مشخصات فنی ماژول امنیت سخت‌افزاری صدف	
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
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 Synchronizatoin (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 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 ماژول امنیت سخت‌افزاری صدف			
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)			**تصدیق اصالت**
Syslog			**Logging/Audit**
TLSv1.2			**پروتکل ارتباطی**
PKCS#11, Java JCA/JCE, OpenSSL Engine, Microsoft CNG (KSP)			**API**
Linux/Unix, Windows			**سیستم عامل**
Algorithm	**LAVAN**	**KISH**	**کارایی (TPS)**
RSA 1024	4500	4500	**RSA Sign/Sec**
RSA 2048	900	2200	
RSA 4096	170	350	
AES 256	8000	12000	**Symmetric Enc/Sec**
TDES	8000	12000	
RSA 1024	1 sec	1 sec	**RSA KeyPair Generation Time**
RSA 2048	3 sec	3 sec	
RSA 4096	20 sec	20 sec	
پشتیبانی می‌شود.			**High Availability (HA) Active-Active Failover Loadbalancing**
پشتیبانی می‌شود.			**Network Time Protocol (NTP)**
• Network Access Control Rules • SNMP			**Network Management**
+ 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, OTA • Secure Email: Mozilla Thunderbird			**پشتیبانی از برنامه‌های کاربردی**
+ Ethernet port (1 Gbps) + USB and Serial ports (for HSM Management) + LED (Power, Tamper) + LCD + PED (PIN Entry Device)			**واسط‌ها و پورت‌های ارتباطی فیزیکی**