

**nShield - Geral**

Índice

[1. Security World 3](#_Toc48120827)

[2. OCS 4](#_Toc48120828)

[3. Chave 5](#_Toc48120829)

[4. Release Notes 7](#_Toc48120830)

# Security World

- Tipos de cartão

- Administrator Card Set (ACS) – controle de acesso para recuperar ou substituir funcionalidade

- Operator Card Sets (OCSs) – controle de acesso a chaves de criptografia

- Quorum

N = número total de cartão

K = número minimo de cartão para realizar a tarefa

N/K; K>N

- Viewing Security World using the command line

|  |
| --- |
| $ **/opt/nfast/bin/nfkminfo --key-list**  Key list - 9 keys  AppName simple Ident c4  AppName simple Ident c2  AppName simple Ident c3  AppName simple Ident c5  AppName pkcs11 Ident uc8b7c43bcdad9c9de0b1deed737c4e0f088c5(…)  AppName simple Ident chave01  AppName simple Ident c1  AppName custom Ident e4c1b3b11499a5ec701b5437ddf73a2cd61dbff6  AppName simple Ident c10 |

# OCS

- Creating an Operator Card Set (OCS) using the nShield Connect front panel

|  |
| --- |
| - 3 > 5 > 1  - [NOME\_OCS]  - 2/3; K/N  - 0 (no time out)  - Not persistent - Persistent - Remoteable/Persistent  - Blank card > OK > Set Card Protection Passphrase > [SENHA] |

- Viewing card sets using the command line

|  |
| --- |
| $ **/opt/nfast/bin/nfkminfo --cardset-list**  Cardset list - 1 cardsets: (P)ersistent/(N)ot, (R)emoteable/(L)ocal-only  Operator logical token hash k/n timeout name  8b7c43bcdad9c9de0b1deed737c4e0f088c5e4ce 2/3 none-NL labocs |

# Chave

- Generating keys using the command line

|  |
| --- |
| **$ sudo /opt/nfast/bin/generatekey --generate simple cardset=labocs plainname=chave ident=chave protect=token recovery=yes** |

- Viewing keys using the command line

|  |
| --- |
| $ **/opt/nfast/bin/nfkminfo --key-list**  Key list - 10 keys  AppName simple Ident c4  AppName simple Ident c2  AppName simple Ident c3  AppName simple Ident chave  AppName simple Ident c5  AppName pkcs11 Ident uc8b7c43bcdad9c9de0b1deed737c4e0f088c5(…)  AppName simple Ident chave01  AppName simple Ident c1  AppName custom Ident e4c1b3b11499a5ec701b5437ddf73a2cd61dbff6  AppName simple Ident c10 |

- Visualizar chave de acordo com o tipo de proteção

|  |
| --- |
| **$ /opt/nfast/bin/nfkminfo --name-list**  Keys with module protection:  key\_simple\_c1 `c1'  key\_simple\_c3 `c3'  key\_simple\_c5 `c5'  Keys protected by cardsets:  key\_custom\_e4c1b3b11499a5ec701b5437ddf73a2cd61dbff6 `DES3'  key\_pkcs11\_uc8b7c43bcdad9c9de0b1deed737c4e0f088c5(…) `chave02'  key\_simple\_c10 `c10'  key\_simple\_c2 `c2'  key\_simple\_c4 `c4'  key\_simple\_chave `chave'  key\_simple\_chave01 `chave01' |

- Apagar chave

|  |
| --- |
| - Erase the OCS that is used to protect it  - Erase the Security World completely |

- Utilizando ROCS para mudar o tipo de proteção da chave

|  |
| --- |
| $ **sudo /opt/nfast/bin/rocs**  `rocs' key recovery tool  Useful commands: `help', `help intro', `quit'.  rocs> **list cardsets**  No. Name Keys (recov) Sharing  module 4 (4) ---  1 labocs 5 (5) 2 of 3  rocs> **list keys**  No. Name App Protected by  1 c4 simple labocs  2 c2 simple **module**  3 c3 simple **module**  4 c5 simple **module**  5 chave02 pkcs11 labocs  6 chave01 simple labocs  7 c1 simple **module**  8 DES3 custom labocs  9 c10 simple labocs  rocs> **set changeprot**  rocs> **module 1**  rocs> **list cardsets**  No. Name Keys (recov) Sharing  module 4 (4) ---  1 labocs 5 (5) 2 of 3  rocs> **target labocs**  rocs> **mark 2**  rocs> **recover**  admin card  1/3 and 2/3 card  rocs> **save**  rocs> **list keys**  No. Name App Protected by  1 c4 simple labocs  2 c2 simple labocs  3 c3 simple module  4 c5 simple module  5 chave02 pkcs11 labocs  6 chave01 simple labocs  7 c1 simple module  8 DES3 custom labocs  9 c10 simple labocs  rocs> **exit** |

# Release Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Caio Ferreira | Primeira versão do documento | 12/08/2020 |
|  |  |  |