای انواع نیازهای داخلی و پشتیبانی از الگوریتم‌های رمزنگاری بومی

Algorithm	SADAF KISH	SADAF MAKRAN	کارایی
RSA 1024	1200	70	Sign/Sec
RSA 2048	800	10	
AES 256 ECB	2000	2000	Enc/Sec

اهداف

- رفع نیاز داخلی شرکتها، سازمانها و ادارات
- رفع نیاز سامانه‌های حیاتی، شبکه مالی و پرداخت
- بومی‌سازی دانش و تجربه تولید یک محصول حساس امنیتی با مشارکت و همکاری مجموعه وسیعی از متخصصان داخلی از شرکت‌های ارتباطات سیار ایران، صنایع قطعات الکترونیک (صقا) شیراز، امن‌افزارگستر شریف، هویتا، پندارکوشک ایمن، و مرکز آپا دانشگاه صنعتی شریف و نیز اعضای هیات علمی دانشگاه‌های معتبر کشور در پژوهشکده پارسا

آدرس: تهران، طرشت، نبش بلوار شهید صالحی و بلوار شهید اکبری، برج فناوری شریف، واحد ۱۰۸ - تلفن: ۶۵۰۱۳۰۳۲ وبگاه: www.parsasharif.ir - رایانامه: info@parsasharif.ir