

Потенциал

BOYA HSM

BoYa HSM – это криптографический модуль безопасности «общего назначения», который предоставляет сервисы шифрования данных, генерации и проверки ЭЦП, хеширования, аутентификации сообщений (MAC), генерации случайных чисел и управления криптографическими ключами для бизнес приложений и систем.

Модуль производства КНР и является прямым аналогом Thales (SafeNet) ProtectServer, LUNA HSMs, Entrust nShield HSM.

Модуль широко используется в электронной коммерции, онлайн-банкинге, электронном правительстве и в других информационных сервисах предприятий.

HSM обеспечивает уровень безопасности и защиты на основе стандарта FIPS 140-2 Level 3.

Характеристики продукта:

- Поддержка алгоритмов
 - RSA 1024/2048/3072/4096 бит,
 - ECDSA с разными параметрами P/K/B кривых,
 - 3DES 128/192-бит
 - AES 128/192/256-бит
 - DSA 1024/2048/3072 бит
 - SHA1, SHA2, MD5
 - HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512
- Безопасное хранение ключей внутри HSM: до 100 пар ключей RSA, 100 пар ключей ECDSA, 100 пар ключей DSA и 2048 симметричных ключей шифрования.
- Управление полномочиями пользователей: поддержка нескольких пользовательских ролей (администратора, оператора и т.д.).
- Поддержка стандартных криптографических интерфейсов PKCS#11, JCE;
- Балансировка нагрузки: до 10 модулей HSM могут работать параллельно в кластере и в отказоустойчивом режиме. Кластер легко разворачивается и требует только настройки IP-адреса HSM в конфигурационном файле.

Item		Low	Base	High
Key Storage	RSA, ECDSA	100 pairs	100 pairs	100 pairs
	Symmetric Key	2048	2048	2048
1024 RSA key generation		40 pair/s	80 pair/s	150 pair/s
1024 RSA sign		6200 Tps	6200 Tps	6200 Tps
1024 RSA verify		40000 Tps	40000 Tps	45000 Tps
2048 RSA key generation		5 pair/s	15 pair/s	30 pair/s
2048 RSA sign		1300 Tps	1300 Tps	3200 Tps
2048 RSA verify		10000 Tps	10000 Tps	20000 Tps
AES en/decryption		400Mbps	800Mbps	4200Mbps
3DES en/decryption		270Mbps	270Mbps	560Mbps
Printing		Optional	Optional	Optional
Maximum concurrent		1000	2000	4000
Interface		RJ-45 10/100/1000Mb x2	RJ-45 10/100/1000Mb x2	RJ-45 10/100/1000Mb x2 SFP 10Gb x2
Specifications		2U		
Dimensions(wide x length x high)		440x520x89mm		
Weigh		12Kg(15Kg)		
Power		220V,50Hz,350W Redundant power		
Power dissipation		280W		
Protocol		TCP/IP		
MTBF		50000h		
Operating temperature		10°C-50°C		
Uncondensable working humidity		5%-85%		
Storage temperature		0°C-60°C		
Uncondensable storage humidity		5%-95%		

