|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1** | **Parâmetro** | **Opção** | **Definição** | **Configuração default** |
| 2 | PIN length | 4 ... 12 | Este valor é usado pelo HSM para definir o tamanho do PIN encriptado | 4 |
| 3 | Echo | On ou Off | Quando configurado como 'On', os passwords, valores secretos e componentes são mostrados na tela de console quando digitados. | Off |
| 4 | Atalla ZMK variant Support | On ou Off | Para interoperabilidade com sistemas Atalla | Off |
| 5 | Transaction key scheme | Racal, Australian ou None | Esquemas de transação de chaves são técnicas onde chaves de criptografias de dados são trocadas em cada transação de uma maneira que não podem ser entendidas por uma terceira parte. O payShield suporta três tipos de esquemas: Racal (i.e. Thales), Australiano (AS2805) e DUKPT. Os esquemas Racal e Australiano podem conflitar em determinados comandos. O uso de comandos DUKPT não é afetado por esta configuração. | None |
| 6 | User storage key length | Single, Double, Triple ou Variable | Este é o tamanho das chaves armazenadas no armazenamento de usuário; pode possuir os tamanhos simples, duplo, triplo ou variável. | Single |
| 7 | Display general information on payShield Manager landing page | Yes ou No | Quando configurado como 'Sim', a página inicial do payShield Manager mostrará informações básicas do HSM. | No |
| 8 | Default LMK identifier | 0 ... 99 | Identifica a LMK padrão, a qual o HSM usará caso receber um comando que não especifique explicitamente qual LMK será usada. | 0 |
| 9 | Management LMK identifier | 0 ... 99 | Identifica a LMK de gerência, a qual será usada para autorizar certas funções de gestão e criptografar a chave MAC de auditoria. | 0 |
| 10 | Enforce Atalla variant match to Thales key type | Yes ou No | Este parâmentro é válido quando 'Atalla ZMK variant Support' é 'Yes' | No |
| 11 | Select clear PINs | Yes ou No | Isto habilita o suporte para PINs em claro para os comandos de host 'NG' e BA'. O modo autorizado também é requisitado para que estes comandos serem processados. | No |
| 12 | Enable ZMK translate command | Yes ou No | Habilita o comando 'BY' que permite a tradução de ZMKs por uma outra ZMK. O modo autoriazado é necessário para este comando ser processado. | No |
| 13 | Enable X9.17 for import | Yes ou No | Habilita o suporte do mecanismo ANSI X9.17 para importação de chaves. | No |
| 14 | Enable X9.17 for export | Yes ou No | Habilita o suporte do mecanismo ANSI X9.17 para exportação de chaves. | No |
| 15 | Solicitation batch size | 1 ... 1024 | Método suportado pelo payShield para permitir que clientes selecionem seus próprios PINs. | 1024 |
| 16 | Prevent single-DES keys masquerading as double or triple-length keys | Yes ou No | Quando configurado como 'Sim', todos os comandos do HSM que importem chaves 3DES de tamanho duplo ou triplo garantirão que a chave importada não é uma chave DES de tamanho simples mascarada como uma chave de tamanho duplo ou triplo. | Yes |
| 17 | Single/Double length ZMKs | Single ou Double | O tamanho da Zone Master Key, simples ou duplo. | Double |
| 18 | Decimalization table Encrypted/Plaintext | Encrypted ou Plaintext | Esta opção determina se a tabela de decimalização será encriptada ou em texto claro. | Encrypted |
| 19 | Enable Decimalization Table Checks | Enabled ou Disabled | Os valores da tabela de decimalização usados para derivar e verificar valores offset de PIN. | Enabled |
| 20 | PIN encryption algorithm | A ou B | Isto seleciona o algoritimo de encriptação do PIN a ser usado quando PIN são encriptados para serem armazenados pelo emissor. O método A, método Visa, é compatível com versões antigas de HSM. O método B, método Racal, possui um algoritmo mais forte. | A (Visa Method) |
| 21 | Use default card issuer password | Yes ou No | Esta opção determina se os cartões emitidos pelo HSM devem manter os passwords do momento de sua emissão ou não. | Yes |
| 22 | Card issuer password (local) | 8 caracteres | Parâmetro válido quando 'Use default card issuer password' é 'No' | n/a |
| 23 | Authorized State required when importing a key under an RSA Key | Yes ou No | Esta configuração determina se o modo autorizado é mandatório para importação de chaves sob chaves RSA. | Yes |
| 24 | Minimum HMAC key length in bytes | 5 ... 64 | Determina o tamanho mínimo de uma chave HMAC gerada pelo HSM. | 10 |
| 25 | Enable PKCS#11 import and export for HMAC keys | Yes ou No | Determina se os comandos de host LU e LW podem importar ou exportar chaves HMAC no formato PKCS#11 | No |
| 26 | Enable ANSI X9.17 import and export for HMAC keys | Yes ou No | Determina se os comandos de host LU e LW podem importar ou exportar chaves HMAC no formato ANSI X9.17 | No |
| 27 | Enable ZEK encryption of ASCII data or Binary data or None | ASCII, Binary ou None | Determina o tipo de mensagem que pode ser processada com os comandos de criptografia de mensagem, M0, M2 e M4. | None |
| 28 | Restrict Key Check Value to 6 hex chars | Yes ou No | Determina se o valor de checagem das chaves (KCV) deve ser restringido a apenas 6 caracteres hexadecimais. | Yes |
| 29 | Enable multiple authorized activities | Yes ou No | Se habilitada, permite a seleção precisa de atividades autorizadas. | Yes |
| 30 | Allow persistent authorized activities | Yes ou No | Se habilitada, permite atividades autorizadas persistentes mesmo após o reinício da unidade. | Yes |
| 31 | Enable support for variable length PIN offset | Yes ou No | Se habilitada, permite os comandos de Offset de PIN 3624 da IBM retornarem um Offset de tamanho correspondente ao PIN. | No |
| 32 | Enable weak PIN checking | Yes ou No | Se habilitada, os comandos de host do HSM que geram/derivam PIN garantirão que o novo PIN não seja considerado fraco. | No |
| 33 | Check new PINs using global list of weak PINs | Yes ou No | Se habilitada, os comandos de host do HSM que geram/derivam PIN garantirão que o novo PIN não corresponda a um dos listados na tabela global de PINs excluídos do HSM. | No |
| 34 | Check new PINs using local list of weak PINs |  | Se habilitada, os comandos de host do HSM que geram/derivam PIN garantirão que o novo PIN não corresponda a um dos listados na tabela local de PINs excluídos, enviada junto ao comando. | No |
| 35 | Check new PINs using rules | Yes ou No | Se habilitada, os comandos de host do HSM que geram/derivam PIN garantirão que o novo PIN não corresponda às regras listadas: | No |
| 36 | Enable PIN Block Format 34 as output format for PIN translations to ZPK | Yes ou No | Se habilitada, o HSM permitirá o uso do PIN Block formato 34. | No |
| 37 | Enable translation of account number for LMK encrypted PINs | Yes ou No | Se habilitada, permite que o PAN de um PIN encriptado pela LMK seja alterado sem alterar o PIN do portador do cartão. | No |
| 38 | Enable 2DES LMK encryption of 3DES/2048-bit RSA keys | Yes ou No | Se habilitada, permite a criptografia de chaves 3DES de tamanho triplo e chaves RSA maiores que 1024 btis por uma LMK Variant de tamanho duplo. | Yes |
| 39 | Use HSM clock for date/time validation | Yes ou No | Se habilitada, o HSM usa seu relógio de tempo real integrado para validar dados temporais nos blocos opcionais nos cabeçalhos de key blocks. | Yes |
| 40 | Additional padding to disguise key length | Yes ou No | Se habilitada, o HSM oculta o tamanho de chaves simples ou duplas dentro de um key block adicionando 8 ou 16 bytes extras de preenchimento. | No |
| 41 | Key export and import in trusted format only | Yes ou No | Se habilitada, o HSM somente importará/exportará chaves usando o formato Key Block. | Yes |
| 42 | Protect MULTOS Cipher Data Checksums | Yes ou No | Usada para controlar se a soma de verificação gerada sob dados sensíveis necessita encriptação. | Yes |
| 43 | Enable Key Scheme Tag 'X' (X9.17) for storing keys under LMK | Yes ou No | Se habilitada, chaves encriptadas sob a LMK Variant permitirão o uso do esquema de chave 'X'. | No |
| 44 | Enable use of Tokens in PIN Translation | Yes ou No | Determina se os comandos de tradução de PIN suportarão o uso de Tokens nos campos de PAN. | No |
| 45 | Enable use of Tokens in PIN Verification | Yes ou No | Determina se os comandos de validação de PIN suportarão o uso de Tokens nos campos de PAN. | No |
| 46 | Allow Error light to be extinguished when viewing Error Log | Yes ou No | Quando 'No', o LED de erro permanecerá aceso quando o log de erros for lido. | No |
| 47 | Ensure LMK Identifier in command corresponds with host port | Yes ou No | Quando usando multiplas LMK Variant, se configurado como 'No', o campo de identificação da LMK no comando de host tem prioridade sobre a porta TCP usada. Se configurado como 'Yes', o campo de identificação da LMK no comando de host deve corresponder a porta TCP usada. | No |
| 48 | Ignore LMK ID in Key Block Header | Yes ou No | Quando 'Yes', o ID de LMK no cabeçalho do Key Block Thales será ignorado. | No |
| 49 | Enforce NIST recommendations when encrypting AES keys using RSA | Yes ou No | Quando 'Yes', o HSM não permitirá chaves RSA de pouca força encriptarem chaves AES fortes. NIST SP800-57 | Yes |
| 50 | Enable import and export of RSA Private keys | Yes ou No | Se habilitada, os comandos de host L6 e L8 estarão disponíveis e permitirão a importação e exportação de chaves privadas RSA. | No |
| 51 | Enable import of a ZMK | Yes ou No | Se habilitada, o comando de console IK e o comando de host A6 e GI permitirão a importação de uma ZMK. | No |
| 52 | Enable export of a ZMK |  | Se habilitada, o comando de console KE e o comando de host A8 e GK permitirão a exportação de uma ZMK. | No |
| **As configurações abaixo afetam o PCI HSM Compliance** | | | | |
| 53 | Enable single-DES | Yes ou No | Se habilitada, permite o uso de chaves DES de tamanho simples. | No |
| 54 | Card/password authorization | Card ou Password | Esta opção seleciona o método de autenticação do security officers quando requisitam mudanças no estado de segurança. | Card |
| 55 | Restrict PIN block usage for PCI HSM compliance | Yes ou No | Se habilitada, o HSM previnirá traduções de PIN Block de formato ISO 0, 1, 3 e 4 para formatos não ISO. O HSM também previnirá tradução de PIN Block que utilizem o PAN em sua formação para PIN Block que não utilizem. | No |
| 56 | Enforce key type 002 separation for PCI HSM compliance | Yes ou No | Se habilitada, o HSM separará as chaves atualmente encriptadas pelo par 14-15 da LMK (key type 002). | No |
| 57 | Enforce Authorization Time Limit | Yes ou No | Se habilitada, tempo máximo de autorização para comandos de console será de 720 minutos. | No |
| 58 | Enforce Multiple Key Components | Yes ou No | Se habilitada, todas as LMKs e chaves formadas no HSM devem ser formadas por pelo menos dois componentes distintos. | No |