AIX Versão 7.2

4765 PCIe Cryptographic Coprocessor AIX CCA Support Program - Manual de Instalação 4.4

AIX Versão 7.2

4765 PCIe Cryptographic Coprocessor AIX CCA Support Program - Manual de Instalação 4.4

Nota
Antes de utilizar estas informações e o produto suportado por elas, leia as informações no “Avisos” na página 65.

Esta edição se aplica ao AIX Versão 7.2 e a todas as liberações e modificações subsequentes até que seja indicado de outra forma em novas edições.

Índice

Sobre Esse Documento

Estas informações de instalação descrevem a Liberação 4.4 do IBM® Common Cryptographic Architecture (CCA) Support Program (daqui em diante referido como Support Program) para o IBM 4765 PCIe Cryptographic Coprocessor. O Support Program inclui drivers de dispositivos, utilitários e o código do coprocessador do CCA.

Use essa informação para ajudar com as tarefas a seguir:
- Obtenha o Support Program pela Internet
- Carregue o software para um computador host e dentro dos coprocessadores.
- Use os utilitários fornecidos com o Support Program para:
  - Carregue o function-control vector (FCV) no coprocessador.
  - Inicialize um ou mais coprocessadores
  - Crie e gerencie dados de controle de acesso
  - Crie uma chave mestra e key-encrypting keys (KEKs) primárias
  - Gerencie o keystore no nó criptográfico
  - Crie as listas de arquivo de inicialização de nó para definir e configurar outros nós criptográficos
- Vincule seu software de aplicativo às bibliotecas CCA
- Obtenha a orientação para as considerações de segurança no desenvolvimento de aplicativo e nas práticas operacionais

Público

O público para essa publicação inclui:
- Administradores do sistema que instalam o software
- Oficiais de segurança responsáveis pelo sistema de controle de acesso do coprocessador
- Os programadores do sistema e os programadores do aplicativo que determinam como o software deve ser usado

Destaque

As seguintes convenções de destaque são usadas neste documento:

Negrito	Identifica os comandos, sub-rotinas, palavras-chaves, arquivos, estruturas, diretórios e outros itens cujos nomes são predefinidos no sistema. Também identifica os objetos gráficos como botões, rótulos e ícones que o usuário seleciona.
Itálico	Identifica os parâmetros cujos nomes ou valores reais devem ser fornecidos pelo usuário.
`Espaçamento Uniforme`	Identifica exemplos de valores de dados específicos, exemplos de texto semelhante ao que você pode visualizar, exemplos de partes de código de programa semelhantes ao que você pode gravar como um programador, mensagens do sistema ou informações que devem realmente ser inseridas.

Distinção entre Maiúsculas e Minúsculas no AIX

Tudo no sistema operacional AIX faz distinção de maiúsculas e minúsculas, o que significa que ele distingue entre letras maiúsculas e minúsculas. Por exemplo, você pode usar o comando **ls** para listar arquivos. Se você digitar `LS`, o sistema responderá que o comando `não foi localizado`. Da mesma forma, `FILEA`, `FiLea` e `filea` são três nomes de arquivo distinto, mesmo se eles residirem no mesmo diretório. Para evitar que ações indesejadas sejam executadas, certifique-se de usar sempre a distinção entre maiúsculas e minúscula correta.

ISO 9000

Os sistemas de qualidade registrados ISO 9000 foram utilizados no desenvolvimento e fabricação deste produto.

Publicações Relacionadas

As publicações do PCIe Cryptographic Coprocessor e os aplicativos criptográficos comerciais são, em geral, o seguinte:

As publicações de hardware criptográfico estão disponíveis no website do *CryptoCards* em http://www.ibm.com/security/cryptocards:

- *Referência e Guia de Serviços Básicos do IBM CCA para os IBM 4765 PCIe e IBM 4764 PCI-X Cryptographic Coprocessors*

4765 PCIe Cryptographic Coprocessor AIX CCA Support Program Installation 4.4

Para usar as informações efetivamente, você deve estar familiarizado com os comandos, chamadas do sistema, sub-rotinas, formatos de arquivo e arquivos especiais.

O que há de novo no 4765 PCIe Cryptographic Coprocessor AIX CCA Support Program Installation 4.4

Leia sobre as informações novas ou significativamente mudadas para a coleção de tópico do 4765 PCIe Cryptographic Coprocessor AIX CCA Support Program Installation 4.4.

Como Ver o Que Há de Novo ou Foi Alterado

Neste arquivo PDF, é possível ver barras de revisão (|) na margem esquerda que identificam informações novas e alteradas.

Dezembro de 2015

As informações a seguir são uma sumarização das atualizações feitas nesta coleção de tópicos:

- O IBM PCIe Cryptographic Coprocessor foi atualizado para o IBM PCIe Cryptographic Coprocessor Versão 4.4.55 nos tópicos a seguir:
  - "4765 PCIe Cryptographic Coprocessor AIX CCA Support Program Installation 4.4"
  - "Instalando a liberação base do Support Program 4.4" na página 3
  - "Obtendo Hardware e Software do Coprocessador"

  É possível fazer download do software de coprocessador a partir do website do IBM PCIe Cryptographic Coprocessor http://www-03.ibm.com/security/cryptocards/pciecc/release4455.shtml.

Visão geral do processo de instalação do Support Program

Esta visão geral do AIX CCA explica o procedimento para instalar e operar o IBM Cryptographic Coprocessor Support Program em um computador host.

Informações relacionadas:

"Instalando o Support Program" na página 2
Procedimento para Instalar o IBM Common Cryptographic Architecture (CCA) Support Program no computador host do coprocessador.

Obtendo Hardware e Software do Coprocessador

Informações sobre selecionar, instalar e pedir o hardware de coprocessador e fazer download do software.

As seguintes seções descrevem como:

- Fazer pedidos de coprocessadores
- Fazendo os pedidos de coprocessador IBM 4765
- Instalando o hardware IBM 4765
- Obtendo o software do coprocessador

Adquirindo Coprocessadores

O IBM 4765-001 é pedido na IBM como um tipo e modelo de máquina. O coprocessador requer um slot PCIe que aceite um adaptador PCIe de 2/3 de comprimento.

O software suporta até oito coprocessadores por sistema, dependendo do número de slots PCIe disponíveis.

Fazendo Pedidos de Coprocessador IBM 4765

Para pedir o hardware do coprocessador, entre em contato com o representante local da IBM ou seu Parceiro de Negócios IBM e peça o modelo e os recursos selecionados.

Os clientes nos Estados Unidos podem entrar em contato com a IBM Direct pelo número 1-800-IBM-CALL. Mencione, especificamente, o *IBM 4765* com o pedido a ser direcionado ao grupo que processa os pedidos do IBM 4765.

Instalando o IBM hardware 4765

O IBM 4765 é instalado de uma maneira semelhante a outros adaptadores PCIe. Siga o processo descrito no *IBM 4765 PCIe Cryptographic Coprocessor Installation 4.4* para obter informações detalhadas.

Obtendo o software do coprocessador

O software pode ser obtido fazendo seu download do Web site: http://www.ibm.com/security/cryptocards/pciecc/ordersoftware.shtml.

Instalando o Support Program

Procedimento para Instalar o IBM Common Cryptographic Architecture (CCA) Support Program no computador host do coprocessador.

O IBM Common Cryptographic Architecture (CCA) Support Program consiste em vários componentes, incluindo:

- Drivers de dispositivo e um sistema operacional para o hardware de coprocessador criptográfico PCIe
- Suporte para a Application Program Interface (API) do IBM Common Cryptographic Architecture (CCA)
- Um function-control vector (FCV)

  Nota: Um FCV é um valor assinado fornecido pela IBM. Ele permite que o aplicativo CCA no coprocessador gere um nível de serviços criptográficos consistentes com regulamentações de importação e de exportação de implementação criptográfica aplicável.
- Os aplicativos utilitários, nos quais o coprocessador é executado na máquina host, devem estar instalados

Para instalar e configurar o IBM Common Cryptographic Architecture (CCA) Support Program, execute essas etapas:

1. Escolha os pacotes de suporte da plataforma que são apropriados à configuração:

   AIX 6.1 ou posterior.

   Consulte “Obtendo Hardware e Software do Coprocessador” na página 1 para obter detalhes.

2. Faça um pedido do hardware para a IBM ou para seu Parceiro de Negócios IBM. Consulte "Obtendo Hardware e Software do Coprocessador" na página 1, que descreve como solicitar e receber o hardware do co-processador da IBM.
3. Faça download do Support Program para seu sistema operacional. Consulte "Obtendo Hardware e Software do Coprocessador" na página 1, que descreve como instalar o sistema operacional integrado e o programa de aplicativo CCA no PCIe Cryptographic Coprocessor.
4. Instale o Support Program no computador host do coprocessador.
5. Instale o hardware do coprocessador. Consulte "Obtendo Hardware e Software do Coprocessador" na página 1 para obter detalhes.
6. Carregue o software do coprocessador. Consulte "Carregando e descarregando o software no coprocessador" na página 7 para obter detalhes.
7. Configure um nó de teste do CCA. É possível estabelecer um nó criptográfico CCA usando os utilitários fornecidos com o Support Program ou vincular os programas de aplicativos com a API do CCA. Além disso, verifique o controle de acesso e outros requisitos de configuração impostos pelo software de aplicativo que você planeja usar com o IBM 4765. O utilitário CCA Node Management (CNM), descrito no "Gerenciando o nó criptográfico usando os utilitários CNM e CNI" na página 16, inclui as funções de configuração e de gerenciamento necessárias para:
   - Carregar o FCV
   - Criar e editar os dados de controle de acesso
   - Gerenciar a chave mestra do coprocessador
   - Gerenciar as key encrypting keys (KEKs) primárias
   - Gerenciar o armazenamento de chaves de dados
   - Criar listas (scripts) para o utilitário CCA Node Initialization (CNI)
8. Execute programas de teste que usam as bibliotecas do CCA. Consulte "Construindo Aplicativos para Usar com a API CCA" na página 39 para obter detalhes.

Informações relacionadas:

"Obtendo Hardware e Software do Coprocessador" na página 1
Informações sobre selecionar, instalar e pedir o hardware de coprocessador e fazer download do software.

"Carregando e descarregando o software no coprocessador" na página 7
Após instalar o IBM Common Cryptographic Architecture (CCA) Support Program no computador host, use o Coprocessor Load Utility (CLU) para carregar o sistema operacional do coprocessador e o aplicativo CCA no coprocessador.

"Gerenciando o nó criptográfico usando os utilitários CNM e CNI" na página 16
Um computador que fornece serviços criptográficos, como geração de chave e suporte a assinatura digital, é definido como um *nó criptográfico*.

Instalando a liberação base do Support Program 4.4

As instruções para instalar o Support Program no computador host do coprocessador.

Pré-requisito

Antes de iniciar a instalação, escolha os pacotes de suporte da plataforma que são apropriados para a configuração. Consulte "Obtendo Hardware e Software do Coprocessador" na página 1 para obter os detalhes sobre requisitos de software e hardware para AIX.

Nota: Se você não estiver instalando o programa pela primeira vez, faça backup dos arquivos de armazenamento de chaves.

Para instalar o Support Program:

1. Insira o comando **smitty install_all** .

2. Insira o local das imagens de instalação obtidas usando o procedimento descrito na seção Obtendo o Software do Coprocessador em "Obtendo Hardware e Software do Coprocessador" na página 1. Pressione Enter.
3. Insira `csufx.4765.cca csufx.4765.man` no campo **Instalação de SOFTWARE** ou pressione F4 (Exibir) para selecionar na lista. Verifique se **Instalar AUTOMATICAMENTE o software de requisito** está configurado como Sim e se **ACEITAR novos contratos de licença** está configurado como Sim. Use a tecla tab para alternar ou a tecla F4 (Exibir) para listar. Pressione Enter e pressione Enter novamente para continuar quando solicitado `TEM CERTEZA`.
4. Saia de **smitty** usando a tecla F10 (Sair).
5. Leia o arquivo `/usr/lpp/csufx.4765/README`. Esse arquivo contém as informações mais recentes sobre o produto Support Program.
6. Use os utilitários de configuração para configurar o software, conforme descrito no "Configurando o Support Program".

Configurando o Support Program

Esta seção descreve os utilitários e o comando do sistema usados para configurar o software do CCA Cryptographic Coprocessor Support Program.

csufadmin

Especifica as permissões de acesso ao sistema associadas aos utilitários csufkeys, csufappl, csufclu (Coprocessor Load Utility), csufcnm (Cryptographic Node Management) e csufcni (Cryptographic Node Initialization).

As permissões padrão restringem o uso desses utilitários para o usuário raiz e para usuários no grupo do sistema. Use o utilitário csufadmin para modificar essas permissões.

csufappl

Especifica as permissões de acesso ao sistema associadas às bibliotecas do CCA.

As permissões padrão restringem o uso das bibliotecas do CCA para o usuário raiz e os membros do grupo do sistema. Use o utilitário csufappl para permitir que outros grupos usem os serviços fornecidos pela API do CCA.

csufkeys

Cria e identifica o arquivo e os nomes do diretório dos locais onde as chaves criptográficas e listas de chaves estão armazenadas. O programa de instalação define, no Object Data Manager (ODM) do AIX, os diretórios padrão a seguir:

- Diretório de lista de gravação da chave de AES: `/usr/lpp/csufx.4765/csufkeys/aeslist`
- Arquivo de armazenamento de chaves de AES: `/usr/lpp/csufx.4765/csufkeys/aes.keys`
- Diretório de lista de gravação da chave de DES: `/usr/lpp/csufx.4765/csufkeys/deslist`
- Arquivo de armazenamento de chaves de DES: `/usr/lpp/csufx.4765/csufkeys/des.keys`
- Diretório de lista de gravação da chave de PKA: `/usr/lpp/csufx.4765/csufkeys/pkalist`
- Arquivo de armazenamento de chaves de PKA: `/usr/lpp/csufx.4765/csufkeys/pka.keys`

Use o utilitário csufkeys para alterar os locais de armazenamento.

Nota: Ao inicializar o armazenamento de chaves usando o utilitário Cryptographic Node Management, assegure-se de especificar os diretórios ODM definidos por esse utilitário.

odmget

Verifica os nomes do arquivo de armazenamento de chaves com o comando do sistema **odmget**. É possível verificar os nomes de armazenamento de chaves usado pelo CCA Support Program, inserindo o comando **odmget csufodm**. Os quatro atributos do nome do parâmetro especificam os valores a seguir:

- **csuaesds**: O arquivo que contém os registros de chave de AES

- **csuaesld**: O diretório que contém os arquivos de lista de gravação da chave de AES
- **csudesds**: O arquivo que contém os registros de chave de DES
- **csudesld**: O diretório que contém os arquivos de lista de gravação da chave de DES
- **csupkads**: O arquivo que contém os registros de chave de PKA
- **csupkald**: O diretório que contém os arquivos de lista de gravação da chave de PKA

Ao inicializar o armazenamento de chaves de CCA com o utilitário CNM ou com o verbo de CCA csnbksi, deve-se usar os nomes dos arquivos retornados do ODM. Use o utilitário csufkeys para alterar esses nomes dos arquivos.

Os verbos DES_Key_Record_List, PKA_Key_Record_List e AES_Key_Record_List produzem os arquivos de listas nos diretórios `/usr/lpp/csufx.4765/csufkeys/deslist`, `/usr/lpp/csufx.4765/csufkeys/pkalist` e `/usr/lpp/csufx.4765/csufkeys/aeslist`, respectivamente. Esses são os nomes de diretório padrão. É possível modificar os nomes de diretórios ao instalar o software. Os arquivos de listas serão criados sob sua propriedade, se você solicitar o serviço de lista. Assegure-se de que os arquivos sejam criados no ID do grupo, conforme requerido pela instalação. Isso também pode ser atingido configurando o bit set-group-id-on-execution nesses três diretórios. Consulte os sinalizadores g+s no comando **chmod** para obter mais informações. Se este procedimento não for seguido, os erros serão retornados nos verbos da lista de gravação da chave.

Para designar um Coprocessador do CCA padrão, use o comando EXPORT para configurar a variável de ambiente **CSU_DEFAULT_ADAPTER** como **CRP0***n*, em que *n* = 1, 2, 3, 4, 5, 6, 7 ou 8, dependendo de qual Coprocessador do CCA instalado você deseja como o padrão. Se essa variável de ambiente não for configurada quando o primeiro verbo do CCA de um processo for chamado, o software da CCA usará o Coprocessador CRP01 como o padrão. Se essa variável de ambiente for configurada para um valor inválido, você receberá um erro até a variável de ambiente for configurada para um valor válido.

Informações relacionadas:

"Criando um Rótulo de Chave" na página 36

Permissões do CCA Support Program e de Arquivo AIX

O CCA Support Program depende das permissões de arquivo no nível do grupo para funcionar com precisão.

Os usuários e administradores do Support Program devem ter as permissões de arquivo de grupo corretas nas bibliotecas compartilhadas do CCA, nos utilitários, nos arquivos de armazenamento de chaves e nos diretórios para serem totalmente funcionais e executarem sem erros.

Nota: Os arquivos e diretórios de armazenamento são definidos como os arquivos e diretórios que estão contidos no diretório de armazenamento de chaves. Este diretório inclui o diretório de armazenamento de chave de nível superior, ou seja, na configuração padrão, todos os arquivos e diretórios sob o diretório `/usr/lpp/csufx.4765/csufkeys/deslist` e o próprio diretório `/usr/lpp/csufx.4765/csufkeys` .

Para operar os arquivos e os diretórios do armazenamento de chaves, deve-se possuir um ID de grupo do grupo de usuários do aplicativo, ou seja, o parâmetro groupname, que é utilizado quando o utilitário `csufappl` foi executado.

Além disso, como regra, todos os diretórios de armazenamento de chaves devem ter permissões de arquivo de 2770 (drwxrws---) e serem possuídos pela raiz. Todos os arquivos de armazenamento de chaves devem possuir permissões de arquivo de 660 (-rw-rw----).

O software CCA 4765 e o keystore não podem existir simultaneamente com o software CCA 4764 e o keystore, por causa de conflitos nas bibliotecas e nos banco de dados ODM.

Revisando os erros de hardware do coprocessador

Os erros que ocorrem no hardware do coprocessador do IBM Power Systems são registrados no log de erros do AIX.

Para processar e visualizar o log, insira o seguinte comando:

```
errpt -a -N Cryptn,libxcrypt.a | more
```

Em que *n* é 0, 1, 2, 3, 4, 5, 6 ou 7 (por exemplo, Crypt 0), dependendo de qual log do Coprocessador CCA deseja visualizar.

Informações relacionadas:

"Carregando e descarregando o software no coprocessador" na página 7
Após instalar o IBM Common Cryptographic Architecture (CCA) Support Program no computador host, use o Coprocessor Load Utility (CLU) para carregar o sistema operacional do coprocessador e o aplicativo CCA no coprocessador.

Removendo o Support Program

Se seus arquivos de armazenamento de chaves estiverem nos diretórios padrão, faça backup deles ou salve-os antes de remover o IBM Cryptographic Coprocessor (CCA) Support Program. Remover o software exclui os arquivos de armazenamento de chaves nos diretórios padrão.

Para remover o IBM Cryptographic Coprocessor Support Program, siga estas etapas:

1. Efetue logon como `raiz`.
2. Insira o comando **rmdev -dl Crypt0** . O driver de dispositivo do coprocessador e as outras informações relacionadas são removidos. É possível usar este comando para cada coprocessador do CCA que você planeja remover ou relocalizar.
3. Insira o comando **smitty install_remove** .

   Nota: Quando o prompt aparecer, digite os nomes do produto `csufx.4765.com` e `devices.pciex.14107a0314107b03.rte`.
4. Verifique se o valor de **REMOVER software dependente** está configurado como NO. Além disso, verifique se o valor de **Somente visualização** está configurado como NO.
5. Pressione a tecla **Enter**

Requisitos de hardware e de software do AIX

Os pré-requisitos que são necessários para instalar o CCA.

Hardware

Instale um servidor IBM Power Systems com um coprocessador criptográfico PCIe 4765 disponível.

Durante a instalação do software, o driver interage com o coprocessador para intermediar configurações de interrupção, canais DMA e outros recursos do sistema. Para obter instruções de instalação sobre o hardware do co-processador e o driver de dispositivo, consulte "Obtendo Hardware e Software do Coprocessador" na página 1.

Software

1. IBM AIX 6.1 e posterior.
2. Java Runtime Environment (JRE) versão 1.6.0 ou posterior, que é necessário para executar o utilitário CCA Node Management (CNM).

3. O pacote de software **csufx.4765** deve ser transferido por download do site http://www.ibm.com/security/cryptocards/pcixcc/ordersoftware.shtml . O pacote de software contém os conjuntos a seguir:
   - **csufx.4765.com** - 4765 CCA Support Program
   - **csufx.4765.cca** - 4765 Support Program - Utilitários Comuns
   - **csufx.4765.man** - Páginas do manual do Support Program

Permissões de Arquivo

Gerenciar a permissão de arquivo utilizando o utilitário CCA Node Management (CNM).

O utilitário CCA Node Management (CNM) fornece uma maneira de gerenciar os pontos de controle de acesso. Para ajudar a proteger-se contra distorções acidentais ou intencionais do arquivo executável do utilitário CNM, configure a permissão do arquivo `CNM.jar` para somente leitura e execução. Da mesma forma, para proteger o arquivo de dados dos pontos de controle de acesso, configure a permissão do arquivo do arquivo `csuap.def` para somente leitura.

Carregando e descarregando o software no coprocessador

Após instalar o IBM Common Cryptographic Architecture (CCA) Support Program no computador host, use o Coprocessor Load Utility (CLU) para carregar o sistema operacional do coprocessador e o aplicativo CCA no coprocessador.

Se você obtiver atualizações para o Support Program, use o CLU para recarregar os segmentos necessários do programa. Também é possível carregar o software do fornecedor usando o CLU.

Esta seção inclui:

- Instruções para o uso do CLU para entender quais coprocessadores são instalados e seus status e para instalar e desinstalar o software que é executado dentro do coprocessador
- Uma seção de referência que descreve:
  - Os segmentos de memória do coprocessador
  - Validação do status do coprocessador
  - A sintaxe usada para iniciar o utilitário CLU
  - Códigos de retorno do CLU

Para um maior entendimento dos controles de carregamento do código e das considerações de segurança implementadas pelo coprocessador, consulte o documento de procura *Construindo um Coprocessador Seguro Programável e de Alto Desempenho*, que está disponível na página da biblioteca do website do produto em http://www.ibm.com/security/cryptocards.

Comunicados:

1. Os locais do arquivo referidos nesta seção são os caminhos do diretório padrão.
2. Os códigos de erros retornados pelo driver de dispositivo do coprocessador são apresentados na forma de um número hexadecimal, como X'8040xxxx'. Pode ser possível encontrar os erros, especialmente, quando usar primeiro o utilitário CLU e for menos familiarizados com o produto e seus procedimentos.
3. O Function-Control Vector (FCV) do coprocessador é carregado pelo utilitário CCA Node Management (CNM).

Informações relacionadas:

"Códigos de Erro do Driver de Dispositivo" na página 45
O driver de dispositivo do coprocessador monitora o status da comunicação com o coprocessador e com os registros de status de hardware do coprocessador.

"Gerenciando o nó criptográfico usando os utilitários CNM e CNI" na página 16
Um computador que fornece serviços criptográficos, como geração de chave e suporte a assinatura digital, é definido como um *nó criptográfico*.

Carregando o Software do Coprocessador

Localize os procedimentos para carregar o software no coprocessador nesta seção.

Consulte o arquivo LEIA-ME que acompanha a distribuição do software que você está instalando para nomes de arquivos específicos `.clu`. O arquivo LEIA-ME também pode fornecer informações adicionais que aumentam ou modificam esses procedimentos gerais.

Use os subtópicos a seguir, seguindo esta sequência de tarefas:

1. Em um prompt de comandos, vá para o diretório com o Coprocessor Load Utility (CLU) arquivos e execute o CLU.
2. Determine o software que está atualmente residente no coprocessador.
3. Altere o conteúdo dos segmentos 1, 2 e 3 do software, conforme apropriado.
4. Valide o conteúdo final dos segmentos do software.

Alterando o diretório padrão e executando o CLU

Para alterar o diretório padrão, deve-se localizar o diretório que contém os arquivos de código do coprocessador (*.clu) e o Coprocessor Load Utility (CLU).

Alterando o diretório padrão

Em um prompt de comandos, altere para o diretório do código do coprocessador do diretório padrão `/usr/lpp/csufx.4765/clu` para acessar os arquivos do código. Se o CLU não estiver no diretório padrão, assegure-se de que o sistema operacional possa localizar o CLU.

Executando o CLU

Nota: Ao usar o CLU, os aplicativos que usam o CCA não devem estar em execução.

Para executar o utilitário CLU, insira o nome do programa **csufclu** no prompt de comandos.

É possível fornecer os parâmetros interativamente para o utilitário CLU ou incluí-los na linha de comandos. Sempre que você usar o CLU, deverá especificar um nome do arquivo de log. Esse é o primeiro parâmetro e pode ser incluído na linha de comandos. Em geral, quando você trabalhar com um coprocessador específico, é melhor usar um número de série do coprocessador como o nome do arquivo de log. Você pode obter o número de série a partir do rótulo no colchete no final do coprocessador.

O CLU anexará as informações a dois arquivos de log. Se os arquivos de log não existirem, eles serão criados. Um arquivo de log contém as mesmas informações que normalmente são exibidas no console. O outro arquivo de log que o CLU designará o MRL como a extensão do nome do arquivo, contém um log legível por máquina. O arquivo MRL é usado com um utilitário de análise.

Nota: As instruções subsequentes nessa seção assumem que você usa o CLU interativamente. Mude para o diretório que contém os arquivos de código do coprocessador Inicie o CLU com o nome apropriado para seu sistema operacional. Responda aos prompts conforme solicitado.

O CLU obtém o número de coprocessadores instalados a partir do driver de dispositivo. Se você tiver mais de um coprocessador instalado, o CLU solicitará o número do coprocessador com o qual deseja interagir. Os números (coprocessor_*number*) podem ser de 0 a 2. Para correlacionar esses números com um coprocessador específico, use o comando System Status (SS) para saber o número para cada um dos coprocessadores instalados. (Para um exemplo de saída, consulte Figura 2 na página 16 no tópico de comandos do Coprocessor Load Utility).

Nota: O utilitário CLU pode operar com um coprocessador quando ele obtiver controle exclusivo do coprocessador. Se algum outro aplicativo como um encadeamento está em execução e executou as chamadas de verbo CCA, os coprocessadores que são carregados com o CCA estarão "ocupados" e inutilizáveis pelo CLU.

Informações relacionadas:

"Sintaxe do Coprocessor Load Utility" na página 13

Determinando o Conteúdo de Segmento do Software do Coprocessador

O coprocessador possui três segmentos: segmento 1, segmento 2 e segmento 3. Cada segmento tem um status, retém o software e uma chave pública de validação e um identificador do proprietário (exceto para segmento 1).

Consulte Tabela 1 para mais informações sobre os segmentos do coprocessador.

Tabela 1. Conteúdo de Segmento do Software

Segmento	Conteúdo
1	A mini-reinicialização contém os diagnósticos e controles de carregamento de código
2	Programa de controle integrado
3	CCA ou outro aplicativo

Determine o conteúdo e o status atual dos segmentos do coprocessador usando o comando **ST**. O Figura 1 mostra uma resposta típica do ST.

```
====================================================================
CSUFCLU V4.1.1 st.log ST    begun Tue Sep 13 09:30:25 2011
********** Command ST started. ---- Tue Sep 13 09:30:25 2011

 *** VPD data;  PartNum = 45D5117
 *** VPD data;  EC Num = 0G43192
 *** VPD data;  Ser Num = 99000543
 *** VPD data;  Description = IBM 4765-001 PCI-e Cryptographic Coprocessor
 *** VPD data; Mfg. Loc. = 91
 *** ROM Status; POST0 Version 1, Release 27
 *** ROM Status; MiniBoot0 Version 1, Release 20
 *** ROM Status; INIT: INITIALIZED
 *** ROM Status; SEG2: RUNNABLE , OWNER2: 2
 *** ROM Status; SEG3: RUNNABLE , OWNER3: 2
 *** Page 1 Certified: YES
 *** Segment 1 Image: S0103 P1v0607 M1v011B P2v0706 F5180 201104151205401A000022000000000000
 *** Segment 1 Revision: 40105
 *** Segment 1 Hash: 177C AF13 C601 2276 90AA 8E20 D3BB BA58 79A6 7EBA 6C2A D68B 0A34 33E0 802C 4EA7
 *** Segment 1 Hash: 177C AF13
 *** Segment 2 Image: 4.1.7    y4_12-lnx-2011-03-04-16    201108111338401A000000000100010900
 *** Segment 2 Revision: 40107
 *** Segment 2 Hash: 698A 29DC EF8A 44D8 A025 3117 491B C552 45DA EC6F 0D0C 6671 BABE 7ABF 41E7 2FF5
 *** Segment 2 Hash: 698A 29DC
 *** Segment 3 Image: 4.1.7    CCA                        201108121155401A000000000000000000
 *** Segment 3 Revision: 40107
 *** Segment 3 Hash: EC02 B93A 309F 882A D859 031D 1F22 839D 2233 4D6A C58D D93C E43F 4A4C 1234 9F48
 *** Segment 3 Hash: EC02 B93A
 *** Query Adapter Status successful ***
Obtain Status ended successfully!
********** Command ST ended. ---- Tue Sep 13 09:31:26 2011

  ...finishing up...
********** Command ST exited. ---- Tue Sep 13 09:31:46 2011
```

Figura 1. Resposta de Status do CLU Típico

Definições dos campos sobre a resposta ST a seguir:

Campo Descrição

PartNum
O número da peça (P/N) do coprocessador.

Núm. de Mudança de Engenharia
O número de mudança de engenharia do coprocessador.

Número de Série
O número de série do fabricante do coprocessador. Este número não é o número de série de controle da IBM que é utilizado para verificação de garantia e para autorização de download.

Descrição
Uma instrução que descreve o tipo de coprocessador em termos gerais. Os auditores devem revisar essas e outras informações de status para confirmar que um coprocessador apropriado esteja em uso.

Status de ROM
O coprocessador deve sempre estar em um status INICIALIZADO. Se o status for ZERADO, o coprocessador detectou um possível evento de violação e está em um estado irrecuperável e não funcional. (Os eventos de violação indesejados serão criados se o coprocessador não for manipulado corretamente). Somente remova as baterias quando você seguir o procedimento recomendado para trocar a bateria, mantenha o coprocessador no intervalo de temperatura seguro e siga as instruções.

Status ROM SEG2 / SEG3
Várias condições de status para o Segmento 2 e Segmento 3 existem, que incluem:

- UNOWNED: Atualmente não está em uso, sem conteúdo
- RUNNABLE: Contém o código e está em um estado utilizável

Os identificadores do proprietário também são mostrados. O CCA Support Program padrão recebe o identificador 2 para o Segmento 2 e Segmento 3. **Qualquer outro identificador de proprietário** indica que o software não é o código do produto IBM CCA padrão. Em todos os casos, assegure-se de que o software esteja carregado no seu coprocessador. Um software não autorizado ou não conhecido pode representar um risco de segurança para sua instalação.

Imagem do Segmento 1
O nome e a descrição do conteúdo de software do Segmento 1. Para um coprocessador enviado do factory, o nome inclui **Factory**. Esta imagem e a chave de validação associada devem ser alteradas.

Para um coprocessador carregado anteriormente, o nome do Segmento 1 provavelmente inclui CCA. Certifique-se de observar o nível de revisão.

Imagens do Segmento 2 e Segmento 3
Se esses segmentos possuírem status Possuído, observe o nome da imagem e o nível de revisão. A IBM incorpora o CCA no nome da imagem para indicar que a imagem é fornecida como parte do CCA Support Program. Certifique-se de observar o nível de revisão.

Valores do Hash do Segmento
Os valores do hash para cada segmento deve corresponder aos valores mostrados no Figura 1 na página 9.

Alterando o Conteúdo de Segmento do Software

Geralmente, o software do coprocessador deve estar no mesmo nível de liberação do software CCA no sistema host.

Não tente usar vários níveis de liberação diferentes, exceto com instruções específicas da IBM.

Inicie o Coprocessor Load Utility (CLU) e digite os parâmetros interativamente. Para obter instruções, consulte “Alterando o diretório padrão e executando o CLU” na página 8.

1. Insira o nome do arquivo de log (*nnnnnnnn*.**LOG**, em que *nnnnnnnn* é o número de série do coprocessador).
2. Insira o comando, **PL**.
3. Se você tiver diversos coprocessadores, insira o número do coprocessador.
4. Insira o nome do arquivo CLU conforme indicado no arquivo LEIA-ME.

Repita conforme necessário, para que o software apropriado seja carregado para os Segmentos 1, 2 e 3.

Validando o Conteúdo de Segmento do Coprocessador

O procedimento a ser seguido para validar o conteúdo dos segmentos do coprocessador.

Após carregar ou substituir o código nos Segmentos 1, 2 e 3, use o comando **CLU VA** para confirmar o conteúdo do segmento e para validar a assinatura digital na resposta criada pelo coprocessador.

Dependendo do coprocessador IBM 4765 (PartNum) em uso,[1] Emita o comando a seguir e substitua o nome do arquivo de certificado de chave de classe de Tabela 2 para o nome do arquivo de dados. Observe que os dados de nome do arquivo `v.clu` é anexado ao número de peça do coprocessador, tudo em caracteres minúsculos.

csuxclu *nnnnnnnn*`.log` **VA** [coprocessor_*n*] *datafile*

O número de peça pode ser obtido utilizando o comando ST Coprocessor Load Utility (CLU).

Tabela 2. O Arquivo de Chave de Classe para Uso com o Comando CLU VA

PartNum	Arquivo de certificado da chave de classe
12R8565	12r8565v.clu
41U0441	41u0441v.clu

O parâmetro [coprocessor_*n*] é o designador opcional para um coprocessador específico e é padronizado como zero.

Descarregando o Software do Coprocessador e Zerando o Nó CCA

As etapas para descarregar o software do coprocessador e zerar o nó CCA para renunciar a propriedade dos segmentos são descritos aqui.

Ao utilizar o Coprocessor Load Utility (CLU) para processar um arquivo que renuncia a propriedade do Segmento 2, o Segmento 2 e Segmento 3 subordinado são limpos e o código é removido. A chave pública de validação para o segmento é limpo e os itens de dados relevantes de segurança que são mantidos no coprocessador para o segmento são zerados. O identificador do proprietário é limpo e o status do segmento é configurado para UNOWNED.

Consulte o arquivo LEIA-ME que acompanha a distribuição do software que você está usando para o determinado nome do arquivo `.clu`, que é utilizado para renunciar a propriedade dos Segmentos 2 e 3. O arquivo LEIA-ME também pode fornecer as informações adicionais que amplifica ou modifica o procedimento geral.

Execute essas ações:

- Altere para o diretório que contém os arquivos do CLU.
- Inicie o utilitário CLU.
- Responda aos prompts e use o número de série do coprocessador no nome do arquivo de log.
- Use o comando **PL** para renunciar o Segmento 2, conforme indicado no arquivo LEIA-ME para a sua plataforma.

---

1. é possível consultar a seção de FAQ do web site do produto IBM (http://www.ibm.com/security/cryptocards), para que o procedimento valide a integridade do coprocessador. Esse tópico transporta a lista atual de arquivos de certificado de chave de classe.

Comunicados:

1. Você também pode zerar o CCA sem remover o software ao usar o processo de reinicialização do CCA.
2. Normalmente, a IBM não disponibiliza um arquivo para restaurar a chave de validação do Segmento 1 da factory para colocar o coprocessador em uma condição semelhante a um produto pronto para factory. O Segmento 1 pode ser alterado para um número limitado de vezes antes que o espaço de certificado de Chave de Dispositivo disponível seja utilizado e que o coprocessador seja potencialmente renderizado não utilizável. Se você requerer a capacidade para restaurar a chave de validação do Segmento 1 e estiver disposto a exibir o coprocessador a uma condição de um possível bloqueio, poderá obter o arquivo necessário da IBM ao enviar uma consulta utilizando o Formulário de Suporte no website do produto, http://www.ibm.com/security/cryptocards. É importante observar que o espaço do certificado é um recurso não renovável. Após ser usado, ele não poderá ser recuperado.

Informações relacionadas:

"Inicializando o nó" na página 24
O procedimento para inicializar o nó CCA para seu estado inicial.

Referência do Coprocessor Load Utility (CLU)

Os segmentos de memória do coprocessador para o qual o software será carregado são descritos aqui. A abordagem que o coprocessador usa para validar o software é carregada, a sintaxe utilizada para iniciar o CLU e os códigos de retorno do CLU.

Se você não precisar dos detalhes nesta seção, vá para "Gerenciando o nó criptográfico usando os utilitários CNM e CNI" na página 16.

Segmentos de Memória do Coprocessador

Os segmentos de memória do coprocessador são organizados em diferentes segmentos.

A organização dos segmentos de memória e suas funções estão a seguir:

Tabela 3. Organização dos Segmentos de Memória

Segmento	Descrição
0	Código básico O código básico gerencia a inicialização do coprocessador e as interfaces do componente de hardware. Esse código não pode ser alterado depois que o processador sair da fábrica.
1	Rotinas de administração de software e criptográficas Software nesse segmento: • Administra a substituição de software já carregado no Segmento 1. • Administra o carregamento de dados e de software nos segmentos 2 e 3. • É carregado na fábrica, mas pode ser substituído usando o utilitário CLU.
2	Sistema operacional integrado O coprocessador do Support Program inclui o sistema operacional. O sistema operacional suporta os aplicativos carregados no Segmento 3. O segmento 2 estará vazio quando o coprocessador for enviado do factory.
3	Software de aplicativo O Support Program do coprocessador inclui o programa de aplicativo da CCA que pode ser instalado no Segmento 3. O aplicativo funciona de acordo com o IBM CCA e executa operações de controle de acesso, gerenciamento de chaves e criptográficas. O Segmento 3 é vazio quando o coprocessador é fornecido de fábrica.

Validando os carregamentos do software do coprocessador

Quando o coprocessador for enviado da fábrica, ele possui nele a chave pública que é necessária para validar o software de substituição para o Segmento 1.

Para carregar o código nos Segmentos 2 e 3 do coprocessador, para cada segmento sigas estas etapas:

1. Identifique um proprietário para o segmento usando um comando **Establish Owner**. O identificador do proprietário será aceito somente se a assinatura digital associada a esse identificador puder ser validada pela chave pública que esteja residindo com o segmento inferior imediatamente. Uma vez estabelecida, a propriedade permanecerá em vigor até um comando **Surrender Owner** for processado pelo coprocessador.
2. Carregue o segmento para o código. Dois comandos diferentes estão disponíveis.
   a. Inicialmente, use o comando **Load**. Os dados do comando **Load** incluem um certificado de chave pública, que deve ser validado pela chave pública que está presente no próximo segmento inferior. O coprocessador aceita o código e mantém a chave pública validada para o segmento, se uma das condições for satisfeita:
      - O certificado é validado.
      - Os dados do identificador de proprietário no comando **Load** corresponde à propriedade atual, que é mantida pelo coprocessador para o segmento.
      - Os dados completos no comando **Load** podem ser validados pela chave pública no certificado que foi utilizado para validação.
   b. Se um segmento já possuir uma chave pública, um comando **Recarregar** pode ser usado para substituir o código em um segmento. As ações do coprocessador são as mesmas para um comando **Load**, com exceção do certificado incluído que deve ser validado pela chave pública associada ao segmento de destino, em vez de pela chave associada ao próximo segmento inferior.

O sistema operacional integrado, trabalhando com o hardware do coprocessador, pode armazenar os security-relevant data items (SRDIs) em nome de si mesmo e um aplicativo no Segmento 3. Os SRDIs são zerados na detecção de violação, no carregamento do software de segmento ou no processamento de um comando **Surrender Owner** de um segmento. O SRDIs para um segmento não são zerados quando o comando **Reload** é utilizado. O aplicativo CCA armazena as chaves mestra, o function control vector (FCV), as tabelas de controle de acesso e as chaves privadas RSA retidas como informações SRDI que estão associadas ao Segmento 3.

A IBM designa o próprio software. Se outro fornecedor deseja fornecer o software para o coprocessador, o comando **Establish Owner** desse fornecedor e o código de assinatura de certificado de chave pública deve ser assinado pela IBM sob um contrato adequado. Essas restrições asseguram que as condições a seguir foram atendidas:

- Apenas o código autorizado pode ser carregado no coprocessador.
- As restrições governamentais são atendidas com relação à importação e à exportação de implementações criptográficas.

Sintaxe do Coprocessor Load Utility

A sintaxe que é utilizada para iniciar o Coprocessor Load Utility (CLU) e as funções descritas do utilitário.

O CLU deve ser utilizado para as funções a seguir:

- Assegure-se de que os coprocessadores não estejam ocupados, encerrando qualquer aplicativo que tenha utilizado um coprocessador. Por exemplo, termine todos os aplicativos que usam a API do CCA.
- Obtenha o nível da liberação e o status do software que está instalado nos segmentos de memória do coprocessador.

---

2. Nessa publicação, os termos *load* e *reload* são usados. Outra documentação pode referir a essas operações como *emergency burn* (EmBurn) e *regular burn*, ou *remote burn* (RemBurn).

- Confirme a validade das mensagens assinadas digitalmente que são retornadas pelo coprocessador.
- Carregar e recarregar partes do software do coprocessador.
- Reconfigurar o coprocessador.

Para iniciar o utilitário, siga estas etapas:

1. Efetue logon conforme necessário pelo seu sistema operacional.
2. Na linha de comandos, altere o diretório para o diretório que contém os arquivos do CLU. O diretório padrão é `/usr/lpp/csufx.4765/clu`.
3. Insira o nome do utilitário **csufclu** seguido pelos parâmetros aplicáveis.

Se você não fornecer os parâmetros necessários, o utilitário avisará quando as informações são necessárias. Os parâmetros opcionais são incluídos entre colchetes. A sintaxe para os parâmetros que seguem o nome do utilitário é

[*log_filecmd*[*coprocessador_#*][*data_file*][*-Q*]]

Em que:

log_file Identifica o nome do arquivo de log. O utilitário anexa as entradas para esse arquivo de texto ASCII, conforme ele executa as operações que são solicitadas. Um segundo arquivo de log legível pela máquina, com um nome de arquivo logfile_name MRL, também é criado. Esse arquivo de log pode ser processado por um programa e conter as respostas binárias codificadas a partir do coprocessador.

cmd Especifica uma abreviatura de duas letras que representa o comando do utilitário a ser executado.

coprocessor_*number*
Fornece o número do coprocessador conforme estabelecido pelo driver de dispositivo. Esse parâmetro é padronizado para 0. Os coprocessadores são designados para o driver de dispositivo como números 0, 1 e 2. É possível usar as informações do número de série que você obtiver com o comandos **ST** ou **VA** e o número de série que é impresso no colchete de fechamento do coprocessador para correlacionar um determinado coprocessador ao coprocessor_*number*. O utilitário suporta até oito coprocessadores por sistema.

data_file
Identifica o arquivo de dados (unidade, diretório e nome do arquivo) que é utilizado para a operação solicitada. Para identificar o nome *data_file*, utilize um dos métodos a seguir:
- Para os carregamentos e recarregamentos do software, o nome *data_file* é o nome do arquivo da imagem de software que você está carregando no coprocessador. O arquivo LEIA-ME do Support Program fornece o nome *data_file* .
- Para o coprocessador, o status do coprocessador é obtido com o comando **VA** . O *data_file* o nome é o nome do arquivo de certificado de chave de classe que é usado para validar a resposta do coprocessador. A seção de FAQ do website do produto (http://www.ibm.com/security/cryptocards) contém uma descrição do procedimento para validar o coprocessador e seu código. Essa descrição também contém uma lista dos nomes do arquivo de certificado de chave de classe atual. É possível fazer o download do arquivo de certificado necessário do Web site.

-*Q* Suprime (silencia) a saída do programa CLU para o dispositivo de saída padrão. As informações de status ainda estão anexadas aos arquivos de log.

Exemplo: Para obter o status do coprocessador e salvar os resultados no arquivo de log, insira:

csufclu nnnnnnnn.log va *datafile_name***.clu**

É sugerido que você faça o número de série *nnnnnnnn* do coprocessador. Não é obrigatório usar o número de série, mas é utilizado para reter um histórico de todas as mudanças de software feitas em cada coprocessador específico.

Informações relacionadas:

"Conteúdo do Machine-Readable Log" na página 45
O utilitário CLU cria dois arquivos de log, um destinado para leitura e outro para uma possível entrada para um programa.

"Comandos do Coprocessor Load Utility"
O Coprocessor Load Utility (CLU) suporta vários comandos do utilitário.

Comandos do Coprocessor Load Utility:

O Coprocessor Load Utility (CLU) suporta vários comandos do utilitário.

Os comandos de carregador e suas funções suportadas pelo CLU são os seguintes:

Tabela 4. Comandos do Utilitário de Carga do CLU

Comando Loader	Descrição
PL: Carregar microcódigo no coprocessador Os comandos R1, E2, L2, R2, S2, E3, L3, R3 e S3 são deduzidos a partir das informações contidas nos arquivos de dados que você usa com o comando PL. Um único arquivo "PL" pode incorporar informações para vários comandos de propriedade e de carregamento.	Processa uma série de comandos conforme direcionado pelo conteúdo do arquivo de dados para estabelecer a propriedade do segmento e para carregar ou recarregar o software do segmento.
RS: Reconfigurar o coprocessador	Reconfigura o coprocessador. Geralmente você não usará esse comando. O comando faz com que o coprocessador execute uma reconfiguração ao ligar. Você pode achar esse comando útil, mas o coprocessador e o software do sistema host podem perder a sincronização. Você deve encerrar todos os processos do software do sistema host que estão operando com o coprocessador antes de emitir esse comando, para ativar o subsistema criptográfico completo para entrar em um estado de reconfiguração.
SS: Obter o status do sistema	Obtém o número da peça, o número de série e a parte do nome da imagem de software Segmento 3 para cada um dos coprocessadores instalados, contanto que não estejam sendo usados por algum aplicativo, como CCA. Consulte o Figura 2 na página 16.
ST: Obter status do coprocessador	Obtém o status do software carregado e o nível de release de outros componentes. O status é anexado aos arquivos de log.
VA: Validar status do coprocessador	Obtém o status do software carregado e o nível de release de outros componentes. Os dados são transmitidos em uma mensagem assinada pela chave de dispositivo do coprocessador e, em seguida, armazenados no arquivo de log do utilitário. O utilitário usa sua chave pública integrada para validar os certificados de uma ou mais chaves de classes contidas no parâmetro de nome *data_file*. Um desses certificados deve validar a chave pública, ou uma cadeia de chaves públicas, obtidas a partir do coprocessador e confirmar que o coprocessador não foi violado.

Em geral, o utilitário pode ser chamado por um arquivo de script ou por um arquivo de comando. Ao criar um arquivo de script ou um arquivo de comando para iniciar o utilitário em um sistema autônomo, inclua a sintaxe "silencioso", o parâmetro **-q** (ou **-Q, /q,** ou **/Q**), para solicitar que nenhuma saída seja enviada para a exibição. Por padrão, o utilitário retorna prompts e mensagens para exibição.

A figura *Resposta do Status do Sistema CLU Típico* mostra a resposta de um sistema CLU.

```
====================================================================
CSUFCLU V4.00 ss.log SS    begun Tue Sep 28 10:49:36 2010
*********** Command SS started. ---- Tue Sep 28 10:49:36 2010

 Card #    P/N        S/N         Segment 3 Description
 ------    -------    --------    -----------------------------------
   0       45D6045    99000627    4.1.0    CCA
 *** Query System Status successful ***
System Status ended successfully!
*********** Command SS ended. ---- Tue Sep 28 10:50:37 2010

  ...finishing up...
*********** Command SS exited. ---- Tue Sep 28 10:50:57 2010
```

Figura 2. Resposta de Status do Sistema CLU Típico

Códigos de Retorno do Coprocessor Load Utility

Esta seção especifica os valores do código retornado do CLU.

Quando o CLU conclui o processamento, ele retorna uma valor que pode ser testado em um arquivo de script ou em um arquivo de comando. Cada um dos valores retornados tem suas implicações.

0 OK. Isto implica que o CLU concluiu o processamento corretamente.

1 Parâmetros de linha de comandos não são válidos.

2 Não é possível acessar o coprocessador. Neste caso, assegure-se de que o coprocessador e seu driver tenham sido instalados corretamente.

3 Verifique o arquivo de log do utilitário para obter um relatório de condição anormal.

4 Nenhum coprocessador foi instalado. Neste caso, assegure-se de que o coprocessador e seu driver tenham sido instalados corretamente.

5 Um número de coprocessador inválido foi especificado.

6 Um arquivo de dados é necessário com esse comando.

7 O arquivo de dados especificado com esse comando está incorreto ou é inválido.

Gerenciando o nó criptográfico usando os utilitários CNM e CNI

Um computador que fornece serviços criptográficos, como geração de chave e suporte a assinatura digital, é definido como um *nó criptográfico*.

Os utilitário CCA Node Management (CNM) e CCA Node Initialization (CNI) fornecidos com o Support Program são ferramentas para configurar e gerenciar os serviços criptográficos do CCA fornecidos por um nó.

Esta seção inclui:

- Utilitários e descrição sobre como iniciá-los.
- Cenários de amostra para o uso dos utilitários que podem ser considerados.
- Como usar as funções administrativas do utilitário CNM: Revise este material após analisar o tópico "Cenário: Criando um nó de teste" na página 18.
- Como criar e gerenciar os dados de controle de acesso: Leia os detalhes sobre a parte de controle de acesso do utilitário CNM.
- Como gerenciar as chaves criptográficas: Leia sobre algumas das tarefas de gerenciamento de chaves que você pode realizar com o utilitário CNM.

- Como estabelecer outros nós usando o utilitário CNI: É possível automatizar o uso do utilitário CNM usando os procedimentos encapsulados.

Esses utilitários são gravados no Java™ e requerem o uso de um Java Runtime Environment (JRE). Também é possível usar o Java Development Kit (JDK).

Visão geral de CNM e CNI

Os usuários típicos dos utilitários CCA Node Management (CNM) e CCA Node Initialization (CNI) são da equipe de administração de segurança, desenvolvedores de aplicativos, administradores de sistemas e, em alguns casos, operadores do modo de produção.

Comunicados:

1. O utilitário CNM apresenta um conjunto limitado de serviços da API do CCA. Depois de familiarizar-se com o utilitário, você pode determinar se ele atende as suas necessidades ou se requer um aplicativo customizado para obter um controle administrativo e um gerenciamento de chaves mais abrangentes.
2. Os arquivos criados por meio do uso do utilitário CNM podem ser dependentes nas liberações do Java Runtime Environment (JRE). Se você alterar a liberação do Java Runtime Environment (JRE) usada, os arquivos criados com o utilitário CNM poderão não funcionar corretamente com a nova liberação.
3. O utilitário CNM foi projetado para uso com um mouse. Use o mouse em vez da tecla **Enter** para resultados consistentes.
4. Nenhum painel de ajuda é fornecido para a parte de Clonagem de Chave Mestra do utilitário.
5. Estes utilitários usam a API do IBM Common Cryptographic Architecture (CCA) Support Program para solicitar serviços do coprocessador. O manual de Referência e Guia de Serviços Básicos do *IBM CA para o IBM 4765 PCIe e 4764 PCI-X Cryptographic Coprocessors* contém uma lista abrangente dos verbos (também conhecida como serviços de chamadas ou chamadas de procedimentos) fornecida pela API do CCA. Consulte este manual e os serviços individuais nele descritos para compreender quais comandos podem requerer autorização nas várias funções definidas, usando os procedimentos descritos nesta seção.

Visão Geral do Utilitário CCA Node Management

O utilitário CCA Node Management é um aplicativo Java que fornece uma interface gráfica a ser usada na definição e na configuração de nós criptográficos CCA do IBM 4765. As funções do utilitário, principalmente para configurar um nó, criam e gerenciam dados de controle de acesso e gerenciam as chaves mestras CCA necessárias para administrar um nó criptográfico.

Você pode carregar os objetos de dados diretamente no coprocessador ou salvá-los no disco. Os objetos de dados são utilizáveis em outros nós CCA do IBM 4765 que usam o mesmo sistema operacional e um nível compatível do aplicativo Java.

Nota: Iniciando o Utilitário CCA Node Management: Para iniciar o utilitário CCA Node Management, insira o comando **csufcnm**, o logotipo do utilitário CNM e, em seguida, a janela principal será exibida.

Visão geral do utilitário CCA Node Initialization

O utilitário CCA Node Initialization executa os scripts criados usando o *CNI Editor* dentro do utilitário CNM. Esses scripts são conhecidos como *Listas de CNI*. O utilitário CNI pode executar as funções de utilitário CNM necessárias para configurar um nó; por exemplo, ele pode ser usado para carregar as funções e os perfis de controle de acesso.

Conforme você cria uma lista de CNI, você especifica o local do disco dos objetos de dados que o utilitário CNI carregará nos nós de destino. Após criar uma lista CNI, será possível distribuir a lista CNI

e quaisquer arquivos de dados de acompanhamento (para funções, perfis, etc.) para os nós em que o utilitário CNI será usado para uma configuração automatizada. O nó de origem e todos os nós que executam a lista CNI distribuída devem empregar o mesmo sistema operacional e um nível compatível do aplicativo Java.

Nota: Iniciando o Utilitário CCA Node Management: Para iniciar o utilitário CCA Node Management, insira o comando **csufcnm**, o logotipo do utilitário CNM e, em seguida, a janela principal será exibida.

Informações relacionadas:

"Cenário: Clonando uma chave mestra DES ou PKA" na página 21
As etapas para clonar um padrão de criptografia de dados (DES) ou algoritmo de chave pública (PKA) chave mestra de um coprocessador para outro.

"Criando outros nós usando o utilitário CNI" na página 37
Criar uma lista CNI para o utilitário CCA Node Initialization (CNI) permite o carregamento as chaves e os dados de controle de acesso armazenados no disco em outros nós criptográficos, sem executar o utilitário CNM nesses nós de destino.

Cenários: Usando os utilitários CNM e CNI

Esta seção descreve o uso do utilitário CCA Node Management (CNM) e do utilitário CCA Node Initialization (CNI) para criar um nó e cloná-lo para outro coprocessador.

O uso dos utilitários é ilustrado nos cenários, que inclui:

1. Criação de um nó de teste a ser usado para desenvolver aplicativos ou estabelecer procedimentos para usar o utilitário CNM. *Os usuários iniciantes devem seguir esse procedimento para iniciar experimentos com o utilitário e com o coprocessador.*
2. Criação de nós para um ambiente de produção que usa partes da chave. Este cenário emprega as listas CNI para automatizar o estabelecimento de nós de produção de destino.
3. Clonagem de uma chave mestra de um coprocessador para outro coprocessador. Esse é um procedimento de interesse para instalações de segurança alta, que emprega vários coprocessadores.

O propósito dos cenários é ilustrar como os procedimentos descritos aqui podem ser usados. Quando apropriado, um cenário fará referência a outras seções desta coleção de tópicos com informações mais detalhadas.

Se você não estiver familiarizado com o do CCA de controle de acesso do sistema, consulte "Visão geral de controle de acesso" na página 27 e "Estado inicial do sistema de controle de acesso" na página 27. Aqui é possível localizar uma explicação dos termos como *função inicial função DEFAULT* e *perfil do usuário*. Os cenários supõem que o sistema de controle de acesso esteja em seu estado inicial.

Nota: Esses cenários são apenas para instrução. Você será incentivado a determinar os procedimentos melhores adequados para seu ambiente específico. Consulte o apêndice sobre as operações seguras na Referência e Guia de Serviços Básicos do IBM CCA para o *IBM 4765 PCIe and 4764 PCI-X Cryptographic Coprocessors*.

Cenário: Criando um nó de teste

Neste cenário, um único programador configura um nó para permitir o acesso ilimitado a serviços criptográficos.

Importante: O nó criptográfico resultante não deve ser considerado seguro, pois, neste cenário, muitos comandos sensíveis são permitidos com uso irrestrito.

Pré-requisito: Você já deve ter instalado um nível apropriado do Java Runtime Environment (JRE) ou do Java Development Kit (JDK).

Para criar um nó de teste, execute as etapas a seguir:

1. Instale o coprocessador e o IBM CCA Cryptographic Coprocessor Support Program, conforme descrito em Instalando o Support Program .
2. Inicie o utilitário CCA Node Management inserindo o comando **csufcnm**. O logotipo e o painel principal do utilitário CNM são exibidos.
3. Se você tiver mais de um coprocessador com o CCA instalado, especifique para o utilitário CNM qual coprocessador deseja usar. No menu **Nó de Criptografia**, selecione **Selecionar Adaptador**. Uma lista de números de adaptadores disponíveis (1 – 8) é exibida. Selecione um adaptador (coprocessador) na lista. Se você não usar a lista **Selecionar Adaptador** para selecionar um adaptador, o adaptador padrão (coprocessador) será usado.
4. Sincronize o relógio no coprocessador e no computador host. No menu **Nó de Crypto**, clique em **Tempo**. No submenu resultante, clique em **Configurar**. Os relógios são sincronizados.
5. Use o utilitário CNM para permitir todos os comandos na função PADRÃO:
   a. No menu **Controle de Acesso**, clique em **Funções**.
   b. Destaque a entrada **PADRÃO** e clique em **Editar**. Uma janela exibe os comandos que são ativados e aqueles que não são ativados pela função PADRÃO.
   c. Clique em **Permitir Todos**.
   d. Carregue a função modificada de volta no coprocessador clicando em **Carregar** e selecione **OK**.
   e. Salve uma cópia da função clicando no botão **Salvar** e no nome da função.
6. Carregue o function-control vector (FCV) no coprocessador. No menu **Nó de Criptografia**, clique em **Autorização**. No submenu resultante, clique em **Carregar** para especificar e carregar o FCV.

   O arquivo FCV é o que foi colocado no servidor durante o processo de instalação. Os FCVs geralmente possuem nomes do arquivo, como `fcv_td4kECC521.crt`, e é procurado usando o utilitário de procura de arquivos disponível no seu sistema operacional.
7. Instale uma chave mestra no menu **Chave Mestra**, clique em **Chaves Mestras de DES/PKA** ou **Chaves Mestras de AES** e clique em **Sim**. O coprocessador gera e configura uma chave mestra aleatória.

   A chave mestra que foi instalada com a opção **Configuração Automática** tem passado atualmente pela memória principal do processador do sistema como partes da chave. Para propósitos de produção, use um método mais seguro de estabelecer uma chave mestra, como a geração ou a instalação aleatória de partes da chave conhecida inseridas por duas ou mais pessoas. Essas opções também são acessadas nos menus mencionados anteriormente.
8. Inicialize os arquivos de armazenamento de chaves. Para mais informações ou para inicializar os arquivos de armazenamento de chaves, consulte “Criando ou inicializando o armazenamento de chaves” na página 36

   O *Armazenamento de Chaves* é um termo do CCA que descreve um local onde o Support Program pode armazenar as chaves criptográficas de Data Encryption Standard (DES), de Algoritmo Rivest-Shamir-Adleman (RSA) e de Advanced Encryption Standard (AES) sob nomes (ou os aplicativos) definidos. Se você pretender usar o armazenamento de chaves, deverá inicializar o arquivo ou os arquivos de armazenamento de chaves que correspondem aos tipos de chaves que você está usando: DES, RSA (PKA) ou AES. Por exemplo, se desejar usar apenas as chaves DES, você deverá inicializar o arquivo de armazenamento de chaves DES, mas não os demais. Por exemplo, se desejar usar as chaves DES e PKA, você deverá inicializar os arquivos de armazenamento de chaves DES e PKA, mas não o arquivo de armazenamento de chaves DES. Se desejar usar os três juntos, inicialize todos eles.

Links Relacionados: “Criação de uma função” na página 28

“Carregando uma Chave Mestra Automaticamente” na página 34

Cenário: Criando nós em um ambiente de produção

Nesse cenário, a responsabilidade para a criação de nós criptográficos é dividida entre três indivíduos, ou seja, um administrador de controle de acesso e dois executivos de gerenciamento de chaves.

O administrador configura o nó e o seu sistema de controle de acesso. Em seguida, os agentes de gerenciamento de chaves carregam uma chave mestra e quaisquer key encrypting keys (KEKs) necessárias. As KEKs podem ser usadas como chaves de transporte para transmitir outras chaves entre os nós.

Este cenário é focado na instalação de chaves mestras e de alto nível, as KEKs do data encryption standard (DES) entre nós das *partes da chave*. A implementação do CCA suporta as alternativas para a técnica de parte de chave como geração e a distribuição de chave mestra aleatória de chaves DES usando as técnicas que são baseadas na chave pública de tecnologia Rivest-Shamir-Adleman (RSA). A *técnica de parte da chave* assume que há dois *executivos de gerenciamento de chaves*, que podem ser confiados para executar suas tarefas e para não compartilhar sua parte de informações chave. Esta tecnologia implementa uma política *divisão de conhecimento* . O sistema de controle de acesso é configurado para aplicar *controle duplo* ao separar as tarefas do primeiro e do segundo oficial.

Neste cenário, o administrador de controle de acesso usa o utilitário Cryptographic Node Management (CNM) para preparar as listas Coprocessor Node Initialization (CNI) para os nós de destino. As listas CNI automatizam o processo de uso do utilitário CNM no nó de destino. O administrador prepara uma lista CNI para as tarefas que são executadas pelo administrador de controle de acesso do nó de destino e dois executivos de gerenciamento de chaves. O administrador deve conhecer os comandos que requerem autorização no nó de destino em diferentes condições, que inclui:

- Normal, operação limitada (quando a função padrão é usada)
- Quando as tarefas do administrador de controle de acesso são executados
- Quando cada uma das tarefas de gerenciamento de chaves de executivo são executados
- Sob quaisquer outras circunstâncias especiais usando as funções e os perfis adicionais.

Nota: Os utilitários CNM e CNI são ferramentas que são utilizadas para configurar e gerenciar os serviços criptográficos do CCA que são fornecidos por um nó.

O administrador autoriza os comandos nas várias funções para assegurar que somente os comandos necessários sejam ativados. Os comandos sensíveis, como carregamento de uma primeira parte da chave ou das partes da chave subsequentes, são ativados somente em funções de usuários com responsabilidade e autoridade para utilizar esses comandos. É importante separar as responsabilidades de modo que as políticas de divisão de conhecimento e de controle duplo sejam aplicadas pelo coprocessador do controle de acesso do sistema.

Informações relacionadas:

"Criando e gerenciando os dados de controle de acesso" na página 26

Cenário: Preparando listas CNI para nós de destino: Nesta tarefa, o administrador de controle de acesso usa o utilitário CCA Node Management (CNM) para preparar as listas CCA Node Initialization (CNI) para os nós de destino.

Para configurar o nó e criar os dados de controle de acesso, o administrador pode controlar o acesso:

1. Em um nó estabelecido, inicie o utilitário CNM.
2. Criar e salvar no disco os dados de controle de acesso para o nó de destino, que inclui:
   - Supervisionar funções e perfis do usuário para o administrador de controle de acesso e executivos de gerenciamento de chaves
   - Uma função padrão para substituir a função padrão inicial

   a. Criar uma lista CNI para sincronizar o relógio e o calendário dentro do coprocessador e do computador host.
      1) Carregar os dados de controle de acesso.
      2) Efetuar logon como um administrador de controle de acesso.
      3) Carregar a função padrão de substituição.

4) Carregar o function control vector (FCV).
5) Efetue logoff.

b. Crie uma lista CNI para o primeiro oficial de gerenciamento de chaves:
1) Efetuar logon como o primeiro oficial de gerenciamento de chave.
2) Carregar uma primeira chave mestra da parte da chave.
3) Carregar a primeira parte da chave de criptografia de informações chave.
4) Efetue logoff.

c. Crie uma lista CNI para o segundo executivo de gerenciamento chave:
1) Efetuar logon como o segundo executivo de gerenciamento chave.
2) Carregar uma segunda chave mestra da parte da chave.
3) Carregar a segunda parte da chave de criptografia de informações chave.
4) Efetue logoff.

3. Instalar o coprocessador e o IBM Common Cryptographic Architecture (CCA) Support Program nos nós de destino.
4. Transportar para os nós de destino os dados de controle de acesso e o FCV especificado na lista CNI.
5. Com o envolvimento de executivos de gerenciamento de chave, em cada nó de destino, execute as listas CNI que você criou nas etapas 2a na página 20, 2b e 2c.

Os nós de destino estão agora prontos para fornecer serviço criptográfico.

Informações relacionadas:

"Criando e gerenciando os dados de controle de acesso" na página 26

"Criando outros nós usando o utilitário CNI" na página 37

Criar uma lista CNI para o utilitário CCA Node Initialization (CNI) permite o carregamento as chaves e os dados de controle de acesso armazenados no disco em outros nós criptográficos, sem executar o utilitário CNM nesses nós de destino.

Cenário: Preparando e carregando partes da chave:

Esta seção descreve o procedimento para preparar, carregar e transportar as partes da chave.

Os agentes de gerenciamento chave preparar partes de chave para uso nos nós de destino e carregar as partes da chave nos nós de destino.

Decida o método para transportar as partes da chave do ponto de geração para o ponto de instalação. A seguir estão algumas possibilidades:

- Gere as partes da chave em um local centralizado e as transfira em disquetes.
- Gere as partes da chave em um local centralizado e as transfira em formulários de papel.
- Gere as partes de chave no ponto e no momento da instalação (primeira). Se as partes da chave forem requeridas após a instalação, para serem recarregadas ou compartilhadas com outros nós, então você deverá decidir sobre o método de transporte das partes da chave.

Revise os recursos específicos do utilitário CNM trabalhando com o utilitário. Em seguida, revise a abordagem específica que você seleciona e teste a lista do utilitário CCA Node Initialization (CNI), que foi preparado em conjunto com o administrador de controle de acesso.

Cenário: Clonando uma chave mestra DES ou PKA

As etapas para clonar um padrão de criptografia de dados (DES) ou algoritmo de chave pública (PKA) chave mestra de um coprocessador para outro.

O termo *clonagem* é usado em vez de cópia, pois a chave mestra é dividida dentro de compartilhamentos para o transporte entre os coprocessadores. A técnica é explicada no tópico "Entendendo e gerenciando

chaves mestras" no Referência e Guia de Serviços Básicos do IBM CCA para o manual do *IBM 4765 PCIe and 4764 PCI-X Cryptographic Coprocessors*. A seção "Clonando uma chave mestra" na página 47 fornece um procedimento passo a passo que pode ser seguido. As informações de segundo plano que permitem a variação do procedimento são descritas nesta seção.

Nota: A clonagem de uma chave mestra AES não é suportada.

A clonagem da chave mestra envolve dois ou três nós:

- O nó de origem da chave mestra.
- O nó de destino da chave mestra.
- O nó Share Administration (SA). O nó SA pode ser o nó de destino ou o nó de origem.

O utilitário CNM pode armazenar dados de vários itens que estão envolvidos nesse processo em um banco de dados, que é possível transportar (com disquete) ou transferir (por FTP) entre nós diferentes. Um banco de dados é `sa.db`, que é o padrão, e contém as informações sobre a chave SA e as chaves que são certificadas. O nó de destino no qual a chave principal está clonada também possui um banco de dados, que é conhecido por padrão como `csr.db`.

É possível executar essas tarefas usando o utilitário CNM:

1. Inicie o utilitário CCA Node Management inserindo o comando **csufcnm**. O logotipo e a janela principal do utilitário CNM são exibidos.
2. Configure os nós de maneira segura com as funções de controle de acesso, perfis de usuário e chaves mestras.

   É necessária uma função e um ou mais perfis de usuário nos nós de origem e de destino para cada usuário que obtiver ou armazenar ações. O processamento de ações é feito por um comando separado de modo que, se você desejar, as funções podem assegurar que indivíduos independentes estejam envolvidos ao obter e instalar os compartilhamentos diferentes.

   Considere o uso da chave mestra aleatória de geração e funções que aplica uma política de segurança de controle duplo. Por exemplo, permite que um indivíduo ou função registre um hash e outro indivíduo ou função registre uma chave pública. Selecione a pessoa ou função diferente para obter e instalar os compartilhamentos de pessoas da chave mestra.

   Consulte a seção de orientação no manual *Referência e Guia de Serviços Básicos do IBM CCA para o IBM 4765 PCIe e 4764 PCI-X Cryptographic Coprocessors*, para a descrição dos verbos Master_Key_Process e Master_Key_Distribute.
3. Instale um ID exclusivo 1 – 16 byte environment (EID) de sua escolha em cada nó.

   No menu **Nó de Criptografia**, clique em Configurar ID do Ambiente, insira o identificador e clique em Carregar. Use somente esses caracteres em um EID: A – Z, a – z, 0 – 9, e @(X'40'), caractere de espaço (X'20'), &, (X'26') e =, (X'3D').

   Deve-se inserir um identificador completo de 16 caracteres. Para identificador curto, conclua a entrada com caracteres de espaço.
4. Inicialize o de compartilhamento de chave mestra m e os valores n nos nós de origem e de destino. Esses valores devem ser os mesmos nos nós de origem e de destino. O valor n é o número máximo de compartilhamentos, enquanto m é o número mínimo de compartilhamentos que deve ser instalado para reconstituir a chave mestra no nó de destino.

   No menu **Nó de Criptografia**, clique em **Administração de Compartilhamento** > **Defina o número de compartilhamentos**, insira os valores e clique em Carregar.
5. Nos nós diferentes, gere essas chaves e faça com que cada chave pública esteja certificada pela chave SA. É possível usar o banco de dados do utilitário `sa.db` para transportar as chaves e os certificados.

   Administração de compartilhamento (SA)
   Essa chave é usada para certificar a si próprio e as seguintes chaves. Deve-se registrar o hash da chave pública SA e a própria chave pública, nos nós SA, de origem e de destino.

Após a criação da chave SA, o utilitário fornece um de valor do caractere de 8 bytes ou 16 caracteres hexadecimais, que é uma parte do hash da chave SA. *Certifique-se de reter uma cópia desse valor.* Será necessário esse valor para confirmar que o valor de hash esteja registrado no banco de dados para registrar a chave pública SA nos nós de origem e de destino.

Coprocessor Share Signing (CSS)
Esta chave é usada para sinalizar os compartilhamentos distribuídos no nó de origem. A chave privada é retida no nó de origem.

Coprocessor Share Receiving (CSR)
Esta chave é usada para receber uma chave de criptografia de compartilhamento no nó de destino. A chave CSR pública de SA certificada é usada no nó de origem para agrupar (criptografar) a chave de criptografia de compartilhamento, que é exclusiva para cada compartilhamento. A chave privada é retida no nó de destino.

Gere os Pares de Chave: SA, CSS e CSR
No menu **Nó de Criptografia**, clique em **Administração de Compartilhamento** > **Criar Chaves**. Clique em **Chaves de Administração de Compartilhamento**, **Chave CSS** ou **Chave CSR**. Clique em **Criar**.

Deve-se fornecer os rótulos de chave para as chaves CSS e CSR que estão retidas nos nós de origem e de destino; por exemplo, `IBM4765.CLONING.CSS.KEY` e `IBM4765.CLONING.CSR.KEY`. Os rótulos que você utiliza não devem conflitar com os outros rótulos de chave que são utilizados em seus aplicativos.

Para gerar a chave CSR no nó de compartilhamento de recebimento, deve-se obter o número de série do coprocessador. No **Nó de Criptografia**, clique em **Status**. Deve-se inserir o valor de número de série para certificar a chave CSR.

6. Registre a chave pública SA no coprocessador nos nós SA, de origem e de destino. Esse processo é um processo de duas etapas que deve ser feito em uma política de segurança de controle duplo.

   Uma pessoa instala o hash da chave pública SA. No menu **Nó de Criptografia**, clique em **Administração de Compartilhamento** > **Registrar Share Administration** e clique em Hash da Chave SA. Deve-se inserir o valor do hash que é obtido durante a criação da chave SA.

   O outro indivíduo instala a chave pública SA real. No menu **Nó de Criptografia**, clique em **Administração de Compartilhamento** > **Registrar Share Administration** e clique em Chave SA. Por padrão, as informações da chave pública estão no arquivo `sa.db`.

7. Use a chave CSS e a chave CSR para o nó SA e tenha as chaves que são certificadas.

   No menu suspenso **Nó de Criptografia**, selecione **Chaves de Administração de Compartilhamento**, **Certificar ChavesChave CSS**ou **Chave CSR**.

   Para a chave CSR, deve-se fornecer o número de série do coprocessador de destino como uma verificação processual, se uma chave apropriada estiver sendo certificada. Os procedimentos devem incluir a comunicação destas informações de uma maneira confiável.

8. No nó de origem, os indivíduos autorizados devem conectar-se à função para que seja permitido obter os compartilhamentos. Pelo menos os compartilhamentos m devem ser obtidos. Estes compartilhamentos são da atual chave mestra.

   No menu **Nó de Criptografia**, clique em **Administração de Compartilhamento** > **Obter Compartilhamento** e digite o número de compartilhamento a ser obtido. **Observe os números de série e os identificadores do banco de dados**. Quando essas ações estiverem de acordo, clique em Obter Compartilhamento. As informações de compartilhamento devem ser colocadas, por padrão, no arquivo `csr.db` e obtêm o certificado de chave CSR, por padrão, do arquivo `sa.db`.

   Obtenha as informações de validação da chave mestra atual para uso posterior no nó de destino. No menu **Chave Mestra**, clique em **Chaves Mestras DES/PKA** > **Verificar**. Clique em **Atual**.

9. No nó de destino, os indivíduos autorizados devem conectar-se à função, para que seja permitido que cada um deles instale a sua parte. Pelo menos os compartilhamentos m devem ser instalados para reconstituir a chave mestra no novo registro da chave mestra.

No menu **Nó de Criptografia**, clique em **Administração de Compartilhamento** > **Carregar Compartilhamento** e selecione o número de compartilhamento a ser instalado. Verifique se os números de série e os identificadores do banco de dados estão corretos e, em seguida, clique em **Observar os números de série e os identificadores do banco de dados**. Quando houver a confirmação de que esses compartilhamentos estão corretos, clique em Obter Compartilhamento. No nó de destino, os indivíduos autorizados devem conectar-se à função para que seja permitido que as pessoas instalem a sua parte. Por padrão, as informações de compartilhamento são obtidas no arquivo `csr.db` e o certificado da chave CSS é obtido, por padrão, no arquivo `sa.db`. Se o seu servidor tiver vários coprocessadores criptográficos que são carregados com o CCA, esses coprocessadores deverão ter as chaves mestras idênticas instaladas para o funcionamento do armazenamento de chaves.

Quando os compartilhamentos m forem carregados, verifique se a chave no novo registro da chave mestra é a mesma que a chave mestra atual no nó de origem, quando as ações foram obtidas. No nó de destino, no menu **Chave Mestra**, clique em **Chaves Mestras DES/PKA** > **Novo**.

10. Quando for confirmado por meio da verificação da chave mestra que a chave mestra foi clonada, um indivíduo autorizado poderá configurar a chave mestra. Essa ação exclui qualquer chave mestra antiga e move a chave mestra atual para o registro de chave mestre antiga. Os programas de aplicativos que usam chaves criptografadas pela chave mestra podem ser impactados por essa mudança, portanto, certifique-se de que a configuração da chave mestra seja feita de acordo com as necessidades dos programas de aplicativos.
11. No menu **Chave Mestra**, clique em **Chaves Mestras DES/PKA** > **Configurar**.

Utilizando as funções de utilitário CNM

Esta seção descreve o procedimento para usar as várias funções do utilitário CNM.

Selecionando um coprocessador específico

O procedimento para escolher um coprocessador dos diversos coprocessadores disponíveis no sistema.

Se seu sistema possuir vários coprocessadores carregados com o código do CCA, será necessário selecionar um coprocessador específico para trabalhar com ele. Se você não fizer uma seleção, você operará com o coprocessador padrão. Após fazer uma seleção do coprocessador, essa seleção entrará em vigor para a sessão do utilitário atual ou até que você faça uma outra seleção dentro da sessão do utilitário.

Para selecionar um coprocessador, clique em **Selecionar Adaptador** no menu **Nó de Criptografia**. Se você não selecionar um adaptador, o adaptador padrão será usado.

Nota:

1. Ao usar o utilitário CLU, os coprocessadores são referidos como 0, 1 e 2. Qualquer coprocessador específico pode ter ou não o aplicativo CCA instalado. Com o utilitário CNM (e outros aplicativos que usam a API do CCA), os coprocessadores carregados com o aplicativo CCA são designados como 1, 2 e 3. Esses novos identificadores são designados pelo CCA enquanto ele varre todos os coprocessadores instalados para aqueles carregados com o aplicativo CCA.
2. Ao codificar um aplicativo CCA, as palavras-chave **CRP01**, **CRP02** e **CRP03** são usadas para alocar um coprocessador. Elas correspondem aos números 1, 2 e 3 usadas no menu do utilitário CNM.

Inicializando o nó

O procedimento para inicializar o nó CCA para seu estado inicial.

Você pode restaurar o nó CCA para o estado inicial, contanto que a função com a qual você está operando (a função padrão ou uma função registrada) permita o uso do comando **Reinicializar Dispositivo** (deslocamento X'0111').

O uso do comando **Reinitialize Device** faz com que as ações a seguir ocorram:

- Limpar os registros da chave Mestra
- Limpar o Public Key Algorithm (PKA) retido e as chaves públicas PKA registradas
- Limpar as funções e os perfis e restaurar o controle de acesso para seu estado inicial.

Para inicializar o nó CCA, selecione **Inicializar** no menu Nó de Criptografia. Você será solicitado a confirmar sua ação.

Informações relacionadas:

"Estado inicial do sistema de controle de acesso" na página 27
O estado inicial tem uma função padrão inicial.

Efetuando logon e logoff no nó

Um usuário deve efetuar logon no coprocessador para poder ativar um perfil do usuário e a função associada. Esta é a única maneira de usar uma função diferente da função padrão.

Para efetuar logon, selecione **Efetuar logon na passphrase** no menu **Arquivo**.

Para efetuar logoff, selecione **Efetuar logoff** no menu **Arquivo**.

Nota: Com exceção da função DEFAULT, o acesso ao coprocessador é restrito pela autenticação por passphrase.

Carregando o Function-Control Vector

O procedimento para carregar o FCV do coprocessador.

Um Function-Control Vector (FCV) é um valor assinado fornecido pela IBM para permitir que o aplicativo CCA no coprocessador forneça um nível de serviços criptográficos consistentes com regulamentações de importação e de exportação aplicáveis. Sob os regulamentos atuais, todos os usuários são designados para o mesmo nível de funcionalidade criptográfica. Portanto, agora a IBM fornece um único FCV com o IBM Common Cryptographic Architecture (CCA) Support Program.

Use o utilitário CNM para carregar o FCV no coprocessador. O arquivo FCV é denominado `fcv_td4kECC521.crt`.

Para carregar o FCV:

1. No menu **Nó de Criptografia**, selecione **Autorização**.
2. No submenu resultante, clique em **Carregar** para especificar o arquivo FCV no disco. Especifique o nome do arquivo e clique em **Atualizar**. O utilitário carrega o FCV.
3. Clique em **OK**.

Configurando o Utilitário CCA Node Management

O procedimento para configurar os valores padrão para o utilitário CNM.

O painel de configuração do utilitário do CNM permite indicar os caminhos do diretório para os arquivos criados com o utilitário. No entanto, geralmente, o utilitário não usa os caminhos armazenados no painel de configuração. Em vez disso, os caminhos padrão são armazenados nas variáveis de ambiente do Windows. Você pode achar o painel de configuração um local útil para gravar quando desejar manter as várias classes de itens de dados.

Sincronizando o relógio e os calendários

O procedimento para sincronizar o relógio e os calendários no coprocessador e no computador host.

O coprocessador usa seu relógio e calendário para registrar o horário e a data e para evitar os ataques de repetição na autenticação de perfil baseada na passphrase. Após instalar o coprocessador, sincronize seu relógio e calendário com o do sistema host.

Para sincronizar o relógio e os calendários:

1. No menu **Nó de Criptografia**, clique em **Tempo**.
2. No submenu resultante, clique em **Configurar**.
3. Digite **Sim** para sincronizar o relógio e os calendários com o host.
4. Clique em **OK**.

Obtendo informações de status do aplicativo CCA

Você pode usar o coprocessador do utilitário CNM para obter o status do aplicativo CCA.

Os painéis do status suportado no coprocessador do utilitário CNM são:

Aplicativo CCA:
Exibe a versão e os dados de construção do aplicativo e exibe também o status dos registros da chave mestra.

Placa: Exibe o número de série, o ID e o nível de hardware do coprocessador.

Histórico do Comando:
Exibe os cinco comandos e subcomandos mais recentes enviados para o coprocessador.

Diagnósticos:
Indica se qualquer um dos sensores de violação do coprocessador foi acionado, se os erros foram registrados e reflete o status das baterias do coprocessador.

Controle de Exportação:
Exibe a força máxima das chaves criptográficas usadas pelo nó, conforme definido pelo Function-Control Vector (FCV) residente dentro do coprocessador.

Para visualizar os painéis de status:

1. No menu **Nó de Criptografia**, clique em **Status**. O status do aplicativo do CCA é exibido.
2. Para selecionar outras informações de status, use os botões na parte inferior.
3. Clique em **Cancelar**.

Informações relacionadas:

"Gerenciando as Chaves Mestras" na página 33
Uma chave mestra é usada para criptografar chaves de trabalho de nó local enquanto estiver armazenada fora do coprocessador.

Criando e gerenciando os dados de controle de acesso

O sistema de controle de acesso do IBM CCA Cryptographic Coprocessor Support Program define as circunstâncias sob as quais o coprocessador pode ser usado. Ele faz isso ao restringir o uso dos comandos do CCA.

Para uma lista desses comandos CCA, consulte a *Referência e Guia de Serviços Básicos do IBM CCA para o IBM 4765 PCIe e 4764 PCI-X Cryptographic Coprocessors*. Consulte também a seção "Comandos Necessários" no final de cada descrição do verbo.

Um administrador pode oferecer autoridade divergente aos usuários, para que alguns usuários possam usar os serviços do CCA não disponíveis para outras pessoas. Essa seção inclui uma visão geral do sistema de controle de acesso e as instruções para gerenciar os dados de controle de acesso. É necessário conhecer os comandos obrigatórios e sob quais circunstâncias. Considere que alguns comandos devem ser autorizados somente para pessoas confiáveis ou para determinados programas que operam em horários específicos. Geralmente, são autorizados somente aqueles comandos que são necessários, de modo a não permitir inadvertidamente um recurso que poderia ser usado para diminuir a segurança da instalação.

Você obterá as informações sobre o uso do comando a partir da documentação para os aplicativos que pretende suportar. Para orientação adicional, consulte *Referência e Guia de Serviços Básicos do IBM CCA para o IBM 4765 PCIe e 4764 PCI-X Cryptographic Coprocessors*.

Visão geral de controle de acesso

O sistema de controle de acesso restringe ou permite o uso de comandos com base nas funções e nos perfis do usuário.

Use o utilitário CNM para criar funções que correspondem às necessidades e privilégios de usuários designados.

Para acessar os privilégios designados a uma função que não é autorizada para uma função padrão, um usuário deve efetuar logon no coprocessador usando um perfil do usuário exclusivo. Cada perfil do usuário é associado a uma função e diversos perfis podem usar a mesma função. O coprocessador autentica os logons usando a passphrase que está associada ao perfil que identifica o usuário.

Nota: O termo *usuário* aplica-se a pessoas e programas.

O coprocessador sempre possui pelo menos uma função, a função padrão. O uso da função padrão não requer um perfil do usuário. Qualquer usuário pode usar os serviços permitidos pela função padrão sem efetuar login ou ser autenticado pelo coprocessador.

Por exemplo, um sistema básico pode incluir as seguintes funções:

- **Administrador do controle de acesso**: Pode criar novos perfis do usuário e modificar os direitos de acesso dos usuários atuais.
- **Executivo de gerenciamento de chaves**: Pode alterar as chaves criptográficas. Esta responsabilidade é melhor compartilhada por duas ou mais pessoas que fazem uso dos direitos de inserir as primeiras partes da chave ou as partes subsequentes.
- **Uso geral**: Pode usar os serviços criptográficos para proteger seu trabalho, mas não tem nenhum privilégio administrativo. Se o plano de segurança não exigir autenticação de logon para os usuários gerais, encaminhe seus requisitos na função padrão.

Nota: Alguns indivíduos seriam designados às funções do executivo de gerenciamento de chave ou do administrador de controle de acesso. Geralmente, a maior parte da população não efetuaria logon e, assim, teria direitos concedidos na função padrão.

Estado inicial do sistema de controle de acesso

O estado inicial tem uma função padrão inicial.

Depois de ter carregado o suporte ao software CCA no Segmento 3 do coprocessador, ou depois que o sistema de controle de acesso for iniciado, nenhum dado de controle de acesso existirá, exceto para uma função padrão inicial que permite que usuários não autenticados criem e carreguem os dados de controle de acesso.

Depois de criar as funções e perfis necessários para seu ambiente, incluindo as funções de supervisão necessárias para carregar os dados de controle de acesso e para gerenciar chaves criptográficas, remova todas as permissões que estão designados à função padrão. Em seguida, inclua apenas as permissões primárias que deseja conceder para usuários não autenticados.

Importante: O nó criptográfico e os dados que ele protege não estarão protegidos enquanto a função padrão puder carregar os dados de controle de acesso.

Informações relacionadas:

"Comandos de Função Padrão Iniciais" na página 44
As características da função padrão após o coprocessador ser inicializado e quando nenhum dado de controle de acesso existir serão descritas. Além disso, os comandos de controle de acesso ativados são

listados.

Criação de uma função

Uma função define as permissões e outras características dos usuários designados a essa função.

Para criar uma função, execute as seguintes etapas:

1. No menu **Controle de Acesso**, clique em **Funções**. Uma lista de funções definidas é atualmente exibida.
2. Selecione **Novo** para exibir a janela Gerenciamento de Função. A qualquer momento no processo, clique em **Lista** para retornar para a lista de funções definidas atualmente.

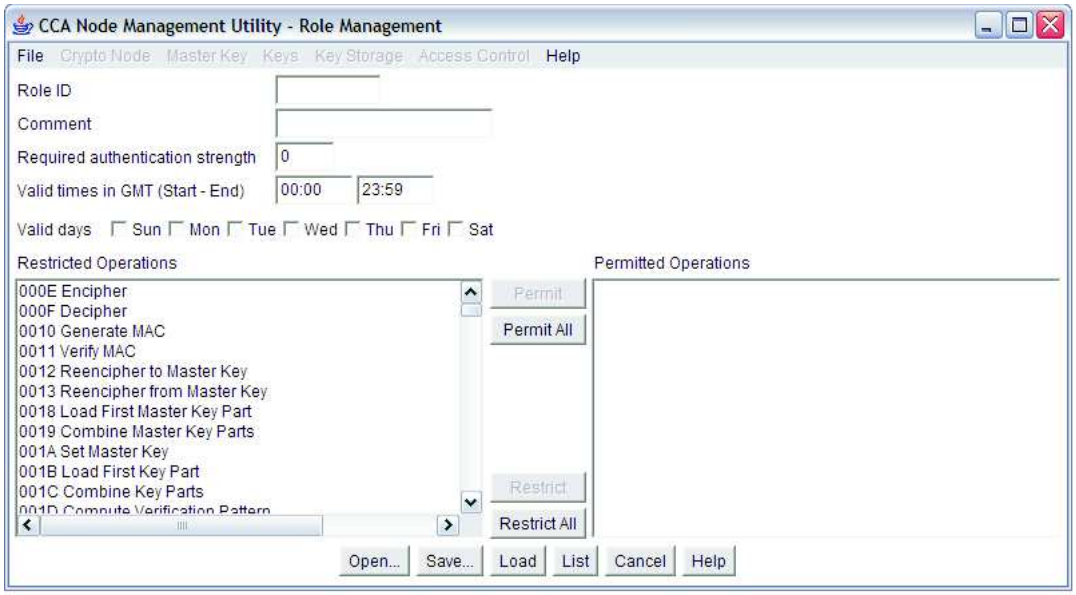

Figura 3. Janela Gerenciamento de Função

3. Defina a função usando os parâmetros a seguir:

ID da Função
Uma cadeia de caracteres que define o nome da função. Este nome está contido em cada perfil do usuário associado a esta função.

Comentário
Uma cadeia de caracteres opcional para descrever a função.

Força de autenticação necessária
Quando um usuário efetua logon, a força de autenticação fornecida é comparada com o nível de força necessário para a função. Se a força de autenticação for menor que a força necessária, o usuário não poderá efetuar logon. Atualmente, somente o método de autenticação da passphrase é suportado. Use uma força de 50.

Horas e dias válidos
Quando o usuário pode efetuar logon. Note que esses horários estão na Hora Universal Coordenada. Se você ainda não estiver familiarizado com o sistema de controle de acesso, consulte o capítulo sobre o sistema de controle de acesso do manual de Referência e Guia de Serviços Básicos do IBM CCA para o *IBM 4765 PCIe and 4764 PCI-X Cryptographic Coprocessors*.

Operações restritas e operações permitidas
Uma lista que define os comandos os quais a função pode usar.

Cada verbo de API CCA pode requerer um ou mais comandos para obter o serviço a partir do coprocessador. O usuário que solicita o serviço deve ser designado a uma função que permite que esses comandos precisem executar o verbo.

Para mais informações sobre as chamadas e os comandos do verbo CCA, consulte o manual de Referência e Guia de Serviços Básicos do IBM CCA para o *IBM 4765 PCIe and 4764 PCI-X Cryptographic Coprocessors*.

4. Clique em **Salvar** para salvar a função no disco.
5. Clique em **Carregar** para carregar a função dentro do coprocessador.

Modificando as funções existentes

É possível usar o utilitário CNM para editar um disco armazenado e uma função armazenada do coprocessador, e excluir uma função armazenada do coprocessador.

Nota: Qualquer função existente pode ser usada como um modelo para criar uma nova função. Ao abrir uma função salva, as informações existentes são exibidas na janela Definição de Função. É necessário somente modificar ou inserir as informações específicas para a nova função, fornecer-lhes um novo ID da função e carregar ou salvá-las.

Editando uma Função Armazenada do Disco:

Esta seção descreve o procedimento para editar uma função existente armazenada no disco.

Para editar uma função armazenada no disco, execute as etapas a seguir:

1. No menu **Controle de Acesso**, clique em **Funções**. Uma lista de funções definidas é atualmente exibida.
2. Clique em **Abrir**. Você será solicitado a selecionar um arquivo.
3. Abra um arquivo. Os dados são exibidos na janela Definição de Função.
4. Edite a função.
5. Clique em **Salvar** para salvar a função no disco.
6. Opcional: Clique em **Carregar** para carregar a função dentro do coprocessador.

Editando uma Função Armazenada do Coprocessador:

Esta seção descreve o procedimento para editar a função armazenada no coprocessador do CCA.

Para editar a função armazenada no coprocessador, execute as etapas a seguir:

1. No menu **Controle de Acesso**, clique em **Funções**. Uma lista de funções definidas é atualmente exibida.
2. Realce a função que deseja editar.
3. Clique em **Editar**. Os dados no painel Definição de Função são exibidos.
4. Edite a função.
5. Clique em **Salvar**. Para salvar a função no disco.
6. Opcional: Clique em **Carregar**. Para carregar a função no coprocessador

Excluindo uma Função Armazenada do Coprocessador:

Esta seção descreve o procedimento para excluir a função do coprocessador do CCA.

Importante: Ao excluir uma função, o utilitário CNM não exclui ou redesigna automaticamente os perfis do usuário associados a essa função. Deve-se excluir ou redesignar os perfis do usuário que são associados a uma função antes de excluir a função.

Para excluir uma função armazenada no coprocessador, execute as etapas a seguir:

1. No menu **Controle de Acesso**, clique em **Funções**. Uma lista de funções definidas é atualmente exibida.
2. Realce a função que deseja excluir.
3. Clique **Excluir**. A função foi excluída.

Criando um perfil do usuário

Um perfil do usuário identifica um usuário específico para o coprocessador.

Para criar um perfil do usuário, execute as seguintes etapas:

1. No menu **Controle de Acesso**, clique em **Perfis**. Uma lista de perfis definidos atualmente é exibida.
2. Selecione **Novo** para exibir a janela Gerenciamento de Perfil. Consulte Figura 4 para visualizar os campos da janela Gerenciamento de Perfil.

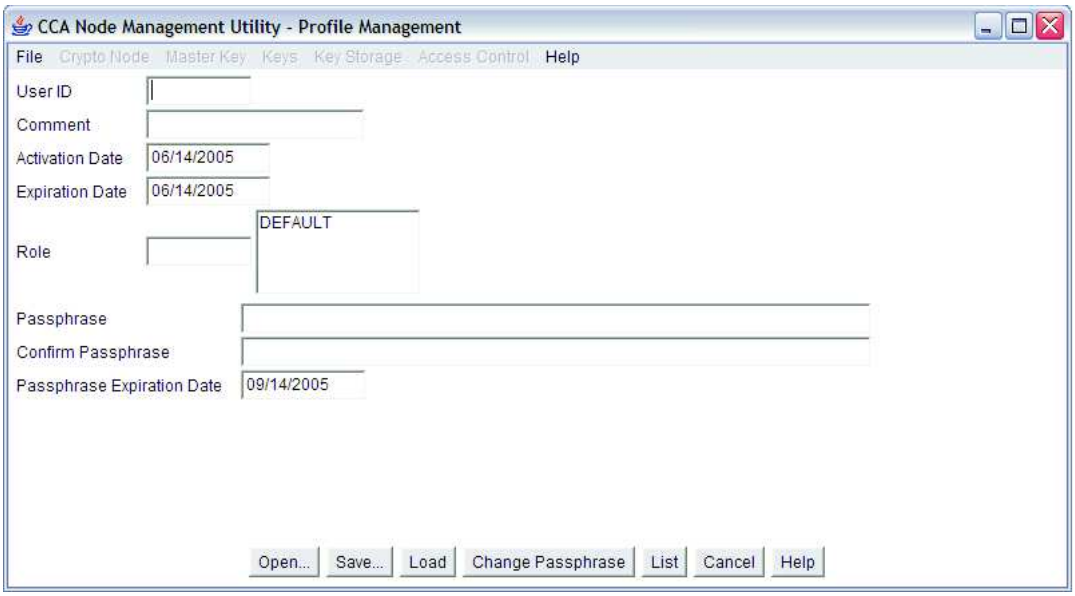

Figura 4. Painel de Gerenciamento de Perfil

3. Definir o perfil do usuário.

   Os campos do perfil do usuário a seguir:

   ID do usuário
   O nome fornecido a um perfil do usuário do coprocessador criptográfico.

   Comentário
   Uma cadeia de caracteres opcional para descrever o perfil do usuário.

   Data de Ativação e Data de Expiração
   A primeira e a última datas que o usuário pode efetuar logon do perfil do usuário.

   Função
   O nome da função que define as permissões concedidas para o perfil do usuário.

   Passphrase e Confirmar Passphrase
   A cadeia de caracteres que o usuário deve inserir para obter acesso ao nó criptográfico.

   Data de Expiração do Passphrase
   A data de expiração do passphrase. O utilitário configurará isso, por padrão, para 90 dias a

partir da data atual. É possível alterar a data de expiração. Cada passphrase contém uma data de expiração, que define o tempo de vida dessa passphrase. Isso é diferente da data de expiração do próprio perfil.

4. Clique em **Salvar**, para salvar o perfil no disco.
5. Opcional: Clique em **Carregar**, para carregar o perfil dentro do coprocessador.

Modificando o perfil existente

É possível usar o utilitário CNM para editar um disco e um perfil armazenados do coprocessador e excluir um perfil armazenado do coprocessador.

Nota: Qualquer perfil existente pode ser usado como um modelo para criar um novo perfil. Ao abrir um perfil salvo, as informações existentes são exibidas na janela Definição de Perfil. É necessário somente modificar ou inserir as informações específicas para o novo perfil, fornecer-lhes um novo ID do perfil e carregar ou salvá-las.

Editando um Perfil de Usuário Armazenado no Disco:

Esta seção descreve o procedimento para editar um perfil do usuário armazenado em um disco.

Para editar um perfil do usuário armazenado no disco, execute as etapas a seguir:

1. No menu **Controle de Acesso**, selecione **Perfis**. Uma lista de perfis definidos atualmente é exibida.
2. Clique em **Abrir**. Você será solicitado a selecionar um arquivo.
3. Abra um arquivo. Os dados são exibidos na janela Definição de Perfil do Usuário.
4. Edite o perfil.
5. Clique em **Salvar** para salvar o perfil no disco.
6. Opcional: Clique em **Carregar** para carregar o perfil dentro do coprocessador.

Editando um perfil do usuário armazenado no coprocessador:

Esta seção descreve o procedimento para editar o perfil do usuário no coprocessador do CCA.

Para editar um perfil do usuário armazenado no coprocessador, execute as etapas a seguir:

1. No menu **Controle de Acesso**, clique em **Perfis**. Uma lista de perfis definidos atualmente é exibida.
2. Destaque o perfil do usuário que deseja editar.
3. Clique em **Editar**. Os dados na janela Definição de Perfil são exibidos.
4. Edite o perfil do usuário.
5. Clique em **Salvar**. Para salvar o perfil no disco.
6. Opcional: Clique em **Carregar**. Para carregar o perfil no coprocessador

Excluindo um Perfil do Usuário Armazenado do Coprocessador:

Esta seção descreve o procedimento para excluir o perfil do usuário armazenado no coprocessador do CCA.

Para excluir um perfil armazenado no coprocessador, execute as etapas a seguir:

1. No menu **Controle de Acesso**, clique em **Perfis**. Uma lista de perfis do usuário definidos é atualmente exibida.
2. Destaque o perfil do usuário que deseja excluir.
3. Clique **Excluir**. O perfil do usuário foi excluído.

Reconfigurando Contagem de Falhas do Perfil do Usuário: Para evitar logons não autorizados, o sistema de controle de acesso mantém uma contagem de falhas de tentativa de logon para cada perfil do usuário. Se o número de tentativas com falhas para um perfil do usuário exceder o limite definido no perfil, o perfil ofensivo será desativado.

Para reconfigurar a contagem de falhas, execute as etapas a seguir:

1. No menu **Controle de Acesso**, clique em **Perfis**. Uma lista de perfis do usuário definidos é atualmente exibida.
2. Destaque o perfil do usuário.
3. Clique em **Reconfigurar o FC**. É exibida uma janela de confirmação.
4. Clique em **Sim** para confirmar. A contagem de falhas da tentativa de efetuar logon é configurada como 0.

Inicializando o sistema de controle de acesso

Quando você inicializa o sistema de controle de acesso, o utilitário CNM limpa os dados de controle de acesso no coprocessador e fornece a função padrão com os comandos necessários para carregar os dados de controle de acesso.

Importante: O nó criptográfico e os dados que ele protege não estarão protegidos enquanto a função padrão permitir carregar os dados de controle de acesso.

A execução bem-sucedida desta ação remove os controles de acesso e as chaves instalados e é, portanto, uma operação sensível que poderá renderizar o nó inoperante para a produção. Algumas instalações podem escolher remover a autorização para esta função a partir de suas funções do coprocessador. Neste evento, se você desejar inicializar o nó criptográfico do CCA, deverá remover o software CCA do coprocessador e reinstalar o software CCA.

Para inicializar o sistema de controle de acesso:

1. No menu **Controle de Acesso**, clique em **Inicializar**. É exibida uma janela de confirmação.
2. Selecione **Sim** para confirmar. O utilitário inicializa o sistema de controle de acesso.

Nota: Para iniciar o utilitário CCA Node Management, insira o comando **csufcnm**. O logotipo e a janela principal do utilitário CNM são exibidos.

Gerenciando chaves criptográficas

É possível usar o utilitário CNM para gerenciar as chaves mestras, gerenciar as Key-Encrypting Keys (KEKs) primárias, reconfigurar e gerenciar os armazenamentos de chaves de Data Encryption standard (DES), de Public Key Algorithm (PKA) e de Advanced Encryption Standard (AES). Os tipos de chaves são definidos da seguinte forma:

Uma **Chave Mestra** é um armazenamento KEK especial no texto não criptografado (não codificado) e é mantida dentro do módulo seguro do coprocessador. Esses três tipos de chave mestra são suportados: DES, PKA e AES. Eles são usados para agrupar outras chaves, de modo que essas chaves sejam armazenadas fora do módulo seguro. As chaves mestras DES e PKA são chaves de 168 bits formadas a partir de três chaves DES de 56 bits. As chaves mestras AES possuem 256 bits.

As **KEK Primárias** são chaves DES compartilhadas por nós criptográficos e, às vezes, referidas como chaves de transporte. Elas são usadas para criptografar outras chaves compartilhadas pelos nós. As KEKs Primárias, como a chave mestra, são instaladas a partir de partes de chave. O conhecimento das partes de chave pode ser compartilhado em partes por duas pessoas para causar uma divisão de conhecimento, uma política de segurança de controle duplo.

Outras chaves de DES, chaves de PKA e chaves de AES são chaves codificadas usadas para fornecer serviços criptográficos, como chaves de Media Access Control (MAC), chaves de DADOS e chaves de PKA privadas.

Nota: Ao trocar partes da chave não criptografada, assegure-se de que cada parte entenda como os dados trocados devem ser usados, porque o gerenciamento de partes da chave varia entre fabricantes diferentes e produtos de criptografia diferentes.

Gerenciando as Chaves Mestras

Uma chave mestra é usada para criptografar chaves de trabalho de nó local enquanto estiver armazenada fora do coprocessador.

Um CCA define três registros de chave mestra:

- O **registro da chave mestra atual** armazena a chave mestra usada atualmente pelo coprocessador para criptografar e decriptografar as chaves locais.
- O **registro da antiga chave mestra** armazena a chave mestra anterior e é usado para decriptografar chaves codificadas por essa chave mestra.
- O **registro da nova chave mestra** é um local provisório usado para armazenar informações da chave mestra conforme acumuladas para formar uma nova chave mestra.

O IBM Common Cryptographic Architecture (CCA) Support Program usa três conjuntos de registros de chave mestra, um conjunto para codificar as chaves DES (simétricas), um conjunto para codificar as chaves privadas PKA (assimétricas) e um conjunto para codificar as chaves AES (simétricas).

Comunicados:

1. O verbo de administração de chave mestra Master_Key_Distribution não suporta as chaves mestras AES. Os programas que usam os verbos de administração de chave mestra CCA Master_Key_Process e Master_Key_Distribution podem usar a palavra-chave ASYM-MK para direcionar as operações dos registros de chave mestra assimétrica PKA, usar a palavra-chave SYM-MK para direcionar os registros de chave mestra simétrica DES ou os dois conjuntos simétricos DES e assimétricos PKA dos registros de chave mestra. O utilitário CNM usa a opção **BOTH**. Se você usar outro programa para carregar as chaves mestras e se este programa operar especialmente nos registros de chave mestra SYM-MK ou ASYM-MK, em geral, você não estará mais apto a usar o utilitário CNM para administrar essas chaves mestras. Note que as chaves mestras do AES trabalham independentemente das chaves mestras DES e PKA.
2. Se a instalação tiver diversos coprocessadores criptográficos carregados com o CCA, será necessário administrar independentemente as chaves mestras em cada coprocessador.
3. Se a instalação tiver um servidor com diversos coprocessadores criptográficos carregados com o CCA, esses coprocessadores precisarão ser instalados com chaves mestras idênticas.

Informações relacionadas:

"Obtendo informações de status do aplicativo CCA" na página 26
Você pode usar o coprocessador do utilitário CNM para obter o status do aplicativo CCA.

Verificando uma Chave Mestra Existente:

O utilitário CNM gera um número de verificação para cada chave mestra que é armazenada nos registros de chave mestra. Esse número identifica a chave, mas não revela informações sobre o valor de chave real.

Para visualizar um número de verificação de chave mestra, siga estas etapas:

1. Na janela Carregar Chave Mestra, clique em **Chave Mestra**.
2. No menu **Chave Mestra**, selecione **Chaves Mestras DES/PKA** ou **Chave Mestra AES** e, em seguida, clique em **Verificar**; um submenu será exibido.
3. No submenu resultante, selecione um registro de chave mestra. O número de verificação para a chave armazenada neste registro é exibido.

Carregando uma Chave Mestra Automaticamente:

O utilitário CNM pode configurar automaticamente uma chave mestra no coprocessador. O valor da chave mestra não pode ser visualizado a partir do utilitário.

Importante: Se uma chave mestra de valor desconhecido for perdida, não será possível decriptografar a chave anexada a ela.

Para carregar automaticamente a chave mestra, siga estas etapas:

1. Na janela Carregar Chave Mestra, clique em **Chave Mestra**.
2. No menu **Chave Mestra**, selecione **Chaves Mestras DES/PKA** ou **Chave Mestra AES**.
3. Selecione **Configuração Automática** ou **Aleatório**. Você será solicitado a verificar o comando.
4. Clique em **Sim**. O coprocessador gera e configura uma chave mestra.

Nota:

1. A opção **Aleatório** é preferencial, pois a opção **Configuração Automática** passa as partes da chave não criptografadas pela memória do sistema host.
2. Ao configurar ou configurar automaticamente uma chave mestra, deve-se recodificar todas as chaves que foram codificadas sob a chave antiga.

Informações relacionadas:

"Recodificar as chaves armazenadas" na página 36

Carregando Uma Nova Chave Mestra a partir de Partes de Chave:

Para configurar uma chave mestra no coprocessador, insira qualquer parte da chave no registro de chave mestra e configure a nova chave mestra.

Para configurar a nova chave mestra, siga estas etapas:

1. No menu **Chave Mestra**, selecione **Chaves Mestras DES/PKA** ou **Chave Mestra AES** e, em seguida, clique em **Partes**. A janela Carregar Chave Mestra é exibida conforme mostrado em Figura 5.

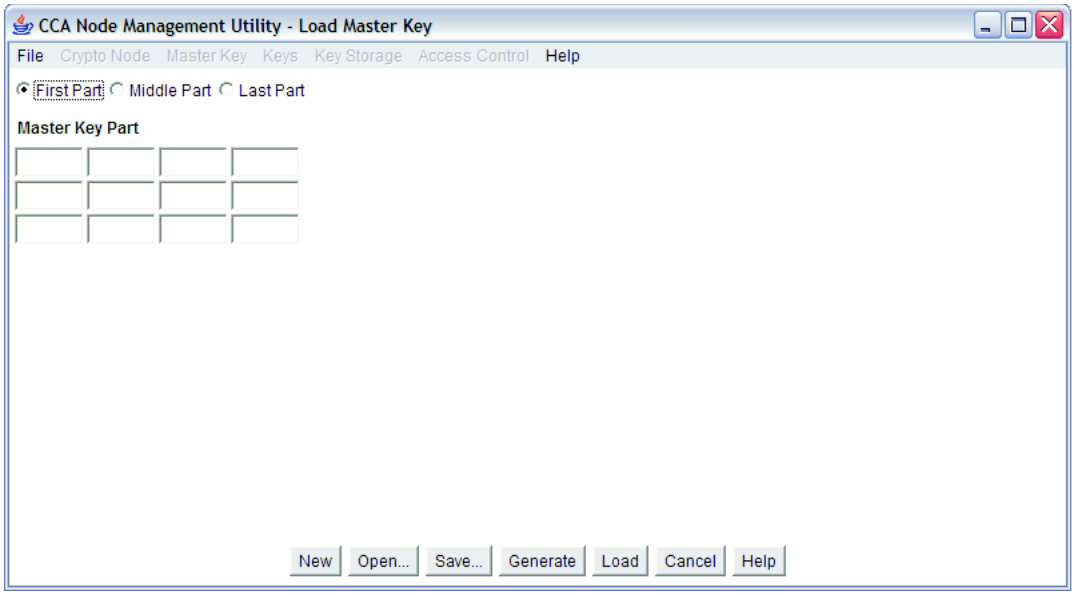

Figura 5. Janela Carregar Chave Mestra

2. Selecione o botão de opções para a parte da chave que você está editando (**Primeira Parte**, **Parte do Meio** ou **Última Parte**).
3. Insira os dados executando uma das ações a seguir:
   - Clique em **Novo** para limpar os dados inseridos com erro.
   - Clique em **Abrir** para recuperar dados pré-existente.
   - Clique em **Gerar** para preencher os campos com números aleatórios gerados pelo coprocessador.
   - Insira manualmente dados nos campos **Parte da Chave Mestra**. Cada campo aceita 4 dígitos hexadecimais.
4. Clique em **Carregar** para carregar a parte da chave no registro da nova chave mestra.
5. Clique em **Salvar** para salvar a parte da chave no disco.

   Importante: As partes da chave salvas no disco não são codificadas. Considere manter um disco com partes de chave nele armazenadas em uma área segura ou protegida.

   Nota: Ao criar uma chave de partes, você deverá ter a primeira e a última partes. A parte do meio é opcional.
6. Repita as etapas anteriores para carregar as partes da chave restantes para o registro da nova chave mestra.

   Nota: Para a política de segurança de conhecimento dividido, pessoas diferentes devem inserir as partes da chave separadamente. Para impingir uma política de segurança de controle duplo, o sistema de controle de acesso deve designar o direito para inserir a primeira chave em uma função e o direito para inserir as partes da chave subsequentes em outra função. Em seguida, os usuários autorizados podem efetuar logon e inserir sua respectiva parte da chave.
7. No menu **Chave Mestra**, selecione **Chaves Mestras DES/PKA** ou **Chave Mestra AES**.
8. Clique em **Configurar** para o utilitário para transferir os dados:
   a. Do registro da chave mestra atual para o registro da antiga chave mestra e para excluir a antiga chave mestra
   b. Do registro da nova chave mestra para o registro da chave mestra atual

Depois de configurar uma nova chave mestra, criptografe novamente as chaves que estão atualmente no armazenamento.

Links Relacionados: "Recodificar as chaves armazenadas" na página 36

Gerenciando o Armazenamento de Chaves

O utilitário CNM permite as funções básicas de gerenciamento de armazenamento de chaves para as chaves. As funções desse utilitário não formam um sistema de gerenciamento de chaves abrangente.

Os programas de aplicativo são mais bem adequados para executar as tarefas de gerenciamento de chaves repetitivas.

O armazenamento de chaves é um repositório de chaves que você acessa por um rótulo de chave usando rótulos definidos por você ou pelo seu aplicativo. O Padrão de Criptografia de Dados (DES), as chaves de algoritmo de chave pública (PKA) e Rivest-Shamir-Adleman (RSA) e as chaves Padrão de Criptografia Avançado (AES) chaves são mantidas em sistemas de armazenamento separados. Além disso, o armazenamento de chaves tem armazenamento interno limitado para as chaves PKA. As chaves armazenadas do coprocessador não são consideradas partes de armazenamento de chave nessa discussão.

Comunicados:

1. Se o seu servidor tiver vários coprocessadores criptográficos que são carregados com o CCA, esses coprocessadores deverão ter chaves mestras idênticas instaladas para que o armazenamento de chaves funcione corretamente.

2. O utilitário CNM exibe um máximo de 1.000 rótulos de chave. Se você tiver mais de 1.000 rótulos de chave no armazenamento de chaves, use um programa de aplicativo para gerenciá-los.

Criando ou inicializando o armazenamento de chaves: Para criar ou inicializar o armazenamento de chaves para as chaves Data Encryption Standard (DES), Public-Key Algorithm (PKA) ou Advanced Encryption Standard (AES), execute as etapas a seguir:

1. No menu **Armazenamento de Chaves**, selecione **Armazenamento de Chaves DES**, **Armazenamento de Chaves PKA** ou **Armazenamento de Chaves AES**.
2. No submenu resultante, clique em **Inicializar**. A janela Inicializar Armazenamento de Chaves DES, Inicializar Armazenamento de Chaves PKA ou Inicializar Armazenamento de Chaves AES é exibida.
3. Insira uma descrição para o arquivo de armazenamento de chaves.
4. Clique em **Inicializar**. Será solicitado que você insira um nome para o conjunto de dados de armazenamento de chaves.
5. Insira um nome para o arquivo e salve-o. O arquivo de armazenamento de chaves é criado no host.

   Nota: Se um arquivo com o mesmo nome existir, será solicitado que você verifique sua opção, pois a inicialização do armazenamento de chaves modificará o arquivo. Portanto, se o arquivo possuir algumas chaves, elas serão apagadas.

Recodificar as chaves armazenadas: Para recodificar as chaves no armazenamento em uma nova chave mestra, execute as etapas a seguir:

1. No menu **Armazenamento de Chave**, selecione **Armazenamento de Chave de DES**, **Armazenamento de Chave de PKA** ou **Armazenamento de Chave de AES**.
2. No submenu resultante, clique em **Gerenciar**; a janela Gerenciamento de Armazenamento de Chaves de DES, Gerenciamento de Armazenamento de Chaves de PKA ou Gerenciamento de Armazenamento de Chaves de AES será exibida. Este painel de janela lista os rótulos das chaves no armazenamento.
3. Clique em **Recodificar**. As chaves são recodificadas na chave no registro da chave mestra atual.

Excluindo uma Chave Armazenada: Para excluir uma chave armazenada, execute as etapas a seguir:

1. No **Armazenamento de Chave**, clique em **Armazenamento de Chaves de DES**, **Armazenamento de Chaves de PKA** ou **Armazenamento de Chaves de AES**.
2. No submenu resultante, clique em **Gerenciar**. A janela Gerenciamento de Armazenamento de Chaves de DES, Gerenciamento de Armazenamento de Chaves de PKA ou Gerenciamento de Armazenamento de Chaves de AES é exibida. Esta janela lista os rótulos das chaves no armazenamento.

   Você pode configurar critérios de filtragem para listar um subconjunto de chaves no armazenamento. Por exemplo, se você inserir `*.mac` como o critério de filtro e atualizar a lista, o subconjunto será limitado às chaves com rótulos que terminam em .mac. (O asterisco é um caractere curinga).
3. Realce o rótulo da chave para a chave a ser excluída.
4. Clique **Excluir**. Uma mensagem de confirmação será exibida.
5. Clique em **Sim**. Para confirmar que a chave armazenada foi excluída.

Criando um Rótulo de Chave: Para criar um rótulo de chave, execute as etapas a seguir:

1. No menu **Armazenamento de Chaves**, clique em **Armazenamento de Chaves de DES**, **Armazenamento de Chaves de PKA** ou **Armazenamento de Chaves de AES**.
2. No submenu resultante, clique em **Gerenciar**. A janela Gerenciamento de Armazenamento de Chaves de DES, Gerenciamento de Armazenamento de Chaves de PKA ou Gerenciamento de Armazenamento de Chaves de AES é exibida. Esta janela lista os rótulos das chaves no armazenamento.

   Você pode configurar critérios de filtragem para listar um subconjunto de chaves no armazenamento. Por exemplo, se você inserir `*.mac` como o critério de filtro e atualizar a lista, o subconjunto será limitado às chaves que possuem rótulos que terminam em .mac. (O asterisco é um caractere curinga).
3. Clique em **Novo**. Você será solicitado a inserir um rótulo de chave.
4. Clique em **Carregar**. O rótulo de chave é carregado no armazenamento.

Criando e armazenando KEKs primárias do DES

As key encrypting keys (KEKs) são criptografadas sob a chave mestra do Padrão de Criptografia de Dados (DES) e armazenados no armazenamento de chaves DES para uso local.

As partes da chave usadas para criar uma KEK podem ser geradas ou inseridas aleatoriamente como informações de texto não criptografado. As partes também podem ser salvas no disco ou no disquete no texto não criptografado a ser transportado para outros nós ou para recriação da KEK local.

Nota: O utilitário Cryptographic Node Management (CNM) suporta somente as KEKs do DES para o transporte de chaves entre nós. Os aplicativos podem usar a API do CCA para fornecer os serviços necessários para a distribuição da chave baseada em chave pública ou baseada no Padrão de Criptografia Avançado (AES).

Para criar e armazenar uma KEK primária do DES (ou outra chave operacional de comprimento duplo), execute as etapas a seguir:

1. No menu **Chaves**, clique em **Chave de criptografia de chaves primárias do DES**. A janela Chave de criptografia de chaves primárias do DES é exibida.

   A qualquer momento, é possível clicar em **Novo** para limpar todos os campos de dados e reconfigurar todos os botões de opções para suas configurações padrão.
2. Selecione o botão de opções para a parte da chave pretendida a ser inserida: **Primeira Parte**, **Parte do Meio** ou **Última Parte**.
3. Insira os dados nos campos **Parte da Chave** executando uma das ações a seguir:
   - Clique em **Abrir** para recuperar os dados **Parte da Chave**, **Vetor de Controle** e **Rótulo da Chave** pré-existentes, que foram previamente armazenados no disco usando o comando **Salvar**.
   - Clique em **Gerar** para preencher os campos **Parte da Chave** com números aleatórios gerados pelo coprocessador.
   - Insira manualmente os dados nos campos **Parte da Chave**. Cada um dos campos **Parte da Chave** aceita 4 dígitos hexadecimais.
4. Selecione um vetor de controle para a chave:
   - Para usar um vetor de controle KEK padrão, selecione o botão de opções **Importador Padrão** ou **Exportador Padrão** apropriado.
   - Para usar um vetor de controle de customização, selecione o botão de opções **Customizar**. Nos campos **Vetor de Controle**, insira a metade esquerda ou direita de um vetor de controle para qualquer chave de comprimento duplo. Observe que o bit da parte da chave (bit 44) deve estar ativo e que cada byte do vetor de controle deve ter uma paridade par.

     Para informações detalhadas sobre os vetores de controle, consulte Referência e Guia de Serviços Básicos do IBM CCA para o manual do *IBM 4765 PCIe and 4764 PCI-X Cryptographic Coprocessors*.
5. Insira um rótulo de chave para identificar o token de chave no armazenamento de chaves.
6. Clique em **Carregar** para carregar a parte da chave no coprocessador e armazenar o token da chave resultante no armazenamento da chave.
7. Clique em **Salvar** para salvar a parte da chave não criptografada e seu vetor de controle associado e os valores da etiqueta no disco.
8. **Salvar** no disco ou **Carregar** no armazenamento de chaves. As informações restantes da parte de chave, seguindo as etapas 2 - 7. Certifique-se de usar o mesmo rótulo de chave para cada parte de uma chave única.

Criando outros nós usando o utilitário CNI

Criar uma lista CNI para o utilitário CCA Node Initialization (CNI) permite o carregamento as chaves e os dados de controle de acesso armazenados no disco em outros nós criptográficos, sem executar o utilitário CNM nesses nós de destino.

Para configurar um nó usando o utilitário CNI, execute as etapas a seguir:

1. Inicie o utilitário CCA Node Management inserindo o comando **csufcnm**. O logotipo e o painel principal do utilitário CNM são exibidos.
2. Salve na mídia do host ou portátil, como um disquete, o acesso ao controle de dados e chaves que deseja instalar em outros nós. Quando executar o utilitário CNI no nó de destino, ele procura pelo caminho do diretório idêntico para cada arquivo. Por exemplo:
   - Se você salvar um perfil do usuário no diretório de nó estabelecido `c:\IBM4764\profiles`, o utilitário CNI procurará pelo diretório de nó de destino `c:\IBM4764\profiles`.
   - Se você salvar um perfil do usuário no diretório de disquete `a:\profiles`, o utilitário CNI procurará pelo diretório de nó de destino `a:\profiles`.
3. No menu **Arquivo**, clique em **Editor do CNI**. A janela Editor de Inicialização do Nó CCA é exibida conforme mostrado em Figura 6.

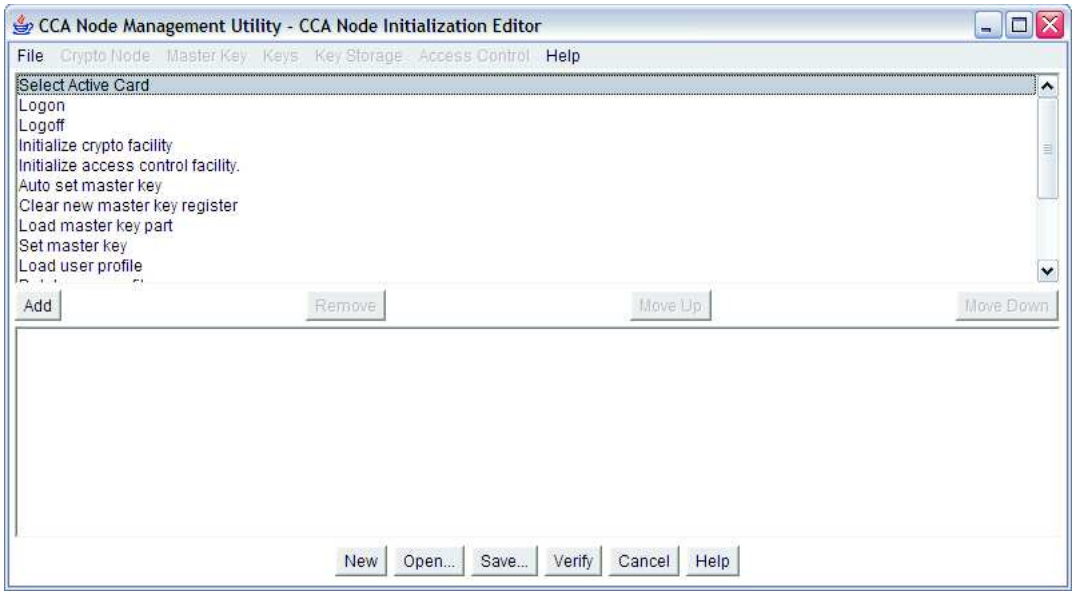

Figura 6. Janela Editor de Inicialização do Nó CCA

A lista na área de janela superior da janela exibe as funções que podem ser incluídas na lista CNI. A área de janela da parte inferior lista as funções incluídas na lista CNI atual. As referências das chaves mestras na lista referem-se às chaves mestras DES e PKA.

4. Incluir as funções desejadas. Para incluir uma função na lista de CNI:
   a. Destaque uma função.
   b. Clique em **Incluir**. A função é incluída na lista CNI.

      Nota: Se a função escolhida carregar um objeto de dados, como uma parte da chave, um arquivo de armazenamento de chaves, um perfil do usuário ou uma função, será solicitado que você insira o nome do arquivo ou o ID do objeto a ser carregado.
5. Usando os botões **Mover para Cima** e **Mover para Baixo**, organize as funções para refletir a mesma ordem a ser seguida quando usar o utilitário CNM. Por exemplo, se você estiver carregando dados de controle de acesso.
6. Clique em **Verificar** para confirmar se os objetos foram criados corretamente.
7. Clique em **Salvar**. Será solicitado que você selecione um nome e um local do diretório para o arquivo de lista CNI.
8. Salve o arquivo de lista CNI. O arquivo de lista não contém os objetos de dados especificados na lista CNI.

9. Copie os arquivos necessários para que o utilitário CNI destine os locais do diretório do host que espelhem seus locais no host de origem. Se você salvou os arquivos na mídia portátil, insira a mídia no nó de destino.
10. No nó de destino, execute a lista usando o utilitário CNI inserindo o comando **csufcni**.

    Se a lista CNI incluir um logon, insira **csulcni** ou **csuncni** na linha de comandos (sem especificar um nome). As informações da ajuda do utilitário CNI descrevem a sintaxe para inserir um ID e uma passphrase.

    O utilitário CNI carrega os arquivos no coprocessador a partir do host ou mídia portátil, conforme especificado pela lista CNI.

Construindo Aplicativos para Usar com a API CCA

Um aplicativo pode ser construído, o qual pode ser usado com a API do Common Cryptographic Architecture (CCA).

O código de origem para a rotina de amostra é incluído com o software. Você pode usar a amostra incluída para testar o coprocessador e o Support Program.

Nota: Os locais do arquivo referidos nesta seção são os caminhos do diretório padrão.

Visão geral de verbos CCA

Programas do aplicativo e do utilitário emitem pedidos de serviço para o coprocessador criptográfico ao chamar os verbos CCA. O termo *verbo* implica em uma ação que um programa de aplicativo pode iniciar. O código do sistema operacional por sua vez chama o physical device driver (PDD) do coprocessador. O hardware e o software acessado pela API são um subsistema integrado.

As chamadas de verbo são gravadas na sintaxe padrão da linguagem de programação C e incluem um nome de ponto de entrada, parâmetros de verbo e as variáveis para esses parâmetros.

Para obter uma listagem detalhada dos verbos, das variáveis e dos parâmetros que podem ser usados ao programar a interface de programação de aplicativos (API) de segurança do CCA, consulte o *Manual de Referência e Guia de Serviços Básicos do IBM CCA para o IBM 4765 PCIe e 4764 PCI-X Cryptographic Coprocessors*.

Chamando Verbos CCA na Sintaxe do Programa C

Em cada ambiente do sistema operacional, você pode codificar as chamadas de verbo da API do CCA usando a sintaxe da linguagem de programação C padrão.

Os protótipos de chamada de função para todos os verbos da API de segurança do CCA estão contidos em um arquivo de cabeçalho. Os arquivos e os locais de distribuição padrão são:

AIX /usr/include/

Para incluir essas declarações de verbo, use a seguinte diretiva do compilador no seu programa:

AIX
```
#include "csufincl.h"
```

Para emitir uma chamada para um verbo da API de segurança do CCA, codifique o nome de ponto de entrada do verbo em caracteres maiúsculos. Separe os identificadores de parâmetro com vírgulas e coloque-os entre parênteses. Termine cada chamada com um caractere ponto e vírgula. Por exemplo:

```
CSNBCKI (&return_code,
         &reason_code,
         &exit_data_length,    /* exit_data_length */
         exit_data,            /* exit_data       */
         clear_key,
         key_token);
```

Nota: O terceiro e quarto parâmetros de uma chamada do CCA, *exit_data_length* e *exit_data*, não são suportados atualmente pelo CCA Cryptographic Coprocessor Support Program. Embora seja permitido codificar ponteiros de endereço nulo para esses parâmetros, é preferível especificar um número inteiro longo avaliado como 0 com o parâmetro *exit_data_length*.

Compilando e vinculando programas de aplicativos CCA

O CCA Cryptographic Coprocessor Support Program inclui o código fonte de Linguagem C e o makefile para um programa de amostra.

O arquivo e seu local de distribuição padrão a seguir:

AIX `/usr/lpp/csufx.4765/samples/c.`

Compile os programas de aplicativos que usam o CCA e vincule os programas compilados à biblioteca do CCA. A biblioteca e seu local de distribuição padrão estão a seguir:

AIX `/usr/lib/libcsufcca.a.`

Rotina C de Amostra: Gerando um MAC

Para ilustrar o aplicativo prático de chamadas de verbo CCA, este tópico descreve a rotina da linguagem de programação C de amostra incluída com o CCA Cryptographic Coprocessor Support Program.

Também há um programa de amostra no website do produto. Esse programa de amostra pode ajudá-lo a entender o desempenho da implementação do CCA.

A rotina de amostra gera um message authentication code (MAC) em uma cadeia de texto e, em seguida, verifica o MAC. Para gerar e verificar o MAC, a rotina:

1. Chama o verbo **Key_Generate** (CSNBKGN) para criar um MAC e um par de chaves MACVER.
2. Chama o verbo **MAC_Generate** (CSNBMGN) para gerar um MAC em uma cadeia de texto com a chave MAC.
3. Chama o verbo **MAC_Verify** (CSNBMVR) para verificar o MAC de cadeia de texto com a chave MACVER.

Uma rotina de amostra é mostrada no Figura 7, consulte o *manual de Referência e Guia de Serviços Básicos do IBM CCA para o IBM 4765 PCIe e 4764 PCI-X Cryptographic Coprocessors* para obter as descrições dos verbos e seus parâmetros. Esses verbos são listados na tabela a seguir.

Tabela 5. Verbo Chamados pela Rotina de Amostra

Verbo	Nome do ponto de entrada
Key_Generate	CSNBKGN
MAC_Generate	CSNBMGN
MAC_Verify	CSNBMVR

Figura 7. Rotina C de amostra: gerando um MAC

```
/*********************************************************************/
/*                                                                   */
/* Module Name: mac.c                                                */
/*                                                                   */
/* NOME DESCRITIVO: Cryptographic Coprocessor Support Program        */
/*                  Exemplo de código de origem da linguagem C       */
/*                                                                   */
/*-------------------------------------------------------------------*/
/*                                                                   */
/* Materiais Licenciados- Propriedade da IBM                         */
/*                                                                   */
```

```
/* (C) Copyright IBM Corp. 1997-2010 Todos os Direitos Reservados    */
/*                                                                   */
/* US Government Users Restricted Rights - Use duplication or        */
/* disclosure restricted by GSA ADP Schedule Contract with IBM Corp. */
/*                                                                   */
/*-------------------------------------------------------------------*/
/*                                                                   */
/*        NOTICE TO USERS OF THE SOURCE CODE EXAMPLES                */
/*                                                                   */
/* The source code examples provided by IBM are only intended to     */
/* assist in the development of a working software program. The       */
/* source code examples do not function as written: additional       */
/* code is required. In addition, the source code examples may       */
/* not compile and/or bind successfully as written.                  */
/*                                                                   */
/* International Business Machines Corporation provides the source   */
/* code examples, both individually and as one or more groups,       */
/* "as is" without warranty of any kind, either expressed or         */
/* implied, including, but not limited to the implied warranties of  */
/* merchantability and fitness for a particular purpose. The entire  */
/* risk as to the quality and performance of the source code         */
/* examples, both individually and as one or more groups, is with    */
/* you. Should any part of the source code examples prove defective, */
/* you (and not IBM or an authorized dealer) assume the entire cost  */
/* of all necessary servicing, repair or correction.                 */
/*                                                                   */
/* IBM does not warrant that the contents of the source code         */
/* examples, whether individually or as one or more groups, will     */
/* meet your requirements or that the source code examples are       */
/* error-free.                                                       */
/*                                                                   */
/* IBM may make improvements and/or changes in the source code       */
/* examples at any time.                                             */
/*                                                                   */
/* Changes may be made periodically to the information in the        */
/* source code examples; these changes may be reported, for the      */
/* sample code included herein, in new editions of the examples.     */
/*                                                                   */
/* References in the source code examples to IBM products, programs, */
/* or services do not imply that IBM intends to make these           */
/* available in all countries in which IBM operates. Any reference   */
/* to the IBM licensed program in the source code examples is not    */
/* intended to state or imply that IBM's licensed program must be    */
/* used. Any functionally equivalent program may be used.            */
/*                                                                   */
/*-------------------------------------------------------------------*/
/*                                                                   */
/* This example program:                                             */
/*                                                                   */
/* 1) Calls the Key_Generate verb (CSNBKGN) to create a MAC (message */
/*    authentication code) key token and a MACVER key token.         */
/*                                                                   */
/* 2) Calls the MAC_Generate verb (CSNBMGN) using the MAC key token  */
/*    from step 1 to generate a MAC on the supplied text string      */
/*    (INPUT_TEXT).                                                  */
/*                                                                   */
/* 3) Calls the MAC_Verify verb (CSNBMVR) to verify the MAC for the  */
/*    same text string, using the MACVER key token created in        */
/*    step 1.                                                        */
/*                                                                   */
/*********************************************************************/
#include <stdio.h>
#include <string.h>

#ifdef _AIX
  #include <csufincl.h>
#elif __WINDOWS__
```

```
  #include "csunincl.h"
#else
  #include "csulincl.h"     /* else linux */
#endif

/* Defines */
#define KEY_FORM            "OPOP"
#define KEY_LENGTH          "SINGLE  "
#define KEY_TYPE_1          "MAC     "
#define KEY_TYPE_2          "MACVER  "
#define INPUT_TEXT          "abcdefghijklmn0987654321"
#define MAC_PROCESSING_RULE "X9.9-1  "
#define SEGMENT_FLAG        "ONLY    "
#define MAC_LENGTH          "HEX-9   "
#define MAC_BUFFER_LENGTH   10

void main()
{
  static long          return_code;
  static long          reason_code;
  static unsigned char key_form[4];
  static unsigned char key_length[8];
  static unsigned char mac_key_type[8];
  static unsigned char macver_key_type[8];
  static unsigned char kek_key_id_1[64];
  static unsigned char kek_key_id_2[64];
  static unsigned char mac_key_id[64];
  static unsigned char macver_key_id[64];
  static long          text_length;
  static unsigned char text[26];
  static long          rule_array_count;
  static unsigned char rule_array[3][8];       /* Max 3 rule array elements  */
  static unsigned char chaining_vector[18];
  static unsigned char mac_value[MAC_BUFFER_LENGTH];

  /* Print a banner */
  printf("Cryptographic Coprocessor Support Program example program.\n");

  /* Set up initial values for Key_Generate call */
  return_code = 0;
  reason_code = 0;
  memcpy (key_form,        KEY_FORM,   4);     /* OPOP key pair              */
  memcpy (key_length,      KEY_LENGTH, 8);     /* Single-length keys         */
  memcpy (mac_key_type,    KEY_TYPE_1, 8);     /* 1st token, MAC key type    */
  memcpy (macver_key_type, KEY_TYPE_2, 8);     /* 2nd token, MACVER key type */
  memset (kek_key_id_1,  0x00, sizeof(kek_key_id_1));  /* 1st KEK not used   */
  memset (kek_key_id_2,  0x00, sizeof(kek_key_id_2));  /* 2nd KEK not used   */
  memset (mac_key_id,    0x00, sizeof(mac_key_id));    /* Init 1st key token */
  memset (macver_key_id, 0x00, sizeof(macver_key_id)); /* Init 2nd key token */

  /* Generate a MAC/MACVER operational key pair */
  CSNBKGN(&return_code,
          &reason_code,
          NULL,                                /* exit_data_length           */
          NULL,                                /* exit_data                  */
          key_form,
          key_length,
          mac_key_type,
          macver_key_type,
          kek_key_id_1,
          kek_key_id_2,
          mac_key_id,
          macver_key_id);

  /* Check the return/reason codes. Terminate if there is an error.         */
  if (return_code != 0 || reason_code != 0) {
    printf ("Key_Generate failed: ");             /* Print failing verb      */
    printf ("return_code = %ld, ",  return_code); /* Print return code       */
```

```
  printf ("reason_code = %ld.\n", reason_code); /* Print reason code      */
  return;
}
else
  printf ("Key_Generate successful.\n");
/* Set up initial values for MAC_Generate call */
return_code = 0;
reason_code = 0;
text_length = sizeof (INPUT_TEXT) - 1;          /* Length of MAC text      */
memcpy (text, INPUT_TEXT, text_length);         /* Define MAC input text   */
rule_array_count = 3;                           /* 3 rule array elements   */
memset (rule_array, ' ', sizeof(rule_array));   /* Clear rule array        */
memcpy (rule_array[0], MAC_PROCESSING_RULE, 8); /* 1st rule array element  */
memcpy (rule_array[1], SEGMENT_FLAG,        8); /* 2nd rule array element  */
memcpy (rule_array[2], MAC_LENGTH,          8); /* 3rd rule array element  */
memset (chaining_vector, 0x00, 18);             /* Clear chaining vector   */
memset (mac_value, 0x00, sizeof(mac_value));    /* Clear MAC value         */

/* Generate a MAC based on input text */
CSNBMGN ( &return_code,
         &reason_code,
         NULL,                                  /* exit_data_length        */
         NULL,                                  /* exit_data               */
         mac_key_id,                            /* Output from Key_Generate*/
         &text_length,
         text,
         &rule_array_count,
         &rule_array[0][0],
         chaining_vector,
         mac_value);

/* Check the return/reason codes. Terminate if there is an error.          */
if (return_code != 0 || reason_code != 0) {
  printf ("MAC Generate Failed: ");             /* Print failing verb      */
  printf ("return_code = %ld, ",  return_code); /* Print return code       */
  printf ("reason_code = %ld.\n", reason_code); /* Print reason code       */
  return;
}
else {
  printf ("MAC_Generate successful.\n");
  printf ("MAC_value = %s\n", mac_value);    /* Print MAC value (HEX-9)    */
}
/* Set up initial values for MAC_Verify call */
return_code = 0;
reason_code = 0;
rule_array_count = 1;                           /* 1 rule array element    */
memset (rule_array, ' ', sizeof(rule_array));/* Clear rule array           */
memcpy (rule_array[0], MAC_LENGTH, 8);          /* Rule array element      */
                                                /*  (use default Ciphering */
                                                /*  Method and Segmenting  */
                                                /*  Control)               */
memset (chaining_vector, 0x00, 18);             /* Clear the chaining vector*/

/* Verify MAC value */
CSNBMVR (&return_code,
         &reason_code,
         NULL,                                  /* exit_data_length        */
         NULL,                                  /* exit_data               */
         macver_key_id,                         /* Output from Key_Generate*/
         &text_length,                          /* Same as for MAC_Generate*/
         text,                                  /* Same as for MAC_Generate*/
         &rule_array_count,
         &rule_array[0][0],
         chaining_vector,
         mac_value);                            /* Output from MAC_Generate*/
```

```
  /* Check the return/reason codes. Terminate if there is an error.         */
  if (return_code != 0 || reason_code != 0) {
    printf ("MAC_Verify failed: ");              /* Print failing verb      */
    printf ("return_code = %ld, ", return_code);  /* Print return code      */
    printf ("reason_code = %ld.\n", reason_code); /* Print reason code      */
    return;
  }
  else                                       /* No error occurred          */
    printf ("MAC_Verify successful.\n");
}
```

Aprimorando Rendimento com o Coprocessador CCA e o 4765

Quando você usa a API do CCA, as características do seu programa de aplicativo host afetarão o desempenho e o rendimento do 4765. Para um melhor desempenho no coprocessador 4765, avalie e projete o aplicativo baseado em multiencadeamento, multiprocessamento e nas chaves de armazenamento em cache Data Encryption Standard (DES), Public-Key Algorithm (PKA) e Advanced Encryption Standard (AES).

Multiencadeamento e multiprocessamento

O aplicativo CCA em execução no 4765 pode processar vários pedidos do CCA simultaneamente. O coprocessador contém vários elementos de hardware independentes, incluindo o mecanismo com o algoritmo Rivest-Shamir-Adleman (RSA), o mecanismo Data Encryption Standard (DES), a CPU, o gerador de número aleatório e a interface de comunicações Peripheral Component Interconnect-X (PCI-X). Todos esses elementos podem trabalhar ao mesmo tempo, processando partes de verbos CCA diferentes. Ao trabalhar com vários verbos ao mesmo tempo, o coprocessador pode manter todos os elementos do hardware ocupados, aumentando o rendimento geral do sistema.

Para aproveitar-se deste recurso, o sistema host deve enviar diversas solicitações CCA para o coprocessador sem ter que aguardar que cada uma seja concluída antes de enviar a próxima. A melhor maneira de enviar diversas solicitações é designar um programa de aplicativo do host multiencadeado, em que cada encadeamento possa enviar independentemente solicitações CCA ao coprocessador. Por exemplo, um servidor da Web pode iniciar um novo encadeamento para cada solicitação que recebe por meio da rede. Cada um desses encadeamentos enviarão os pedidos criptográficos necessários para o coprocessador, independente de do que outros encadeamentos estão fazendo. O modelo multiencadeado garante que o coprocessador não esteja subutilizado. Outra opção é ter vários programas de aplicativo host independentes usando o coprocessador ao mesmo tempo.

Armazenando em Cache as Chaves DES, PKA e AES

O software CCA para o 4765 mantém cópias de as chaves DES, PKA e AES criptografadas (sem texto não criptografado) usadas recentemente em caches dentro do módulo seguro. As chaves são armazenadas em um formulário que foi decriptografado e validado e que está pronto para o uso. Se a mesma chave for reusada em um pedido CCA posterior, o 4765 poderá usar a cópia em cache e evitar a sobrecarga associada à decriptografia e validar o token de chave. Além disso, para chaves PKA retidas, o cache elimina a sobrecarga de recuperação da chave da memória flash interna Erasable Programmable Read Only Memory (EPROM).

Como resultado, os aplicativos que reutilizam um conjunto comum de chaves podem ser executados muito mais rápido que esses que usam chaves diferentes para cada transação. A maioria dos aplicativos comuns usam um conjunto comum de chaves DES, chaves privadas PKA e chaves AES criptografadas e o armazenamento em cache é efetivo na melhoria do rendimento. As chaves públicas PKA e chaves não criptografadas AES, que têm pouco gasto adicional de processamento, não são armazenadas em cache.

Comandos de Função Padrão Iniciais

As características da função padrão após o coprocessador ser inicializado e quando nenhum dado de controle de acesso existir serão descritas. Além disso, os comandos de controle de acesso ativados são listados.

Para os comandos de função padrão inicial, o ID de função é o padrão e a força de autenticação é zero. A função padrão é válida todas as vezes do dia e em todos os dias da semana. As únicas funções permitidas são aquelas necessárias para carregar os dados de controle de acesso.

Importante: O modo criptográfico não é seguro quando usuários não autenticados puderem carregar os dados de controle de acesso utilizando a função padrão. Restrinja esses comandos para as funções supervisoras selecionadas.

O Tabela 6 lista os comandos de controle de acesso que são ativados na função padrão, quando o software CCA for inicialmente carregado e quando o nó CCA for inicializado.

Tabela 6. Comandos de Função Padrão Iniciais

Cód.	Nome do comando
X'0107'	Hash Unidirecional, SHA-1
X'0110'	Configurar Relógio
X'0111'	Reinicializar Dispositivo
X'0112'	Inicializar Sistema de Controle de Acesso
X'0113'	Alterar Data de Expiração do Perfil do Usuário.
X'0114'	Alterar Dados de Autenticação do Perfil do Usuário.
X'0115'	Reconfigurar Contagem de Falhas de Tentativas de Logon do Perfil do Usuário
X'0116'	Ler Informações de Controle de Acesso Público
X'0117'	Excluir Perfil do Usuário
X'0118'	Excluir Função
X'0119'	Carregar Function-Control Vector
X'011A'	Limpar o Function-Control Vector

Conteúdo do Machine-Readable Log

O utilitário CLU cria dois arquivos de log, um destinado para leitura e outro para uma possível entrada para um programa.

O arquivo de log legível por máquina (MRL) contém as saídas binárias do coprocessador, em resposta a vários comandos submetidos ao coprocessador.

As informações detalhadas sobre o conteúdo do MRL estão disponíveis no desenvolvimento do IBM 4764 e do IBM 4765. Entre em contato com a IBM usando a guia de Suporte e downloads no website do produto IBM em *http://www.ibm.com/security/cryptocards*.

Códigos de Erro do Driver de Dispositivo

O driver de dispositivo do coprocessador monitora o status da comunicação com o coprocessador e com os registros de status de hardware do coprocessador.

Cada vez que o processador for reconfigurado e a reconfiguração não for causada por um evento de falha ou de violação, o coprocessador será executado através de uma mini-inicialização, seu autoteste inicial (POST), o carregamento de código e as rotinas de status. Durante esse processo, o coprocessador tenta coordenar-se com um driver de dispositivo do sistema host. As operações de reconfiguração do coprocessador podem ocorrer por causa da inicialização, de um comando **reset**, enviado do driver de dispositivo ou por causa da atividade interna do coprocessador, como a conclusão das atualizações de códigos.

A falha do coprocessador ou um conjunto de circuitos de detecção de violação também podem reconfigurar o coprocessador.

Programas como o Coprocessor Load Utility (CLU) e o CCA Support Program podem receber um status incomum no formato de um código de retorno de 4 bytes a partir do driver de dispositivo.

Os possíveis códigos de 4 bytes, são da forma X'8xxxxxx'. Os códigos que são obtidos frequentemente são descritos no Tabela 7. Se você encontrar códigos da forma XX'8340xxxx' ou X'8440xxxx' e o código não estiver na tabela, contate a equipe criptográfica da IBM por meio do e-mail da página de Suporte no website do produto IBM em *http://www.ibm.com/security/cryptocards*.

Tabela 7. Códigos de erros do driver da classe de dispositivo na classe X'8xxxxxxx'

4 bytes código de retorno (hex)	**Razão**	**Descrições**
8040FFBF	Intrusão externa	A intrusão suscita devido a conexão elétrica opcional com o coprocessador. Essa condição pode ser reconfigurada.
8040FFDA	Bateria inativa	As baterias foram descarregadas ou removidas. O coprocessador foi zerado e não está mais funcional.
8040FFDB	Violação de raio X ou sem bateria	O coprocessador foi zerado e não está mais funcional.
8040FFDF	Raio X ou sem bateria	O coprocessador foi zerado e não está mais funcional.
8040FFEB	Violação de temperatura	O limite de temperatura alta ou baixa foi excedido. O coprocessador foi zerado e não está mais funcional.
8040FFF3	Violação de voltagem	O coprocessador foi zerado e não está mais funcional.
V8040FFF9	Violação de Rede Mesh	O coprocessador foi zerado e não está mais funcional.
8040FFFB	Reconfigurar bit está ativado	Uma baixa voltagem foi detectada, a temperatura da operação interna do coprocessador ficou fora dos limites ou o driver do host enviou um comando de reconfiguração. Tente remover e reinserir o coprocessador no barramento PCI-X.
8040FFFE	Aviso de bateria	A energia da bateria é marginal. Para o procedimento a ser seguido para colocar as baterias, consulte o *IBM 4764 PCI-X Cryptographic Coprocessor Installation Manual*.
804xxxxx (por exemplo, **80400005)**	Problema de comunicação geral	Exceto para os códigos X'8040xxxx' anteriores, as condições adicionais suscitaram na comunicação do coprocessador do host. Determine que o sistema host de fato possua um coprocessador. Tente remover e reinserir o coprocessador no barramento PCI-X. Execute o comando de status do CLU (ST). Se o problema persistir, entre em contato com Contatar a Equipe Criptográfica da IBM por meio do e-mail da Página de Suporte no Web Site do Produto IBM em *http://www.ibm.com/security/cryptocards*.
8340xxxx	Códigos de Miniboot 0	Essa classe de código de retorno surge a partir do nível mais baixo do teste de reconfiguração. Se ocorrerem códigos nesta classe, contate a equipe criptográfica da IBM por meio do e-mail da página de Suporte no website do produto IBM em *http://www.ibm.com/security/cryptocards*.
8340038F	Falha de geração de número aleatório	O monitoramento contínuo do gerador de número aleatório detectou um possível problema. Há uma pequena probabilidade estatística de que esse evento está ocorrendo sem indicar um problema contínuo real. Execute o comando (ST) do status do CLU pelo menos duas vezes para determinar se a condição pode ser limpa.
8440xxxx	Códigos de Miniboot 1	Essa classe de código de retorno surge a partir do código POST e de carregamento de código substituíveis.
844006B2	Assinatura inválida	A assinatura no envio de dados do utilitário CLU para a mini-inicialização não pôde ser validada pela mini-inicialização. Certifique-se de estar usando um arquivo apropriado (por exemplo, **CR1**xxxxx.clu versus **CE1**xxxxx.clu). Se o problema persistir, obtenha a saída de um relatório de status do CLU e encaminhe o relatório com uma descrição da tarefa que deseja atingir para a equipe criptográfica da IBM por meio do e-mail da página de Suporte no website do produto IBM em *http://www.ibm.com/security/cryptocards*.

Clonando uma chave mestra

Esta seção fornece instruções para Clonagem de uma Chave Mestra e fornece considerações sobre controle de acesso durante a clonagem.

Visão geral de clonagem de uma chave mestra

O procedimento de clonagem descreve como clonar uma chave mestra de um coprocessador para outro coprocessador usando o utilitário Cryptographic Node Management (CNM).

Nota: Assegure-se de que o utilitário CNM esteja no mesmo nível em todos os sistemas envolvidos no procedimento de clonagem.

O procedimento de clonagem da chave mestra não faz nenhuma suposição sobre qual servidor contém os coprocessadores usados para:

- Share Administration (**nó SA**)
- Origem da chave mestra (nó Coprocessor Share-Signing **CSS**)
- Destino da chave mestra (nó Coprocessor Share-Receiving **CSR**)

Nota: A clonagem das chaves principais do AES não é suportada.

A chave do SA pode residir no mesmo coprocessador do CSS ou da chave CSR, ou pode residir em um nó de coprocessador separado. Qualquer um dos coprocessadores poderá residir juntos no mesmo servidor, se diversos coprocessadores com CCA estiverem disponíveis.

O procedimento ignora as ações do operador para efetuar logon e logoff, porque essas etapas dependem das funções específicas em uso na instalação. É possível alternar entre coprocessadores, quando você estiver usando mais de um coprocessador em um servidor.

O procedimento é dividido em várias fases, como descrito em Tabela 8.

Tabela 8. Visão Geral da Fase do Procedimento de Clonagem de Chave Mestra

Fase	Nó	Tarefa
1	SA	Estabelecer o nó Share Administration. Crie o banco de dados AS, gere a chave SA e armazene sua chave pública e o hash dentro do banco de dados AS.
2a	Origem	Estabelecer o nó de origem. Gere a chave CSS e inclua a chave pública no banco de dados AS. Instale a chave pública SA.
2b	SA	Certifique a chave CSS e armazene o certificado no banco de dados SA.
Para cada nó de destino, repita os procedimentos de 3 fases.		
3a	Destino	Estabelecer o nó de destino. Crie um banco de dados CSR, gere uma chave CSR e inclua a chave pública no banco de dados CSR para este nó. Instale a chave pública SA.
3b	SA	Certifique a chave CSR e armazene o certificado no banco de dados CSR para o nó de destino.
3c	Origem	Obtenha os compartilhamentos e as informações de verificação da chave mestra atual.
3d	Destino	Instale os compartilhamentos e confirme a nova chave mestra. Configure a chave mestra.

Antes de iniciar o procedimento de clonagem da chave mestra, é sugerido que você preencha os formulários localizados na tabela Tabela 9 na página 48 e na Figura Figura 8 na página 49.

Tabela 9. Clonando responsabilidades, perfis e funções

Tarefa	Nó	Perfil	Função	Indivíduo responsável
Auditar controles de acesso	SA			
Gerar chave SA	SA			
Registrar hash de chave SA	SA			
Registrar chave SA	SA			
Auditar controles de acesso	CSS			
Gerar chave CSS	CSS			
Obter a chave mestra CSS	CSS			
Registrar hash de chave SA	CSS			
Registrar chave SA	CSS			
Certificar chave CSS	SA			
Auditar controles de acesso	CSR1			
Gerar chave CSR	CSR1			
Registrar hash de chave SA	CSR1			
Registrar chave SA	CSR1			
Certificar chave CSR1	SA			
Obter compartilhamentos	CSS			
Instalar compartilhamentos	CSR1			
Verificar novo CSR	CSR1			
Configure a chave mestra CSR	CSR1			
Auditar controles de acesso	CSR2			
Gerar chave CSR	CSR2			
Registrar hash de chave SA	CSR2			
Registrar chave SA	CSR2			
Certificar chave CSR2	SA			
Obter compartilhamentos	CSS			
Instalar compartilhamentos	CSR2			
Verificar novo CSR	CSR2			
Configure a chave mestra CSR	CSR2			

INFORMAÇÕES DE NÓ	Nó	Máquina	Número do Seletor	Número de Série do Coprocessador	Nome e Caminho do Banco de Dados
	Controle de Nó SA				(sa.db)
	Origem de Nó CSS				(sa.db)
	Destino 1 de Nó CSR				(csr1.db)
	Destino 2 de Nó CSR				(csr2.db)

HASH SA-KEY				

NÚMERO DE COMPARTILHAMENTOS	Mínimo: “m”	Máximo: “n”

DISTRIBUIÇÃO DOS COMPARTILHAMENTOS	Obtido de:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	Instalado no CSR-1:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Obtido de:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Instalado no CSR-2:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Figura 8. Clonando a planilha de informações

Fase 1 para a clonagem de uma chave mestra: Estabelecendo o nó Share Administration

Para usar o coprocessador como o Nó Share Administration (SA), siga as etapas de clonagem da chave mestra mencionada no Tabela 10 na página 50. Este coprocessador também pode servir como o nó de origem da chave principal ou um nó de destino de chave mestra.

Pré-requisito: Antes de executar esse procedimento, familiarize-se com as etapas descritas na seção “Cenário: Clonando uma chave mestra DES ou PKA” na página 21 e o capítulo sobre como compreender e gerenciar chaves mestras no manual *Referência e Guia de Serviços Básicos do IBM CCA para o IBM 4765 PCIe and 4764 PCI-X Cryptographic Coprocessors*.

Para estabelecer o nó SA, execute as etapas na tabela a seguir:

Tabela 10. Clonando o procedimento de chave mestra: Estabelecendo o nó SA

Fase	Tarefa	✓
1.1	Auditar a adequação dos controles de acesso.	
1.2	Executar a sincronização de tempo e assegurar que a autorização (`fcv_td4kECC521.crt`) esteja instalada.	
1.3	Confirmar (ou instalar) a chave mestra.	
1.4	Usando os recursos do sistema operacional, apague qualquer banco de dados SA anterior da mídia de banco de dados SA.	
1.5	Se ainda não estiver estabelecido, insira o Environment ID (EID) executando as etapas a seguir: • Clique em **Nó de Criptografia** >**Configurar Environment ID**. • Insira o EID, clique em **Carregar**.	
1.6	Gerar a chave SA: • Clique em **Nó de Criptografia** >**Administração de Compartilhamento** >**Criar Chaves** >**Chaves de Administração de Compartilhamento**. • Aceite a chave pública SA padrão e os rótulos da chave privada e insira o nome e o local do banco de dados SA (`sa.db`). • Clique em **Criar**. • Registre o valor hash da chave SA para uso posterior no procedimento.	
1.7	Registre o hash da chave pública SA: • Clique em **Nó de Criptografia** >**Administração de Compartilhamento** >**Criar Chaves** >**Chave de Administração de Compartilhamento** >**Registrar Chave de Administração de Compartilhamento** > **Hash da Chave SA**. • Insira o nome e o local do arquivo de banco de dados SA e clique em **Avançar**. • Insira o rótulo da chave pública SA (ou aceite o padrão). • Insira o hash da chave SA e clique em **Registrar**.	
1.8	Registre a chave pública SA: • Clique em **Nó de Criptografia** >**Administração de Compartilhamento** >**Criar Chaves** >**Chave de Administração de Compartilhamento** >**Registrar Chave de Administração de Compartilhamento** > **Hash da Chave SA**. • Insira o nome e o local do arquivo de banco de dados SA e clique em **Avançar**. • Insira o rótulo da chave pública SA (ou aceite o padrão) e clique em Registrar.	

Fase 2 para a clonagem de uma chave mestra: Estabelecendo o nó de origem

Usando o coprocessador designado como o nó de origem da chave mestra, siga as etapas para clonagem da chave mestra mencionada no Tabela 11. Este coprocessador também pode servir como o nó SA.

Tabela 11. Clonando a chave mestra: Estabelecendo nó de origem (CSS)

Fase	Tarefa	✓
2a.1	Auditar a adequação dos controles de acesso.	
2a.2	Executar a sincronização de tempo e assegurar que a autorização `fcv_td4kECC521.crt` esteja instalada.	
2a.3	Confirme o número de série do coprocessador: • Clique em **Nó de Criptografia** >**Status**. • Clique em **Adaptador**. • Observe o número de série do coprocessador e clique em **Cancelar**.	
2a.4	Confirmar (ou instalar) a chave mestra.	
2a.5	Obtenha as informações de verificação da chave mestre atual: • Clique em **Chave Mestra** > **Verificar** > **Atual**. • Clique em **Salvar** para transportar a mídia, clique em **Cancelar**.	

Tabela 11. Clonando a chave mestra: Estabelecendo nó de origem (CSS) (continuação)

Fase	Tarefa	✓
2a.6	Se ainda não estiver estabelecido, insira o Environment ID (EID): • Clique em **Nó de Criptografia** > **Configurar Environment ID**. • Insira o EID, clique em **Carregar**.	
2a.7	Se ainda não estiver estabelecido, configure os valores compartilhados m e n do número: • Clique em **Nó de Criptografia** > **Administração de Compartilhamento** > **Configurar Número de Compartilhamentos**. • Configure o número máximo e mínimo de compartilhamentos necessários e clique em **Carregar**.	
2a.8	Gerar a chave CSS: • Clique em **Nó de Criptografia** > **Administração de Compartilhamento** > **Criar Chaves** > **Chave CSS**. • Insira o rótulo da chave CSS (por exemplo, CSS.KEY). • Confirme o número de série do coprocessador. • Confirme ou insira o nome e o local do banco de dados SA. • Clique em **Criar**.	
2a.9	Registre o hash de chave pública SA: • Clique em **Nó de Criptografia** > **Administração de Compartilhamento** > **Registrar Chaves de Administração de Compartilhamento** > **Hash da Chave SA**. • Insira o nome e o local do arquivo de banco de dados SA e clique em **Avançar**. • Insira o rótulo da chave pública SA (ou aceite o padrão). • Insira o hash da chave SA e clique em **Registrar**.	
2a.10	Registre a chave pública SA: • Clique em **Nó de Criptografia** > **Administração de Compartilhamento** > **Registrar Chaves de Administração de Compartilhamento** > **Chave SA**. • Insira o nome e o local do arquivo de banco de dados SA e clique em **Avançar**. • Insira o rótulo da chave pública SA (ou aceite o padrão) e clique em **Registrar**.	

Fase 3 para a clonagem de uma chave mestra: Estabelecendo o nó de destino e a clonagem de uma chave mestra

Usando os nós designados, estabeleça o nó de destino e clone a chave mestra seguindo as etapas para clonagem da chave mestra mencionada no Tabela 12. Este coprocessador também pode servir como o nó SA.

Tabela 12. Clonando uma chave mestra: Estabelecendo o nó CSR e a clonagem de uma chave mestra

Fase	Nó	Tarefa	✓
No nó de destino			
3a.1	Destino	Auditar a adequação dos controles de acesso.	
3a.2	Destino	Execute a sincronização de tempo e assegure que a autorização `fcv_td2k.crt` esteja instalada.	
3a.3	Destino	Confirme o número de série do coprocessador: • Clique em **Nó de Criptografia** > **Status**. • Clique em **Adaptador**. • Observe o número de série do coprocessador e clique em **Cancelar**.	
3a.4	Destino	Assegurar a existência de uma chave mestra (temporária).	
3a.5	Destino	Se ainda não estiver estabelecido, insira o Environment ID (EID): • Clique em **Nó de Criptografia** > **Configurar Environment ID** > **Nó de Criptografia**. • Insira o EID (por exemplo, CSR1 NODE e extensão com espaços para 16 caracteres inseridos). • Clique em **Carregar**.	

Tabela 12. Clonando uma chave mestra: Estabelecendo o nó CSR e a clonagem de uma chave mestra (continuação)

Fase	Nó	Tarefa	✓
3a.6	Destino	Se ainda não estiver estabelecido, configure os valores de compartilhamentos de número *m* e *n* : • Clique em **Nó de Criptografia** > **Administração de Compartilhamento** > **Configurar Número de Compartilhamentos**. • Configurar número máximo e mínimo de compartilhamentos necessários. • Clique em **Carregar**.	
3a.7	Destino	Ao usar os recursos do sistema operacional, apague o arquivo de dados `csr.db`.	
3a.8	Destino	Gerar a chave CSR: • Clique em **Nó de Criptografia** > **Administração de Compartilhamento** > **Criar Chaves** > **Chave CSR**. • Insira o rótulo da chave CSR (por exemplo, CSR1.KEY). • Confirme o número de série do coprocessador. • Selecione o tamanho da chave. • Forneça o nome e o local do banco de dados CSR (por exemplo, CSR1.DB). • Clique em **Criar**.	
3a.9	Destino	Registre o hash de chave pública SA: • Clique em **Nó de Criptografia** > **Administração de Compartilhamento** > **Registrar Administração de Compartilhamento** > **Hash da Chave SA**. • Insira o nome e o local do arquivo de banco de dados SA e clique em **Avançar**. • Insira o rótulo da chave pública SA (ou aceite o padrão). • Insira o hash da chave SA e clique em **Registrar**.	
3a.10	Destino	Registre a chave pública SA: • Clique em **Nó de Criptografia** > **Administração de Compartilhamento** > **Registrar Administração de Compartilhamento** > **Chave SA**. • Insira o nome e o local do arquivo de banco de dados SA e clique em **Avançar**. • Insira o rótulo da chave pública SA (ou aceite o padrão) e clique em **Registrar**.	
No nó SA			
3b.1	SA	Certifique a chave CSS (conforme necessário): • Clique em **Nó de Criptografia** > **Administração de Compartilhamento** > **Certificar Chaves** > **Chave CSS**. • Insira o nome e o caminho para o banco de dados SA e clique em **Avançar**. • Confirme o rótulo da chave CSS, o número de série do coprocessador e o ID do ambiente do Administrador do Sistema. • Clique em **Certificar**.	
3b.2	SA	Certificar a chave CSR: • Clique em **Nó de Criptografia** > **Administração de Compartilhamento** > **Certificar Chaves** > **Chave CSS**. • Insira o nome e o caminho para os bancos de dados SA e CSR e clique em **Avançar**. • Confirme o rótulo da chave SA, o rótulo da chave CSR e o ID do ambiente do Administrador do Sistema. • Insira o número de série do CSR. • Clique em **Certificar**.	
No nó de origem			

Tabela 12. Clonando uma chave mestra: Estabelecendo o nó CSR e a clonagem de uma chave mestra (continuação)

Fase	Nó	Tarefa	✓
3c.1	Origem	Obtenha pelo menos o número de compartilhamentos m e n. Execute a subetapa a seguir para cada compartilhamento. Note que o logon e logoff podem ser necessários para obter cada compartilhamento. • Clique em **Nó de Criptografia** > **Administração de Compartilhamento** > **Obter Compartilhamento**. • Selecione o compartilhamento. Observe que se você estiver obtendo um ou mais conjuntos de compartilhamentos adicionais, as Mensagens distribuídas poderão não ser significativas. • Insira o nome e o caminho para os bancos de dados SA e CSR e clique em **Avançar**. • Confirme o rótulo da chave CSS, o número de série do coprocessador CSS e o número de série do coprocessador CSR. • Clique em **Obter Compartilhamento**. Repita conforme necessário.	
No nó de destino			
3d.1	Destino	Instale o número de compartilhamentos m e n. Execute o seguinte para cada compartilhamento e observe a resposta. A resposta indica quando compartilhamentos suficientes foram instalados para formar a nova chave mestre. Note que o logon e logoff podem ser necessários para instalar cada compartilhamento. • Clique em **Nó de Criptografia** > **Administração de Compartilhamento** > **Carregar Compartilhamento**. • Selecione o compartilhamento. • Insira o nome e o caminho para os bancos de dados CSR e SA, clique em **Avançar**. • Confirme o rótulo da chave CSS, o número de série do coprocessador CSS e o número de série do coprocessador CSR. • Clique em **Carregar Compartilhamento**. Observe a resposta. Carregar compartilhamentos suficientes completa a nova chave mestra. Repita conforme necessário.	
3d.2	Destino	Confirmar a nova chave mestra: • Clique em **Chave Mestra** > **Verificar** > **Novo**. • Clique em **Comparar** ou **Selecionar o Arquivo**, ou clique em **OK** ou clique em **Cancelar**	
3d.3	Destino	Apague o arquivo de dados `csr.db`. Isso não é um problema de segurança; é somente para evitar complicações durante a operação de cópia da chave mestra.	
3d.4	Destino	Configure a chave mestra, conforme apropriado: • Clique em **Chave Mestra** > **Configurar**. • Clique em **OK**.	

Considerações sobre o controle de acesso na clonagem

Há três classes de funções a serem consideradas para operações de clonagem.

- Funções no nó share administration (SA).
- Funções no nó de origem: assinatura do nó coprocessor share signin (CSS)
- Funções no nó de destino: assinatura do nó coprocessor share signin (CSS)

A política de segurança deve definir quem terá a autoridade para:

- Gerar uma chave mestra aleatória no nó de origem.

- Configure a chave mestra, a ação que traz uma nova chave mestra na operação. Quando a chave mestra for alterada, as chaves criptografadas pela chave mestra deverão ser atualizadas.
- Gerar as chaves retidas Rivest-Shamir-Adleman (RSA) para certificar as chaves públicas dos nós de origem e de destino (a chave SA) e para gerar as chaves retidas nos nós de origem (CSS) e de destino (CSR).
- Registrar a chave SA e seu hash e determinar se ela será uma responsabilidade dividida.

Além disso, deve-se decidir como quantos nós devem cooperar para clonar uma chave mestra. É claro, este deve ser selecionado para evitar atos de má fé.

Ao decidir os valores m e n, considere o momento em que a clonagem ocorrerá e se é necessário reconstituir a chave mestra em um número menor de compartilhamentos do que o número total obtido do nó de origem (talvez por causa da distorção de compartilhamento ou da indisponibilidade de uma ou mais pessoas que podem obter ou instalar um compartilhamento).

Nota: O utilitário Cryptographic Node Management (CNM) coloca todos os compartilhamentos de um nó no arquivo `csr.db`. Cada compartilhamento é criptografado em uma chave Data Encryption Standard (DES) padrão de criptografia de dados de comprimento triplo e exclusiva, em que ele próprio é criptografado pela chave pública CSR do nó de destino.

O Tabela 13 fornece a orientação para selecionar as permissões aplicáveis às funções que são relacionadas à clonagem.

Tabela 13. Comandos CCA relacionados à clonagem de chave mestra

Cód.	Nome do comando	Nome do verbo	Consideração
X'001A'	Configurar Chave Mestra	**Master_Key_Process**	Crítico. Essa função deve ter conhecimento do conteúdo do novo registro de chave mestre e das implicações de uma mudança de chave mestra.
X'001D'	Padrão de Verificação de Computador	**Muitos**	Todos
X'0020'	Gerar Chave Mestra Aleatória	**Master_Key_Process**	Não crítico, exceto que preenche o novo registro de chave mestre.
X'0032'	Limpar Registro da Nova Chave Mestra	**Master_Key_Process**	Esta função é designada à função que pode configurar a chave mestra. A função pode substituir os compartilhamentos coletados. Ela deve ser mutuamente exclusiva com o comando Generate Random Master Key.
X'0033'	Limpar Registro da Chave Mestra Antiga	**Master_Key_Process**	Geralmente não usado.
X'008E'	Gerar Chave	**Key_Generate** **Random_Number_Generate**	Todos
X'0090'	Recriptografar Chave Mestra Atual	**Key_Token_Change**	Esta função depende de quem atualizará as chaves de trabalho criptografadas pela chave mestra.
X'0100'	Gerar Assinatura Digital PKA96	**Digital_Signature_Generate**	Esta função certifica as chaves SA, CSS e CSR.
X'0101'	Verificar Assinatura Digital PKA96	**Digital_Signature_Verify**	Todos
X'0102'	Alterar Token de Chave PKA96	**PKA_Key_Token_Change**	Esta função depende de quem atualizará as chaves de trabalho criptografadas pela chave mestra.
X'0103'	Gerar Chave PKA PKA96	**PKA_Key_Generate**	Esta função é necessária para gerar as chaves SA, CSS e CSR.
X'0107'	Hash Unidirecional, SHA-1	**One_Way_Hash**	Todos

Tabela 13. Comandos CCA relacionados à clonagem de chave mestra (continuação)

Cód.	Nome do comando	Nome do verbo	Consideração
X'0114'	Alterar Dados de Autenticação do Perfil do Usuário.	**Access_Control_Initialization**	Esta função permite alterar a passphrase em qualquer perfil. Use com critério.
X'0116'	Ler Informações de controle de acesso público	**Access_Control_Maintenance**	Todos
X'011C'	Consulte o EID	**Cryptographic_Facility_Control**	Esta função é necessária para configurar os nós CSS e CSR.
X'011D'	Inicializar Clonagem de Chave Mestra	**Cryptographic_Facility_Control**	Esta função é necessária para configurar os valores m e n nos nós CSS e CSR.
X'0200'	Registrar Hash de Chave Pública PKA	**PKA_Public_Key_Hash_Register**	Esta função deve ser usada nos nós CSS e CSR para assegurar que a chave SA possa ser reconhecida. Divida a responsabilidade com X'0201'.
X'0201'	Registro de Chave Pública PKA	**PKA_Public_Key_Register**	Esta função deve ser usada nos nós CSS e CSR para assegurar que a chave SA possa ser reconhecida. Divida a responsabilidade com X'0200'.
X'0203'	Excluir Chave Retida	**Retained_Key_Delete**	Esta função é usada para remover as chaves SA, CSS e CSR obsoletas. Tenha cuidado com a negação de serviço.
X'0204'	Gerar Chave de Clonagem PKA	**PKA_Key_Generate**	Esta função é necessária para gerar as chaves CSS e CSR.
X'0211' - X'021F'	Obter informações do clone (Compartilhamento)	**Master_Key_Distribution**	Esta função designa um perfil e uma função para cada compartilhamento para impingir a responsabilidade dividida.
X'0221' - X'022F'	Instalar informações do clone (Compartilhamento)	**Master_Key_Distribution**	Esta função designa um perfil e uma função para cada compartilhamento para impingir a responsabilidade dividida.
X'0230'	Listar Chave Retida	**Retained_Key_List**	Todos

Considerações de Ameaça para um Servidor de Assinatura Digital

Considere diversas ameaças quando você implementar o IBM 4765 com o IBM Common Cryptographic Architecture (CCA) Support Program em um aplicativo de assinatura digital. A maior parte da discussão aplica-se a outros ambientes nos quais você pode aplicar o coprocessador.

Uma organização que coloca uma autoridade de certificação (CA), uma autoridade de registro (RA), um respondente do Online Certificate Status Protocol (OCSP), ou um serviço de data e hora na operação precisa considerar como sua instalação irá tratar várias ameaças. O Tabela 14 na página 56 lista potenciais ameaças e apresenta soluções de design e de implementação do produto para muitas dessas ameaças. As notas descrevem as etapas necessárias a considerar para atenuar sua exposição aos problemas.

Consulte o manual de Referência e Guia de Serviços Básicos do IBM CCA para o *IBM 4765 PCIe and 4764 PCI-X Cryptographic Coprocessors* , que descreve as ações possíveis de utilizar na implementação do coprocessador, as políticas a serem consideradas, as funções de aplicativo a serem incluídas.

Leia o conteúdo do Tabela 14 na página 56 após tomar as decisões iniciais sobre a instalação.

Tabela 14. Considerações de Ameaça para um Servidor de Assinatura Digital

Discussão da Ameaça	Mitigação da Ameaça
Ameaças associadas ao ataque físico no coprocessador	
Análise Física do Coprocessador Um inimigo pode executar uma análise física do coprocessador para revelar informações de design e conteúdo operacional. Tal análise pode incluir funções elétricas, mas é referida aqui como físicas, porque requer contato direto com as funções internas do coprocessador. A análise física pode implicar a leitura de dadosdo coprocessador por meio de técnicas comumente implementadas na análise de falhas de IC e nos esforços da engenharia reversa de IC. O objetivo do adversário é identificar tais detalhes de design como mecanismos de segurança de hardware, mecanismos de controle de acesso, sistemas de autenticação, sistemas de proteção, particionamento de memória ou programas de criptografia. A determinação do design do software, incluindo dados de inicialização, senhas, PINs ou chaves criptográficas, também pode ser um objetivo.	Os eletroeletrônicos do coprocessador incorporam um conjunto sofisticado de sensores de detecção de violação e mecanismos de respostas. Sensores de temperatura alta e baixa, de níveis de voltagem e de sequenciamento, de radiação e de penetração física são designados a detectarem situações ambientais incomuns. Todos os componentes eletrônicos são incluídos em um pacote blindado fisicamente. Ao detectar um evento de violação potencial, o coprocessador limpa imediatamente toda a memória RAM interna, que também zera as chaves usadas para recuperar os dados sensíveis e persistentes da memória flash. Um controlador de estado independente também é reconfigurado, o que indica que o coprocessador não está mais em uma condição de certificado da factory. Os vários sensores de violação são ativados no tempo de fabricação do coprocessador até o final da vida do coprocessador. O coprocessador assina digitalmente uma resposta de consulta que é possível verificar para confirmar se o coprocessador é genuíno e se não está corrompido. Quase todo o software que é executado no processador principal dentro do coprocessador está disponível na Web e, portanto, está sujeito a realizar engenharia reversa. Entretanto, o coprocessador valida as assinaturas digitais no código que ele é solicitado a aceitar, de modo que o código modificado por um inimigo não possa ser carregado no coprocessador. As chaves públicas usadas para validar o código oferecido são destruídas quando um evento de violação é reconhecido. O design e a implementação são avaliados e certificados de modo independente pelo USA NIST sob o padrão FIPS PUB 140-2 de Nível 4. **Nota:** Você deve validar a condição do coprocessador e o conteúdo do código.
Modificação Física do Coprocessador Um adversário pode modificar fisicamente o coprocessador para revelar as informações relacionadas à segurança ou design. Essa modificação pode ser obtida por meio de técnicas normalmente empregadas nas análises de falha de hardware e nos esforços de engenharia reversa. O objetivo é identificar tais detalhes de design como mecanismos de segurança de hardware, mecanismos de controle de acesso, sistemas de autenticação, sistemas de proteção de dados, particionamento de memória ou programas de criptografia. A determinação do design do software, incluindo dados de inicialização, senhas ou chaves criptográficas, também pode ser um objetivo.	Os componentes eletrônicos são todos incluídos no pacote de resposta à violação montado no coprocessador. No processo de alteração os eletroeletrônicos sensíveis, a certificação da factory do coprocessador seria destruída, renderizando o dispositivo inútil. **Nota:** Confirme se um coprocessador específico com o número de série está em uso e a auditoria da resposta de consulta de status para confirmar se ele permanece um coprocessador inalterado carregado da IBM inalterado com o software apropriado.
Manipulação Ambiental do Coprocessador Um adversário pode usar condições ambientais além daquelas da especificação do coprocessador para obter ou modificar o fluxo de dados ou de programa para uso do coprocessador fraudulento. Essa modificação pode incluir manipulação de linhas de energia, taxas de relógio ou exposição a altas e baixas temperaturas e radiação. Como resultado, o coprocessador pode ser obtido em uma situação em que as instruções não são executadas corretamente. Como resultado, dados críticos de segurança podem ser modificados ou divulgados em contradição com os requisitos de segurança para o coprocessador.	O coprocessador possui sensores para detectar estresses ambientais que podem induzir a operações errôneas. Condições anormais podem causar um zeramento da unidade.

Tabela 14. Considerações de Ameaça para um Servidor de Assinatura Digital (continuação)

Discussão da Ameaça	Mitigação da Ameaça
Processos substituídos Os pedidos e respostas do coprocessador podem ser direcionados a uma implementação alternativa que permite que um inimigo influencie os resultados. Uma implementação alternativa pode ser substituída com recursos de segurança diferentes. Por exemplo, a geração de chave privada e a produção de assinaturas digitais podem ser executadas em uma implementação alternativa que permitiria a exposição da chave privada.	**Comunicados:** 1. Os auditores precisam concluir os processos descritos para assegurarem que a chave de assinatura seja realmente mantida no coprocessador apropriado. 2. O acesso ao sistema host deve ser supervisionado para que as medidas de segurança do sistema host e a operação correta possam ser confiáveis.
Ameaças associadas ao ataque lógico no coprocessador	
Inserção de falhas Um inimigo pode determinar informações críticas de segurança por meio da observação dos resultados da inserção repetitiva dos dados selecionados. A inserção da entrada selecionada seguida pelo monitoramento da entrada para as mudanças é um método de ataque relativamente bem conhecido para os dispositivos criptográficos. A intenção é determinar as informações baseadas em como o coprocessador responde à entrada selecionada. Essa ameaça é diferenciada pela escolha deliberada e repetitiva e pela manipulação de dados de entrada, ao contrário da seleção ou da manipulação aleatória das características físicas envolvidas nas operações de entrada ou saída.	O design eletrônico do coprocessador rende abordagens clássicas para ataques smart card inviáveis. **Nota:** A supervisão do sistema host e o controle de acesso ao sistema, sendo logicamente e fisicamente, são etapas de segurança importantes a serem seguidas por uma organização.
Reconfiguração Forçada Um adversário pode forçar o coprocessador em um estado não seguro por meio do término inadequado das operações selecionadas. A tentativa de gerar um estado não seguro no coprocessador pode ser feita pelo término prematuro de transações ou comunicações entre o coprocessador e o host, pela inserção de função de interrupção ou por uso inadequado de funções de interface.	O coprocessador é designado a sempre executar por meio de sua sequência de ativação inicial no evento de condições de trap ou de reconfiguração. Cada pedido no nível de aplicativo é tratado como uma unidade de trabalho separada e processado a partir de um conjunto único definido de condições iniciais.
Entrada Inválida Um adversário ou um usuário autorizado do coprocessador pode comprometer os recursos de segurança do coprocessador pela introdução de entrada inválida. A entrada inválida pode levar a forma de operações que não são formadas corretamente, solicitações para obter informações além dos limites de registro ou tentativas de localizar e executar comandos não documentados. O resultado de como um ataque pode ser um comprometimento nas funções de segurança, uma geração de erros exploráveis na operação ou a liberação de dados protegidos.	Os pedidos de transação transportam informações de autenticação aplicadas no domínio do responsável pela chamada e validadas pelo coprocessador. Cada pedido é processado a partir de um estado único e conhecido com condições predefinidas. O software do coprocessador valida as características de cada pedido para endereçar cenários mau usados.
Mau Funcionamento de Carregamento dos Dados Um inimigo pode gerar maliciosamente erros nos dados de configuração para comprometer as funções de segurança do coprocessador. Durante os estágios de preparação do coprocessador, que envolvem o carregamento do coprocessador com chaves especiais, a identificação de funções e assim por diante, os próprios dados podem ser alterados das informações desejadas ou podem ser corrompidos. Um evento pode ser uma tentativa de introduzir as funções de segurança do coprocessador ou expor a segurança de maneira não autorizada.	**Nota:** Conforme descrito nos procedimentos do auditor, a configuração de controle de acesso deve ser verificada junto com a confirmação do software do coprocessador instalado.

Tabela 14. Considerações de Ameaça para um Servidor de Assinatura Digital (continuação)

Discussão da Ameaça	**Mitigação da Ameaça**
Carregamento de Programa Não Autorizado Um adversário pode usar programas não autorizados para penetrar ou modificar as funções de segurança do coprocessador. Os programas não autorizados podem incluir a execução de programas legítimos não intencionados para uso durante uma operação normal ou o carregamento não autorizado de programas especificamente destinados à introdução ou à modificação das funções de segurança.	O coprocessador aceita somente o software assinado digitalmente, após a assinatura ter sido validada. Uma avaliação independente de construção de software da IBM e de procedimentos de assinatura e o design do coprocessador afirma a confiança que pode ser colocada na identidade do software carregado. **Nota:** Um auditor deve seguir os procedimentos para afirmar que o software especificado está em uso.
Ameaças associadas ao controle de acesso	
Acesso Inválido Um usuário ou um inimigo do coprocessador pode acessar informações ou serviços sem precisar de permissão, conforme definido no perfil da função. Cada função possui privilégios definidos que permitem acesso somente a serviços selecionados do coprocessador. O acesso além dos serviços especificados podem resultar na exposição de informações seguras.	Um auditor pode confirmar as permissões concedidas em cada função estabelecida e o conjunto de perfis do usuário associado a cada função. Uma avaliação independente da implementação e de teste do software do coprocessador revisou a integridade da implementação do controle de acesso.
Fraude no primeiro uso Um adversário pode obter acesso às informações do coprocessador pelo uso não autorizado de um novo coprocessador ainda não instalado. Um adversário pode tentar obter acesso a um coprocessador durante ou imediatamente após o processo de manufatura e carregar o software fraudulento no coprocessador ou modificar os dados críticos armazenados dentro do coprocessador durante o processo de manufatura e de inicialização da factory antes que ele seja enviado ao cliente.	A prática de manufatura e distribuição da IBM assegura que, antes de certificar a factory, o usuário final de um coprocessador é desconhecido e não designado. O software instalado pela factory é validado por meio da verificação de assinaturas digitais. **Comunicados:** 1. Trazer o processo de instalação padrão substitui todo o software do coprocessador no tempo de execução. 2. Deve-se assegurar que os Segmentos 2 e 3 estejam sem proprietários antes de carregar o software do coprocessador para a produção. Esta ação assegura que nenhum dado residual permaneça para influenciar as operações subsequentes.
Personificação Um inimigo pode obter acesso às informações ou serviços do coprocessador ao personificar um usuário autorizado do coprocessador. O coprocessador é necessário para definir determinadas funções, que incluem o mecanismo de autenticação necessário, e os serviços que a função pode usar. Um adversário pode tentar personificar um usuário autorizado, operando dentro de um definido, para obter acesso às informações ou executar serviços permitidos para o usuário autorizado.	As duas classes de usuário estão a seguir: 1. Assinante do código do Coprocessador da (IBM): Uma avaliação independente do procedimento da IBM para o código de construção e de assinatura assegura que o código legítimo possa ser identificado por um auditor do usuário. 2. A designação de controle de acesso da CCA protege a integridade e a confidencialidade de um passphrase de controle de acesso do usuário, a partir do domínio do processo do usuário no coprocessador. A identificação correta de passphrase e de perfil concede o uso de uma função. **Nota:** A segurança do sistema host, o design do aplicativo de sistema host e as políticas administrativas são necessários para assegurar que a passphrase do usuário designado seja seguro.
Ameaças associadas à interações não antecipadas	

Tabela 14. Considerações de Ameaça para um Servidor de Assinatura Digital (continuação)

Discussão da Ameaça	Mitigação da Ameaça
Uso de Funções do Aplicativo Desaprovadas Um inimigo pode explorar interações entre os aplicativos para expor dados sensíveis do coprocessador ou do usuário. As interações podem incluir a execução de comandos que não são necessários ou permitidos no aplicativo específico que está sendo executado. Os exemplos incluem o uso de funções relacionadas ao gerenciamento de chave mestra ou às funções relacionadas aos serviços simétricos de criptografia ou financeiros. Essas funções não devem causar nenhum impacto negativo às funções do coprocessador necessárias para o aplicativo de assinatura digital.	O design do coprocessador requer a configuração do controle de acesso. O software CCA foi examinado para assegurar que as funções sejam desaprovadas quando comandos necessários não forem ativados. **Comunicados:** 1. A configuração de controle de acesso deve seguir os princípios discutidos no Apêndice H da publicação de Redbooks de Referência e Guia de Serviços Básicos do *IBM CCA para o IBM 4765 PCIe and 4764 PCI-X Cryptographic Coprocessors*, de modo que somente as funções necessárias para a fase operacional possam ser chamadas nesta fase. 2. Para o aplicativo de assinatura digital, estabeleça diretrizes para um conjunto de funções com capacidades muito limitadas e uma sequência de configuração que restrinja a funcionalidade do coprocessador, que é essencial para assinatura digital. Em algumas instalações, pode ser desejável acomodar uma abordagem diferente para funções ou considerar as funções de aplicativos adicionais, ou ambos. Nesses casos, assegure-se de revisar as orientações e as observações no Apêndice H da publicação de Redbooks de Referência e Guia de Serviços Básicos do *IBM CCA para o IBM 4765 PCIe and 4764 PCI-X Cryptographic Coprocessors* obter aplicabilidade para suas circunstâncias.
Ameaças referentes às funções de criptografia	
Ataque criptográfico Um inimigo pode derrubar as funções de segurança por meio de um ataque criptográfico contra o algoritmo ou por meio de um ataque de força bruta. Esse ataque pode incluir também as funções de geração e de verificação de assinatura ou geradores de número aleatório.	O coprocessador implementa as funções criptográficas padronizadas e bem estabelecidas. A implementação de geração de número aleatório estava sujeita à avaliação extensiva sob os critérios publicados pela USA NIST e pela German Information Security Agency (German Bundesamt fur f³r Sicherhert in der Informations Technik ou German BSI). O sigilo oferecido às chaves privadas retidas é o assunto de uma avaliação independente. Essas etapas de design e de implementação fornecem garantia contra ataques criptográficos. **Nota:** Para um servidor de assinatura digital, consulte as diretrizes no Apêndice H da publicação de Redbook de Referência e Guia de Serviços Básicos do *IBM CCA para o IBM 4765 PCIe and 4764 PCI-X Cryptographic Coprocessors*.
Ameaças referentes às assinaturas digitais	
Falsificando Dados Assinados Um inimigo pode modificar os dados assinados digitalmente pelo coprocessador de modo que essa modificação não seja detectada pelo assinante e nem por um terceiro. Esse ataque pode usar a fragilidade da função hash segura, a fragilidade na codificação de assinatura ou a fragilidade no algoritmo criptográfico usado para gerar uma assinatura falsificada.	O coprocessador implementa as funções criptográficas padronizadas e bem estabelecidas. **Comunicados:** 1. Precauções no uso do CCA devem ser observadas conforme documentado no Apêndice H da publicação de Redbook de Referência e Guia de Serviços Básicos do *IBM CCA para o IBM 4765 PCIe and 4764 PCI-X Cryptographic Coprocessors*. 2. Os usuários devem manter um reconhecimento das vulnerabilidades discutidas nos fóruns (abertos) sobre o fortalecimento dos algoritmos e processos de criptográficos empregados.
Falsificando dados antes de serem assinados Um inimigo pode modificar os dados para serem assinados digitalmente pelo coprocessador antes que a assinatura seja gerada no coprocessador. Esse ataque pode usar a fragilidade da implementação que permite que um inimigo modifique os dados transmitidos da assinatura para o coprocessador antes que o coprocessador calcule efetivamente a assinatura.	As solicitações de memória de processo do aplicativo host executa um valor de verificação de integridade que o coprocessador confirma antes de incorporar o hash em uma assinatura digital. **Nota:** Os usuários devem revisar a segurança do programa do sistema host e do aplicativo host para assegurar que os valores hash autenticados recebidos no coprocessador não sejam comprometidos e que representem os dados a serem protegidos.

Tabela 14. Considerações de Ameaça para um Servidor de Assinatura Digital (continuação)

Discussão da Ameaça	Mitigação da Ameaça
Mau uso da função de assinatura Um inimigo pode fazer mau uso da função de criação de assinatura do coprocessador para assinar os dados que o coprocessador não deveria assinar. O adversário pode tentar enviar os dados para o coprocessador e obtê-los assinados sem passar pelas verificações de autorização do coprocessador, que são executadas antes de gerar uma assinatura digital. Como alternativa, um inimigo pode tentar modificar os dados no coprocessador por meio do uso de funções do coprocessador ou ao tentar influenciar o coprocessador de modo que os dados nele sejam modificados.	Uma revisão independente do software do coprocessador é esperada para afirmar que: • O serviço de geração de assinatura digital requer uma permissão apropriada em uma função. • O processamento de solicitações e a integridade do design impedem a mudança de dados. **Comunicados:** 1. A integridade do coprocessador e seu código devem ser afirmados por um auditor que revisa uma consulta de status do coprocessador. 2. Um auditor deve confirmar que as funções de controle de acesso e os perfis apropriados tenham sido estabelecidos e excluir os usuários não autorizados de usarem a função assinatura digital.
Falsificando função de verificação de assinatura Um inimigo pode modificar a função para verificação de assinatura, de modo que uma assinatura falsa seja aceita como válida. Esse ataque pode tentar modificar a função de verificação de assinatura ou os dados assinados a serem verificados, para que o coprocessador retorne uma mensagem de êxito quando essa assinatura falsa for apresentada para verificação.	Aqui a assinatura de verificação de função de interesse primário ocorre no processo de carregamento de código do coprocessador (em Mini-inicialização). Com esse produto: • O código de miniboot, como o programa de controle e o código do programa do aplicativo (CCA)é aceito apenas no coprocessador quando o coprocessador valida a assinatura no código assinado. • O código inicial de Mini-inicialização carregado no factory também está sujeito à verificação da assinatura digital. • Os processos criptográficos padronizados são usados (SHA-1, RSA, ISO 9796) para assinatura. • A construção de código e o processo de assinatura são o sujeito de uma revisão independente.
Divulgação de uma chave privada de assinatura RSA Um adversário pode usar as funções que divulga uma chave de assinatura RSA privada.	Uma avaliação independente é esperada para afirmar quer o CCA Support Program não contém nenhuma função para gerar ou revelar o valor de uma chave privada retida. Espera-se que as avaliações certificadas demonstrem que o programa de controle não gere os dados retidos no armazenamento persistente do coprocessador e nem haja nenhuma função de nível inferior para ler tal armazenamento.
Excluindo uma chave de assinatura privada RSA Um inimigo pode usar uma função que exclui uma chave de assinatura RSA privada sem estar autorizado para tal e sem violar fisicamente o coprocessador.	Espera-se que as avaliações independentes afirmem que uma chave privada retida é excluída somente nas circunstâncias a seguir: 1. No controle do CCA com o verbo Retained_Key_Delete 2. Ao carregar o software* CCA do coprocessador 3. Ao remover o software CCA do coprocessador 4. Ao causar um evento de violação **Comunicados:** Para abordar estas exposições, execute estas ações: 1. Ative seletivamente o comando Delete Retained Key, X'0203'. 2. Utilize os controles de acesso do sistema host para gerenciar a utilização do CLU. 3. Gerencie o acesso físico para o coprocessador. * O recarregamento do software do coprocessador com um arquivo como CEXxxxxx.clu não zera o conteúdo de armazenamento persistente. O arquivo CNWxxxxx.clu zerará o armazenamento persistente. Consulte o “Carregando e descarregando o software no coprocessador” na página 7.
Ameaças que monitoram as informações	

Tabela 14. Considerações de Ameaça para um Servidor de Assinatura Digital (continuação)

Discussão da Ameaça	**Mitigação da Ameaça**
Vazamento de informações Um adversário pode fazer uso de informações que são vazadas do coprocessador durante o uso normal. O vazamento de informações pode ocorrer por meio de emanações, variações no consumo de energia, características de E/S, frequência do clock ou por mudanças nos requisitos de tempo de processamento. Esse vazamento pode ser interpretado como um canal de transmissão secreto, mas está mais relacionado à uma medida dos parâmetros operacionais, que podem ser derivados de medidas diretas (contato) ou de medidas de emanações podendo, então, serem relacionadas à uma operação específica sendo executada.	Os meios práticos para interpretar o vazamento de informações estão sujeitos a uma pesquisa contínua em laboratórios comerciais e governamentais. Uma defesa mais aprofundada deve incluir limite de acesso ao ambiente criptográfico e restrições sobre o uso de equipamento especializado no e próximo ao ambiente criptográfico.
Ligação de Várias Observações Um inimigo pode observar o uso de vários recursos ou serviços e, ao vincular essas observações, pode deduzir informações que revelariam dados críticos de segurança. A combinação das observações durante um período de vários usos do coprocessador, ou a integração de conhecimento obtida da observação de operações diferentes, pode revelar informações que permitem que um inimigo saiba informações diretamente ou formule um ataque que possa revelar mais informações que o coprocessador precisa para manter em segredo.	**Comunicados:** 1. O uso do equipamento criptográfico deve ser controlado, incluindo as diretrizes a seguir no Apêndice H da publicação do Redbook de Referência e Guia de Serviços Básicos do *IBM IBM 4765 PCIe and 4764 PCI-X Cryptographic Coprocessors*. 2. Um inimigo pode ter acesso normal aos dados assinados e assinaturas, de modo que os controles devem ser ativados para limitar a possibilidade de um usuário ao enviar pedidos de assinatura arbitrários. 3. O uso dos procedimentos criptográficos padronizados e o monitoramento do entendimento da comunidade criptográfica das vulnerabilidade desses processos (SHA-1, RSA, ISO 9796, X9.31, HMAC e DES triplo) podem fornecer garantia de operação segura.
Ameaças Variadas	
Ataques Vinculados Um adversário pode executar ataques sucessivos, o que resulta em tornar o coprocessador instável ou degradar alguns aspectos das funções de segurança. Um seguinte ataque pode então ser executado com sucesso. Monitoramento de saídas enquanto manipula entradas na presença de stress ambiental em um exemplo de um ataque vinculado.	**Comunicados:** 1. O uso do sistema criptográfico deve ser limitado às situações autorizadas impingidas pelos controles de acesso do coprocessador e pelo uso dos controles do sistema host. 2. Os controles do sistema host e as políticas organizacionais devem restringir o acesso ao sistema para monitoramento e envio de pedidos arbitrários.
Ataque Repetitivo Um inimigo pode usar tentativas repetitivas e não detectadas na penetração para expor o conteúdo de memória ou para alterar os elementos críticos de segurança no coprocessador. As tentativas repetitivas relacionadas a algum ou todas as outras ameaças discutidas arqui podem ser usadas para desenvolver interativamente uma penetração efetiva na segurança do coprocessador. Em todos os casos, se esses ataques puderem permanecer indetectados, não haverá nenhum aviso de vulnerabilidade aumentada.	**Nota:** O uso do sistema criptográfico deve ser limitado às situações autorizadas impingidas pelos controles de acesso do coprocessador e pelo uso dos controles do sistema host. Os controles do sistema host e as políticas organizacionais devem restringir o acesso ao sistema para o monitoramento e o envio de pedidos arbitrários.
Clonagem Um inimigo pode clonar parte de ou todo um processador funcional para desenvolver mais ataques. As informações necessárias para clonar uma parte ou todo um coprocessador podem derivar de uma inspeção detalhada do próprio coprocessador ou da apropriação ilícita de informações de design.	**Nota:** Os auditores devem confirmar que a chave de assinatura digital, o código apropriado e o regime de controle de acesso sejam residentes no coprocessador autorizado.
Ameaças endereçadas pelo ambiente operacional	

Tabela 14. Considerações de Ameaça para um Servidor de Assinatura Digital (continuação)

Discussão da Ameaça	Mitigação da Ameaça
Modificação e reutilização do coprocessador Um inimigo pode usar um coprocessador diferente para disfarçar-se como sendo um coprocessador original, de modo que os recursos de informações possam ser acessados de forma fraudulenta. A remoção, modificação ou reinserção desse coprocessador em um sistema host pode ser usado para transmitir tal combinação como um original. Isso pode, então, ser usado para acessar ou alterar as chaves de assinatura privada ou outras informações críticas de segurança a serem protegidas.	**Comunicados:** 1. Um auditor deve confirmar, por meio de exame de uma resposta de consulta assinada pelo coprocessador, que o dispositivo é genuíno e que um código apropriado foi carregado. 2. O auditor também deve confirmar que a chave de assinatura digital é uma chave retida no coprocessador.
Abuso pelos usuários privilegiados Um administrador descuidado, voluntariamente negligente ou hostil ou outro usuário privilegiado pode criar um comprometimento nos ativos do coprocessador pela execução de ações que expõem as funções de segurança ou os dados protegidos. Um usuário ou um administrador privilegiado pode implementar ou facilitar diretamente ataques baseados em qualquer uma dessas ameaças descritas aqui.	**Nota:** Uma organização deve estabelecer, impingir e auditar as políticas que limitam o acesso que uma única pessoa possui ao sistema criptográfico. O procedimento de configuração deve assegurar que um único usuário não tenha a oportunidade de colocar um sistema impróprio em produção.
Modificação de Dados Os dados a serem designados pelo coprocessador podem ser modificados por um inimigo ou por falhas no ambiente operacional depois que eles forem aprovados pelo usuário legítimo e antes que eles sejam enviados para o coprocessador para serem assinados. Os dados que foram aprovados pelo usuário legítimo a serem assinados podem ser modificados por um inimigo, por programas falsos ou maliciosos ou por erros ambientais (por exemplo, erros de transmissão), depois que eles forem aprovados pelo usuário legítimo e antes que sejam transferidos para o coprocessador para serem assinados.	**Nota:** As precauções de segurança do sistema host e as políticas da organização devem ser definidas, impingidas e auditadas para impedir tais ataques.
Verificação de Dados Os dados a serem verificados pelo coprocessador podem ser modificados por um inimigo ou por falhas no ambiente operacional antes de serem enviados para o coprocessador para verificação de assinatura, de modo que a resposta do coprocessador não reflita a validade da assinatura. Os dados assinados enviados por um usuário podem ser modificados dentro do ambiente do coprocessador antes de serem transmitidos para o coprocessador para verificação. Isso pode resultar em uma resposta a partir do coprocessador que não reflita a validade real da assinatura digital que deve ser verificada. Também há a possibilidade de que a resposta do coprocessador seja modificada no ambiente do coprocessador antes de ser transmitida para o usuário que solicitou a verificação de assinatura.	O coprocessador verifica a assinatura no código e os comandos de carregamento de código determinados. Uma avaliação independente é esperada para confirmar que isso não pode ser ignorado. O design do CCA suporta a validação da integridade dos pedidos e responde entre o coprocessador e a camada superior do código CCA no sistema host. **Nota:** As medidas de segurança do sistema host devem endereçar o bloqueio da modificação das entradas e saídas do pedido.

Avisos do IBM Cryptographic Coprocessor

Os avisos do IBM Cryptographic Coprocessor incluem três avisos, que fornecem as recomendações para o descarte seguro de componentes eletrônicos.

Reciclagem e Descarte do Produto

Essa unidade contém materiais como placas de circuito, cabos, gaxetas de compatibilidade eletromagnética e conectores que podem conter chumbo, cobre e berílio, o que requer cuidados especiais no manuseio e no descarte no fim de vida. Antes que essa unidade seja descartada, esses materiais

devem ser removidos e reciclados ou descartados de acordo com os regulamentos aplicáveis. A IBM oferece programas de retorno de produto em vários países. As informações sobre as ofertas de reciclagem do produto podem ser localizadas no Web site da IBM em http://www.ibm.com/ibm/environment/products/prp.shtml. A IBM incentiva os proprietários de equipamentos de tecnologia da informação (IT) a reciclarem com responsabilidade os aparelhos quando não foram mais necessários. A IBM oferece uma variedade de programas e serviços para ajudar os proprietários de equipamentos a reciclarem os produtos de TI. As informações sobre as ofertas de reciclagem do produto podem ser localizadas no Web site da IBM em:

http://www.ibm.com/ibm/environment/products/prp.shtml

Aviso: Essa marca se aplica apenas aos países na União Européia (UE) e na Noruega. Os dispositivos são rotulados de acordo com a Diretiva Européia 2002/96/EC referente ao Waste Electrical and Electronic Equipment (WEEE). A Diretiva determina a estrutura de retorno e de reciclagem de dispositivos usados como aplicáveis em toda a União Européia. Esse rótulo é aplicado à vários produtos para indicar que o produto não deve ser descartado incorretamente, mas em vez disso, deve ser reciclado ou aproveitado no final da vida de acordo com essa Diretiva.

Programa de Retorno de Bateria

Esse produto pode conter baterias do tipo Chumbo Ácido, Níquel Cádmio (NiCad), Hidreto Metálico de Níquel (NiMH), Lítio ou Lítio Íon. Consulte seu manual do usuário ou o manual de serviço para obter informações específicas da bateria. A bateria deve ser reciclada ou descartada corretamente. Os recursos para reciclagem podem não estar disponíveis na sua área. Para obter informações sobre o descarte de baterias fora dos Estados Unidos, acesse http://www.ibm.com/ibm/environment/products/batteryrecycle.shtml ou entre em contato com seu recurso de descarte de lixos. Nos Estados Unidos, a IBM estabeleceu um processo de retorno para reutilização, reciclagem ou descarte correto de baterias IBM do tipo ácido chumbo, níquel cádmio, hidreto metálico de níquel (NiMH) e outras baterias a partir do Equipamento IBM. Para obter informações sobre o descarte correto dessas baterias, entre em contato com aIBM pelo número 1-800-426-4333. Consulte o número de peça IBM listado na bateria disponível antes de ligar.

Para Taiwan: Recicle as baterias.

Programa de Retorno de Placa do IBM Cryptographic Coprocessor

Essa máquina pode conter um recurso opcional, a placa de coprocessador criptográfico, que inclui um material de poliuretano que contém mercúrio. Siga as orientações ou regulamentos locais para descartar essa placa. A IBM estabeleceu um programa de retorno para determinadas placas IBM Cryptographic Coprocessor. Mais informações podem ser localizadas em:

http:/www.ibm.com/ibm/environment/products/prp.shtml

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM, poderá ser usado em substituição. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não-IBM são de inteira responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não garante ao Cliente nenhum direito sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
Brasil

Para pedidos de licenças relativos a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO A, AS GARANTIAS IMPLÍCITAS DE NÃO-INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, esta disposição pode não se aplicar ao Cliente.

Estas informações podem conter imprecisões técnicas ou erros tipográficos. Periodicamente, são feitas alterações nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais nesses websites não fazem parte dos materiais deste produto IBM e o uso desses websites é de inteira responsabilidade do usuário.

A IBM por usar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Os licenciados deste programa que desejarem obter informações sobre este assunto com o propósito de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações trocadas, deverão entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo,
Rio de Janeiro, RJ
Brasil

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriados, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM do Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Os dados de desempenho e exemplos de clientes citados são apresentados apenas para propósitos ilustrativos. Os resultados de desempenho reais podem variar, dependendo de configurações e condições operacionais específicas.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras origens disponíveis publicamente. A IBM não testou esses produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não-IBM devem ser dirigidas aos fornecedores destes produtos.

As declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio e representam apenas metas e objetivos.

Todos os preços da IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudança sem aviso. Os preços de revendedores podem variar.

Essas informações apenas têm a finalidade de planejamento. As informações aqui contidas estão sujeitas a alterações antes que os produtos descritos estejam disponíveis.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos contam com nomes de pessoas, empresas, marcas e produtos. Todos esses nomes são fictícios e qualquer semelhança com pessoas ou empresas reais é mera coincidência.

LICENÇA DE DIREITOS AUTORAIS:

Estas informações contêm exemplo de programas aplicativos na linguagem fonte, que ilustram técnicas de programação em várias plataformas operacionais. Você pode copiar, modificar e distribuir esses programas de amostra em qualquer formato sem o pagamento à IBM, para os propósitos de desenvolvimento, uso, marketing ou distribuição de programas aplicativos de acordo com a interface de programação de aplicativos para a plataforma operacional para a qual os programas de amostra foram escritos. Estes exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou assegurar a confiabilidade, capacidade de manutenção ou função desses programas. Os programas de amostra são fornecidos "no estado em que se encontram", sem garantia de qualquer tipo. A IBM não deve ser responsabilizada por nenhum dano decorrente do uso das amostras de programas.

Cada cópia ou parte destes programas de amostra ou qualquer trabalho derivado deve incluir um aviso de copyright com os dizeres:

© (nome da sua empresa) (ano).

Partes deste código são derivadas dos Programas de Amostra da IBM Corp.

© Copyright IBM Corp. _insira o ano ou os anos_.

Considerações sobre política de privacidade

Os Produtos de software IBM, incluindo soluções de software como serviço, (“Ofertas de Software”) podem usar cookies ou outras tecnologias para coletar informações de uso do produto, para ajudar a melhorar a experiência do usuário final, para customizar as interações com o usuário final ou para outros fins. Em muitos casos, nenhuma informação pessoalmente identificável é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar a coletar informações pessoalmente identificáveis. Se esta Oferta de Software usar cookies para coletar informações pessoalmente identificáveis, informações específicas sobre o uso de cookies desta oferta serão definidas abaixo.

Esta Oferta de Software não usa cookies ou outras tecnologias para coletar informações pessoalmente identificáveis.

Se as configurações implementadas para esta Oferta de Software fornecerem a você como cliente a capacidade de coletar informações pessoalmente identificáveis de usuários finais via cookies e outras tecnologias, você deve buscar seu próprio aconselhamento jurídico sobre quaisquer leis aplicáveis a tal coleta de dados, incluindo requisitos para aviso e consenso.

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para estes fins, consulte a Política de Privacidade da IBM em http://www.ibm.com/privacy e Declaração de Privacidade Online da IBM na http://www.ibm.com/privacy/details seção titulada “Cookies, Web Beacons and Other Technologies” e “IBM Software Products and Software-as-a-Service Privacy Statement” em http://www.ibm.com/software/info/product-privacy.

Marcas Registradas

IBM, o logotipo IBM e ibm.com são marcas comerciais ou marcas registradas da International Business Machines Corp., registradas em vários países no mundo todo. Outros nomes de produtos e serviços podem ser marcas comerciais da IBM ou de outras empresas. Uma lista atual de marcas comerciais da IBM está disponível na web em Copyright and trademark information em www.ibm.com/legal/copytrade.shtml.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

Windows é uma marca comercial da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Java e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas da Oracle e/ou de suas afiliadas.

Índice Remissivo

A

B

C

D

E

F

G

I

K

L

M

N

O

P

R

S

U

V

Z

Impresso no Brasil