# Manual do usuário do IDProtect client middleware

Rev. 2 – 26 de setembro de 2016 Manual do usuário

### Informações do documento

Info	Conteúdo
Palavras-chave	-
Resumo	Este manual descreve as utilidades e bibliotecas do IDProtect client middleware. Explica o suporte e a configuração dos smart cards PIN e biométricos. Destina-se a gestores de TI, administradores de sistemas e engenheiros de software responsáveis pela implementação de suporte a smart card em suas organizações.



# Manual do usuário do IDProtect client

Histórico de	e revisões	
Rev	Data	Descrição
v.2	20160926	O banner foi removido.
v.1	20160606	Versão inicial.

# Informações de Contato

Para mais informações, visite: http://www.nxp.com

Para endereços dos escritórios de vendas, enviar e-mail para salesaddresses @nxp.com/iconductors N.V. 2016. Todos os direitos

. Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

UM10947 Manual do Usuário

# 1. Introdução

O IDProtect client middleware é um conjunto de utilidades e bibliotecas de middleware. Quando combinado com um smart card ou token IDProtect LASER, ChipDoc ou CNS, suporta serviços de smart card no Microsoft Windows. Estes serviços incluem logon interativo, e-mail seguro e VPN. Além disso, suporta a maioria das aplicações de smart card de terceiros, que utilizam padrões de middleware CAPI, PKCS#11 e Minidriver/CNG.

Os cartões NXP são programados de fábrica para suportar apenas PIN ou biométrica de digitais e/ou PIN. Neste manual, cartões que suportam apenas PIN são chamados de **PIN cards**. Cartões que suportam PIN e biometria são chamados de **Bio cards**.

Este manual destina-se a gestores de TI, administradores de sistema e engenheiros de software responsáveis pela implementação de suporte a smart card em suas organizações.

Este manual assume que o leitor tenha familiaridade com:

- Uso geral de computadores
- Windows XP, Windows 7, Windows 8, Windows 10
- Windows Server 2008, Windows Server 2012
- Active Directory e Microsoft Certificate Authority and Services

# 2. Pré-requisitos

Os pré-requisitos para configurar o logon de smart card no Windows 2003/2008/2008 R2/Windows Server 2012 Server/Server 2012 R2 são:

- Controlador de domínio instalado em um servidor de domínio Windows Server 2003/2008/2008R2/2012/2012R2
- Um Microsoft CA configurado com o Enterprise Policy Module
- Estação de registro de smart cards configurada com políticas de usuário de smart card ou logon por smart card. Consulte o documento separado intitulado *Windows Server Smart Card Integration Guide*

Para informações detalhadas sobre a instalação e configuração de um Microsoft CA e diretório ativo, consulte a documentação da Microsoft.

Quando a instalação do controlador de domínio for concluída e o CA estiver configurado com uma estação de registro de smart card, prossiga para a próxima sessão para obter instruções passo a passo.

Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

Manual do Usuário

# 3. IDProtect client para Windows

# 3.1 Instalação

O IDProtect client pode ser instalado nos sistemas operacionais a seguir:

- Windows XP, 32 bit e 64 bit
- Windows Vista, 32 bit e 64 bit
- Windows 7, 32 bit e 64 bit
- Windows 8 e 8.1, 32 bit e 64 bit
- Windows 10, 32 bit e 64 bit
- Windows Server 2003, 32 bit e 64 bit
- Windows Server 2008, 32 bit e 64 bit, Windows Server 2008 R2
- Windows Server 2012, Windows Server 2012 R2

O IDProtect client suporta sistemas operacionais de x86 e x64 bits e a última versão/pacotes de serviços de cada sistema operacional. Para instalar em sistemas x86, execute o programa de instalação setup.exe ou utilize o IDProtectClient.msi. Para instalar em sistemas x64, execute o programa de instalação setupx64.exe ou utilize o IDProtectClient64.msi. O arquivo .msi permite a instalação do IDProtect client para usuários de domínio utilizando a Política de Grupo. Há diversas opções de instalação que permitem controlar a instalação do IDProtect client e componentes do cliente a serem instalados em cada máquina. Veja <u>Seção 18</u> <u>"Opções avançadas de instalação por linha de comando"</u> para uma lista de sinais de instalação e o seu uso.

Para suportar a emissão de certificados de smart card e atribuí-los a smart cards NXP, o PC da estação de trabalho de registro de smart cards deve ter o IDProtect cliente instalado. Isso também se aplica a cada estação de trabalho de usuário final que exija logon por smart card ou qualquer outra interação com o smart card.

### 3.1.1 Instalação do IDProtect client para suporte de PIN cards

Ao instalar o IDProtect Client para suportar Cartões PIN, há 2 métodos de instalação:

- Microsoft Base CSP: Instala o Microsoft Base Smart Card CSP como provedor CAPI padrão (Minidriver). Também instala PKCS#11, "Athena Key Storage Provider" (Athena KSP), o IDProtect Format Tool, o IDProtect Manager, as Opções e ferramentas PIN. Não instala componentes de software que são necessários para o suporte de logon biométrico, seja localmente ou em serviços de terminal e ambientes Citrix.
- 2. Personalizada: Permite a seleção de itens específicos. Por exemplo, permite que os componentes CSP do NXP IDProtect client middleware sejam definidos como provedor CAPI padrão. Não é necessário instalar a documentação ou diversas ferramentas em cada PC de usuário final. Os PIN cards não exigem instalação do Biometric Support, Biometric RDP e componentes biométricos Citrix.

UM10947

© NXP Semiconductors N.V. 2016. Todos os direitos

### Manual do usuário do IDProtect client



Custom Setup Select the program features you want installed.	
Click on an icon in the list below to change how a feature i	s installed. Feature Description Allows biometric logon support This feature requires 0KB on your hard drive.
Install to:	Change
nstallShield Sack	Next > Cancel

Para formatar, reformatar e limpar os cartões, mudar os PINs do usuário ou admin., cadastrar impressões digitais e outras propriedades, a ID Protect format tool deve ser instalada. Se os cartões adquiridos não tenham sido formatados, eles devem ser personalizados antes do uso.

Direitos de administrador local no host são necessários para instalar o IDProtect client.

UM10947

. Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

**NOTA:** O IDProtect client instala o "Athena Key Storage Provider" juntamente com o "Microsoft Key Storage Provider", acessível pelo Athena Minidriver. O "Athena Key Storage provider" suporta CNG e está disponível em todos os sistemas operacionais que suportem CNG. Inclui SOs de clientes Vista e posteriores, assim como Server 2008 e servidores posteriores.

#### 3.1.2 Instalação do IDProtect client para suporte de BIO cards

Ao instalar o IDProtect client para suporte de BIO Cards, e os BIO cards forem destinados ao Logon do Windows, escolha a opção de instalação Personalizada (Custom).

**Personalizada (Custom):** Esta opção permite a seleção dos itens a serem instalados. Por exemplo, pode não ser necessário instalar a documentação e/ou as diversas ferramentas em cada PC de usuário final. Para BIO cards, pode ser necessário selecionar uma das funcionalidades a seguir:

- Suporte biométrico Esta opção é padrão para Microsoft GINA ou Credential Provider no Vista e versões posteriores que suportem apenas logon por Nome de Usuário/Senha ou por PIN Smart Card. Oferece uma nova interface que permite logon por verificação de digitais e/ou PIN. A instalação de suporte biométrico exige a reinicialização do PC.
- Componentes de servidor biométrico RDP Para fazer o logon a PCs remotos, instale este componente no PC que atua como servidor para a sessão RDP.
- Componentes de cliente biométricos Citrix Quando os Bio cards são usados no ambiente Citrix, este componente e o ambiente Citrix devem ser instalados no PC do cliente. Nota: o cliente Citrix deve ser instalado antes do IDProtect client. Se o cliente Citrix já estiver instalado quando o IDProtect client for instalado, a instalação do IDProtect deve ser executada no modo de Reparo (Repair).

Select the program features you want installed.	-4
Click on an icon in the list below to change how a feature is	s installed.
Set Athena as Default Provider     Documentation     Tools     Athena KSP Support     RDP Biometric Server Components     Citrix Biometric Client Components     Install in Mozilla Firefox     Biometric Support	Feature Description Allows biometric logon support This feature requires 13MB on your hard drive.
Install to: C: \Program Files (x86) \Athena \IDProtect Client \ InstallShield	Change
Help < Back	Next > Cancel

**Nota:** O logon por smart card e logon por smart card biométrico é obtido usando o provedor de credenciais Microsoft. O provedor de credenciais NXP foi removido do Windows 7 e sistemas operacionais posteriores e Windows Server 2008 R2 e sistemas operacionais posteriores. O provedor de credenciais Microsoft agora é usado para logon biométrico, independentemente do CSP padrão. O provedor de credenciais NXP pode ser instalado no sistema operacional Windows Vista, já que o logon biométrico não funciona com o provedor de credenciai MS.

A instalação do IDProtect client configura o serviço de smart card para **Inicialização automática** e inicia o serviço.

# 3.1.3 Instalação do IDProtect client em Citrix e ambiente de servidor terminal Windows

Ao usar um Bio Card no Citrix um ambiente de servidor terminal, o IDProtect client deve estar instalado tanto no lado do cliente como no lado do servidor.

Instale o IDProtect client antes de prosseguir para a Seção 4.

© NXP Semiconductors N.V. 2016. Todos os direitos

UM10947

Rev. 2 — 26 de Setembro de 2016

#### 4. Parâmetros de formatação padrão

Os NXP smart cards exigem formatação antes de serem registrados para certificados de smart card. Se não tiver certeza se o cartão está formatado, é possível visualizar esta informação nas ferramentas IDProtect Format ou IDProtect Manager.

A ferramenta de formatação do IDProtect é oferecida com dois perfis de formatação padrão, que definem diversos parâmetros de comportamento do cartão. O perfil de formatação ASEDefault é desenvolvido para que cartões sejam usados com o Admin PIN padrão. O perfil de formatação MDDefault é desenvolvido para cartões serem usados com 3DES Challenge/Response Admin PIN. A diferença entre os dois tipos de Admin PIN é explicada posteriormente neste guia. Ao trabalhar no modo Minidriver, o Admin PIN deve ser do tipo 3DES Challenge/Response.

Nota: Os perfis de formatação mencionados acima não podem ser mudados ou editados de qualquer forma. Se eles forem necessários como base para um perfil de formatação personalizado, copie suas configurações e aplique todas as mudanças ao novo perfil de formatação.

Seguindo a formatação do cartão, alguns dos parâmetros podem ser apenas mudados pela reformatação. Outros parâmetros podem ser atualizados sem reformatação, mas podem exigir uma credencial de usuário (PIN ou biométrica) ou Admin PIN. A Tabela 1 mostra detalhes relacionados aos diversos parâmetros e seu método de atualização.

Os principais parâmetros dos perfis ASEDefault e MDDefault encontram-se listados na Tabela 1.

#### Parâmetros principais ASEDefault e MDDefault Tabela 1.

Assunto	Valor ASEDefault	Valor MDDefault	Atualização sem reformatação	Protegido por
nome do perfil	ASEDefault.ppf	MDDefault.ppf	não relevante	não relevante
rótulo do cartão	IDProtect "IDProtect" + Número de Série do Cartão	IDProtect "IDProtect" + Número de Série do Cartão	sim	usuário
mudar PIN no primeiro uso	não	não	sim	admin
mudar PIN após Destravamento	não	não	sim	admin
(PIN) permanece válido por Min.	não definido	não definido	sim	admin
(PIN) expira após Dias	não definido	não definido	sim	admin
lembra últimos x PINs	X = 1	não definido	não	n.a.
PIN do usuário	11111111	11111111	sim	usuário
tipo de verificação	PIN	PIN	não	n.a.
extensão mínima de PIN do usuário	4 caracteres	4 caracteres	não	n.a.
extensão máxima de PIN do usuário	10 caracteres	10 caracteres	não	n.a.
verificações máximas de PIN do usua tentativas	ário 10	10 tentativas	não	n.a.
desbloqueios máximos do PIN do usu	uário ilimitados	ilimitados	não	n.a.
máximo de dados registrados	não definido	não definido	não	n.a.
qualidade da imagem	não definido	não definido	durante FEED	NIV, 2016. Todos os direitos

Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

# **NXP Semicondutores**

# UM10947

#### Manual do usuário do IDProtect client

taxa de aceitação falsa	não definido	não definido	durante FEP <sup>[1]</sup>	n.a.
Regras de complexidade PIN	nenhum	nenhum	não	n.a.
Valor PIN admin	0000000	3DES 303030303030303030	sim	admin <sup>[2]</sup>
extensão mínima de desbloqueio PIN	4 caracteres	n.a.	não	n.a.

#### Tabela 1 Parâmetros pricipais ASEDefault e MDDefault ... continuação

Assunto	Valor ASEDefault	Valor MDDefault	Atualização sem reformatação	Protegido por
extensão mínima de desbloqueio PIN	10 caracteres	n.a.	não	n.a.
máximo de tentativas para verificação de desbloqueio PIN	3 tentativas	3 tentativas	não	n.a.
Regras de complexidade PIN	nenhum	n.a.	não	n.a.
PIN de assinatura digital do usuário	não	não	não	n.a.

[1] FEP = Finger Enrollment Process (Processo de Registro de Dedos)

[2] 3DES pode ser apenas mudado pela reformatação do cartão

# 4.1 Formatação rápida do IDProtect card

O suporte para Secure Messaging com base em ECC aplica-se apenas aos IDProtect laser cards e ChipDoc cards. Esta funcionalidade utiliza chaves ECC ao realizar envio de mensagens seguro entre o cartão e o host.

O tipo de chaves (ECC ou RSA) usado com envio de mensagens seguro é definido durante o processo de formatação dos cartões.

É possível habilitar esta funcionalidade especificando o parâmetro MSI (veja Seção 18 "Opções avançadas de instalação por linha de comando") ou modificando uma chave de registro DWORD:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Athena Smartcard Solutions\IDProtect Client\aseSMFormatType

Se definido como 1, os cartões são formatados para usar Secure

Messaging com base em ECC. Se definido como 0, os cartões são

formatados para usar Secure Messaging com base em RSA.

Em hosts X64 esta chave também deve ser criada no local de registro a seguir:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Athena Smartcard Solutions\IDProtect Client\aseSMFormatType

A configuração padrão é formatar os cartões usando Secure Messaging com base em ECC. Apenas aplique esta configuração em hosts com base em Windows usados para formatar os cartões. © NXP Semiconductors N.V. 2016. Todos os direitos

UM10947

Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

#### Notas:

- O envio de mensagens seguro com base em ECC NÃO é retrocompatível. Cartões personalizados para usar o envio de mensagens seguro com base em ECC não funcionam com versões do IDProtect client posteriores ao IDProtect client 6.20.
- O IDProtect client funciona com clientes de envio de mensagens seguro com base em ECC e RSA.

# 4.2 Cartões habilitados com RSA 4096

O NXP suporta a geração e importação de chaves RSA 4096 em algumas configurações do produto. O suporte para chaves RSA 4096 depende do smart card. O smart card deve também suportar chaves RSA 4096, além de suportar este tamanho de chave no IDProtect client. Chaves RSA 4096 são suportadas no IDProtect client 6.13 e posteriores.

Para habilitar suporte para chaves RSA 4096 no IDProtect client, o valor do registro aseKeySizeMax deve ser definido como 4096 (decimal) O aseKeySizeMax está localizado em:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Athena Smartcard Solutions\IDProtect Client

Em hosts X64 este valor também deve ser configurado em:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Athena Smartcard Solutions\IDProtect Client

Esta configuração deve ser aplicada nos hosts usados para formatar os cartões.

© NXP Semiconductors N.V. 2016. Todos os direitos

UM10947

Rev. 2 — 26 de Setembro de 2016

# 5. Uso da ferramenta de formatação IDProtect em PIN cards

Veja a <u>Seção 6.2</u> para personalização de Bio Cards.

# 5.1 Descrição geral

A ferramenta de formatação do IDProtect é uma aplicação de simples utilização que dá ao administrador controle total sobre a política de segurança e diversos parâmetros do cartão. A ferramenta pode ser usada para:

- Visualizar detalhes do cartão, tais coo número de série, espaço livre na memória, etc.
- Gerenciar PINs de usuário e administração e outros parâmetros sem invalidar as credenciais armazenadas no cartão.
- Visualizar, editar e criar perfis de formatação.
- Formatar e reformatar cartões.
- Limpar um cartão (reverter o cartão para um estado não formatado).

# 5.2 Uso da ferramenta IDProtect Format

Para iniciar a ferramenta IDProtect Format:

```
Clique em Start -> All Programs -> IDProtect Client -> IDProtect Format
```

A janela do IDProtect Format é exibida:

	Card Info	
	Card name No Card	
	Card label	
	Card state	
Athena ASEDr	Version	
	Serial number	
	Total memory	
	Total free memory	
	Format	
	Profile: ASEDefault.ppf   Format	
	Close	

Para iniciar o trabalho com a ferramenta IDProtect Format, insira um smart card ou token NXP em um leitor de smart card instalado.

© NXP Semiconductors N.V. 2016. Todos os direitos

# Manual do usuário do IDProtect client

O monitor do IDProtect, que é uma tarefa de plano de fundo que monitora eventos de smart card, identifica que o cartão inserido não está formatado. Ele exibe um alerta mostrado na Figura 5. Há uma opção para que este alerta não seja exibido no future.

	The card that was inserted is	not pesonallized.	
4	To personallize the card use	IDProtect Format Tool	
-	· De net den this measure entit	Class	
	Do not show this message again	L	5

A janela da ferramenta IDProtect Format exibe os detalhes do cartão inseridos.

A janela da ferramenta IDProtect Format exibe os detalhes do cartão inseridos. A imagem do leitor de smart card, à esquerda da janela, indica que o cartão foi inserido.

	Card Info	
	Card name	IDProtect
	Card label	Net Decemplized
Athens ACED	Version	3 0032
Athena ASEDT	Serial number	0A52001626323124
	Total memory	73728 Bytes
	Total free memory	57406 Bytes
	Biometrics enabled	Yes
	Format Profile: ASEDefault.	ppf Format
		Close

## 5.2.1 Formatação de PIN card

Para formatar um PIN card:

- 1. Selecione o Perfil de Formato necessário na lista pop-up de perfis.
- 2. Clique no botão Format.

**Nota:** Se um cartão anteriormente formatado for formatado, será exibido um prompt para inserir o Admin PIN. Use "00000000" para o perfil ASEDefault. Use "303030303030303030303030" chave 3DES, para o perfil MDDefault.

3. Espere pela mensagem "Success".

Se for necessário revisar, adicionar, remover ou editar um perfil de formatação, selecione Manage Profiles...

no menu File.

File Card PIN	Help	
Modify Admi Manage Profi Exit	les	IDProtect
Athena ASEDr	Version Serial number Total memory Total free memory Biometrics enabled	Not Personalized 3.0032 0A52001626323124 73728 Bytes 57406 Bytes Yes
	Format Profile: ASEDefault	ppf Format Close
		aaa-(

A janela **Profile List** é exibida conforme mostrado na Figura 8.

### Manual do usuário do IDProtect client

Profiles
ASEDefault.ppf
MDDefault.ppf
Remove New Modify

Selecione o perfil de formatação necessário e clique em **Modify**... para modificar ou revisar os parâmetros de personalização ou clique em **New**... para criar um perfil. Clicar em **Remove** exclui o perfil selecionado.

Clicar em Modify.... ou New... abre a janela Manage Profile.

#### Notas:

- Os perfis ASEDefault.ppf e MDDefault.ppf não podem ser excluídos. Eles podem ser salvos apenas com um nome diferente.
- Os perfis são salvos sob o diretório do usuário atualmente logado (C:\Users\UserName\AppData\Local\NXP). Eles não são visíveis a partir de outras contas, salvo se forem manualmente copiados para esta conta.

# 5.3 Gestão de perfis

A janela **Manage Profile** é onde a política de segurança é definida e os parâmetros relevantes dos cartões a serem formatados são encontrados: Há 4 abas separadas – **General, User PIN, Admin PIN e Digital Signature**.

Manual do usuário do IDProtect client

General User	PIN Admir	PIN	Digital Signat.	ıre
Profile Na	me			
ASEDefa	ult.ppf			
Card Inf Card la	o bel			
Chang	e user PIN a hange user F	t first u PIN afte	se er unblock	
Stays •	valid for	60	Min	
Expire:	s after	30	Days	
Remen	nber last	1	PINs	
Cancel			Si	ave

# 5.3.1 Manage Profile – aba Geral

**<u>Profile Name:</u>** Use para definir um nome para o novo perfil ou modificar o nome de um perfil existente.

#### Card Info:

**Card Label** - O Card Label é usado para ajudar a identificar os cartões a serem formatados. O rótulo não possui efeito sobre quaisquer serviços de smart card do Windows. Ele equivale ao PKCS#11 Token Label. Se o rótulo não for definido, é definido automaticamente o padrão "IDProtect + número de série do cartão" ou "CNS + número de série do cartão", dependendo do tipo de cartão usado.

**Change user PIN at first use** – O usuário é solicitado a alterar o PIN do usuário quando o cartão é usado pela primeira vez. Além de mudar o PIN, nenhuma outra ação habilitada por smart card protegido por PIN é permitida até que o PIN seja alterado para um novo valor. O PIN pode ser mudado durante o procedimento de Logon do Windows (no Logon do Windows Vista, é suoportado apenas com o IDProtect Credential Provider).

**Must change user PIN after unblock** – Durante o procedimento de desbloqueio, um novo valor de PIN é selecionado. Escolher esta opção exigirá que o usuário mude o User PIN novamente durante o próximo uso do cartão.

**Stays valid for** – Define o tempo de duração da validade do PIN do usuário. Quando o número de minutos inserido passar, o usuário é solicitado a verificar o PIN.

© NXP Semiconductors N.V. 2016. Todos os direitos

O PIN é sempre exigido. Quando um PIN de usuário for exigido para todas as operações de chave privada, insira um valor de 0 minutos.

Expires after – Força o usuário a mudar o PIN após um número de dias especificado.

**Remember last** – Aplica uma política pela qual um novo PIN não pode ser igual a um dos últimos X valores de PIN utilizados. Até 16 valores podem ser armazenados no cartão. Por motivos de segurança, apenas um HASH do PIN antigo é armazenado.

Gener	al User PIN Admin PIN Digital Signature
	PIN value
	Default - 11111111
	Verification Policy:
	Verification type User PIN
	Biometric settings
	Maximum fingers to enroll: 2
	Image quality FAR.
	51 * 1: 10000 *
	Complexity rules
Ca	ncel Save

### 5.3.2 Manage Profile – aba User PIN

### PIN Value:

Para configurar os PINs durante a personalização, 3 seleções são possíveis a partir do menu pop-up.

**Manual** – Um prompt é mostrado para inserir o PIN do usuário durante o processo de formatação de cada cartão.

**Default** – Cada cartão é formatado com o PIN de usuário padrão, conforme especificado no perfil.

Random – Um PIN aleatório é gerado e apresentado durante a formatação do cartão.

Importante: Se a geração aleatória de PIN for selecionada, copie o valor do PIN da tela e mantenha-o em local seguro. Não há como recuperar um PIN aleatório perdido.

© NXP Semiconductors N.V. 2016. Todos os direitos

PINs de usuário aleatórios são gerados de acordo com regras de complexidade de PIN pré-definidas. Por exemplo, ao escolher um valor de PIN de usuário aleatório, o diálogo mostrado na Figura 11 aparece durante a personalização do cartão.

© NXP Semiconductors N.V. 2016. Todos os direitos

UM10947 Manual do Usuário

### Manual do usuário do IDProtect client

User User PIN	WErRTnsOCT	nkxBjp
Confirm User Pin		
Please make sure to c the randomly generat	opy and backup ed User PIN in	Set
a safe place!		Cancel

Certifique-se de que a escolha das opções de geração do PIN do usuário esteja de acordo com a política de segurança da organização.

#### Verification Policy:

Verification type - Selecione o PIN de usuário para PIN cards (para Bio Cards, veja a Seção 6).

#### **Complexity Rules:**

As regras de complexidade habilitam a aplicação de diversas regras ao PIN do usuário. As regras são definidas de acordo com a política de segurança da organização.

PIN Rules Max attempts	Max unblocks	Min chars	Max chars
10 🔻	Unlimit 🔹	4 🔹	16 🔻
Complexity non AlphaNumeric Alphabetic Max sequence	0 <b>v</b> 0 <b>v</b> 16 <b>v</b>	Upper case Numeric Max repeating chars	0 • 0 • 16 •
		Cancel	Set

Max Attempts - O número de tentativas de verificação consecutivas mal sucedidas, antes que o PIN do usuário seja bloqueado. © NXP Semiconductors N.V. 2016. Todos os direitos

. Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

Max Unblocs - Número total de desbloqueios do PIN do usuário bem sucedidos, permitidos durante a vida de um cartão. Atingir o número máximo exige que o cartão seja reformatado.

Min and Max chars - define o comprimento exigido do User PIN.

Estes parâmetros podem ser mudados na janela Manage Profile - User PIN complexity rules (veja Figura 12) para se adequar à política de segurança. Quando a edição estiver concluída, salve o perfil com o mesmo nome, para substituir o perfil anteriormente salvo ou salve-o com um nome diferente (recomendado). Selecionar Cancel anula e descarta quaisquer alterações feitas ao perfil atual.

Para utilizar um perfil específico para formatação de cartão, selecione-o a partir da lista pop-up Profile na janela principal da Ferramenta de Formatação (veja Figura 8) e clique em Format.

#### 5.3.3 Manage Profile – aba Admin PIN

General	User PIN Admin PIN Digital	Signature
	value fault <b>v</b> 00000000	
Ver	fication Policy: fication type PIN	•
3D C Ke	<b>s key policy</b> Ise Admin Card Generate random diversification Value	data
C	mplexity rules	
Cance		Save

O uso da aba Admin PIN é similar ao uso da aba User PIN. Há 2 diferencas principais:

1. Definir o máximo de tentativas do Admin PIN tem importantes conseguências, pois uma vez que o Admin PIN tenha sido bloqueado, o cartão não pode ser mais usado.

Atenção: Após o Admin PIN ter sido bloqueado, o cartão ainda pode ser usado. No entanto, qualquer ação administrativa que exija o Admin PIN, tal como desbloqueio de PIN de usuário e a Formatação ,falhará. © NXP Semiconductors N.V. 2016. Todos os direitos

2. O valor do Amin PIN pode também ser definido para o Admin Card. O Admin Card é uma poderosa ferramenta para formatação segura de cartões e desbloqueio de PIN. Ela é oferecida separadamente do IDProtect client. O Admin Card patenteado é uma solução poderosa e segura de gestão de cartões. Ela evita o uso de CMS totalmente desenvolvido para projetos de smart cards de pequeno a médio porte que exijam gerenciamento seguro de smart card.

O acesso ao Admin Card é protegido com o uso de um PIN de usuário. Se segurança mais alta for necessária, um Match-on-Card PIN biométrico pode ser usado. Entre em contato com a NXP ou revendedor NXP para mais informações sobre esta funcionalidade.

Ger	neral User PIN Admin PIN Digital Signature
	PIN value
	Default   00000000
	Manual
	Random V:
	Verification type PIN -
	3Des key policy
	Use Admin Card
	Generate random diversification data
	Key value
	0000000
	Complexity rules
	Cancel
	Cancel

UM10947

Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

# Manual do usuário do IDProtect client

Gener	al User PIN Admin PIN	Digital Signature	-
100	PIN value		
	Default 🔻 000	00000	
	Verification Policy:		
	Verification type 3DES	Key 🔻	
	3Des key policy		
	Use Admin Card		
1	Generate random dive	rsification data	
	30303030303030303030303030303030303030	D	
	Complexity rules		
Car	ncel	Save	
Car	ncel	Save	

Ao configurar o Admin PIN para que seja uma chave 3DES, o valor de chave inserido deve ser um valor de chave DES/3DES válido. O valor pode ser uma entrada de 8 bytes, 16 bytes ou 24 bytes h (16, 32 ou 48 dígitos).

# 5.3.4 Manage Profile – aba Digital Signature

A aba Digital Signature define as configurações de assinatura digital do cartão. Nota: nem todos os tipos de cartão suportam todas as opções de assinatura digital. A tentativa de formatar um cartão que não suporte PIN de assinatura digital falhará. Para mais informações sobre assinatura digital, veja <u>Seção 12 "Assinatura digital"</u>.

	General User PIN Admin PIN Digital Signature	
	V use Digital Signature PIN Key properties Max 2048 bit keys Max 1024 bit keys 2 • 0 • PIN value Default • 11111111 Complexity rules	
	Unblock PIN value       Default     00000000       Complexity rules	
8	Cancel	

#### Use digital signature PIN

Ao marcar a caixa **use digital Signature PIN**, o cartão com o PIN de assinatura digital será formatado e posteriormente associado a definições de chaves específicas. As configurações relevantes podem ser definidas após esta opção ter sido marcado.

#### Key properties

**Max 2048-bit Keys** – Define o número máximo de chaves de assinatura digital de 2048 bits que podem ser criadas no cartão formatado.

**Max 1024-bit Keys** – Define o número máximo de chaves de assinatura digital de 1024 bits que podem ser criadas no cartão formatado.

#### **Digital signature PIN value**

Para configurar os PINs durante a formatação, 3 seleções são possíveis a partir do menu pop-up:

© NXP Semiconductors N.V. 2016. Todos os direitos

Manual – Um prompt é mostrado para inserir o PIN de assinatura digital durante o processo de formatação de cada cartão.

**Default** – Cada cartão é formatado com o PIN de assinatura digital, conforme especificado no perfil.

**Random** – Um PIN de assinatura digital aleatório é gerado e apresentado durante a formatação do cartão.

Importante: Se a geração aleatória de PIN for selecionada, copie o valor do PIN da tela e mantenha-o em local seguro. Não há como recuperar um PIN aleatório perdido.

PINs aleatórios são gerados de acordo com regras de complexidade de PIN pré-definidas.

#### **Unblock PIN value**

O valor Unblock PIN é similar às configurações Admin PIN do PIN de usuário.

**Atenção:** Após Ublock PIN ter sido bloqueado, o cartão ainda pode ser usado, mas qualquer ação que exija o Unblock PIN, tal como desbloqueio de PIN de assinatura digital, falhará.

Para configurar os PINs durante a formatação, 3 seleções são possíveis a partir do menu pop-up:

**Manual** – Um prompt é mostrado para inserir o Admin PIN durante o processo de formatação de cada cartão.

**Default** – Cada cartão é formatado com o PIN de usuário padrão, conforme especificado no perfil.

Random – Um PIN aleatório é gerado e apresentado durante a formatação do cartão.

Importante: Se a geração aleatória de PIN for selecionada, copie o valor do PIN da tela e mantenha-o em local seguro. Não há como recuperar um PIN aleatório perdido.

# 6. Uso da ferramenta de formatação IDProtect em Bio Cards

Veja a <u>Seção 5.2</u> para personalização de PIN cards.

# 6.1 Descrição geral

A ferramenta de formatação do IDProtect é uma aplicação de simples utilização que dá ao administrador controle total sobre a política de segurança e diversos parâmetros do cartão. A ferramenta pode ser usada para:

- Visualizar detalhes do cartão, tais coo número de série, espaço livre na memória, etc.
- Gerenciar PINs de usuário e administração e cadastrar dados biométricos sem invalidar as credenciais armazenadas no cartão.
- Visualizar, editar e criar perfis de formatação.
- Formatar e reformatar cartões.
- Determinar o tipo de Match on Card (MoC) biométrico suportado.

Começando com o IDProtect Versão 6.13.00, diversas ofertas de smart cards da NXP também suportam formatação de MoC ISO IEC 19794-2. O Biometric MoC é configurado durante a produção do cartão e é mutualmente exclusivo. Em outras palavras, um cartão habilitado biometricamente pode suportar ISO MoC e Precise Biometrics MoC, mas não os dois tipos simultaneamente.

# 6.2 Uso da ferramenta IDProtect Format

Para iniciar a ferramenta **IDProtect Format**:

Clique em **Start** ->**Programs**->**IDProtect Client** ->**IDProtect Format**. A janela do IDProtect Format é exibida conforme mostrado na <u>Figura 17</u>. Insira um smart card NXP em um leitor de smart card instalado.

Manual do usuário do IDProtect client

	Card Info		
	Card name	No Card	
	Card label		
	Card state		
Athena ASEDr	Version		
	Serial number		
	Total memory		
	Piometrics enabled		
	Format		
	Profile: ASEDefa	ult.ppf 🔹	Personalize
			Close

O IDProtect Monitor é uma tarefa de plano de fundo que monitora eventos de smart card. Ele verifica se o cartão inserido não é personalizado e exibe o alerta mostrado na <u>Figura 18</u>. Para optar por não mostrar este alerta no futuro, marque a caixa "Do not show this message again".

	The card that was inserted is	not pesonalized		
	to personalize the card use	IDProtect Forma	it 1001	
L Do	not show this message again	ſ	Close	
			****	
			aaa-02095	57

A janela da ferramenta IDProtect Format exibe os detalhes do cartão inseridos. A imagem do leitor de smart card, à esquerda da janela, indica que o cartão foi inserido.

File Card PIN	Help	
	Card Info	
	Card name Card label	IDProtect
	Card state	Not Personalized
Athena ASEDr	Version	3.0039
	Serial number	1017C8A08C403949
	Total memory	73728 Bytes
	Total free memory	51798 Bytes
	Biometrics enabled	ISO
	Format	
	Profile: ASEDefa	ult.ppf   Format
		Close

## Cartão com ISO MoC habilitado

Cartão com Precise MoC habilitado

<u>File</u> <u>Card</u> <u>PIN</u>	Help		
	Card Info		
	Card name	IDProtect	
	Card label		
	Card state	Not Personalized	
Athena ASEDr	Version	3.0032	
	Serial number	0A52001626323124	
	Total free memory	57406 Bytes	
	Biometrics enabled	Yes	
	Format		3
	Profile: ASEDefault.	ppf  Format	
2		Close	
		close	
<u></u>			

**Nota:** Se o rótulo de biometria habilitado do cartão não mostrar **ISO** ou **Yes**, o cartão não poderá ser usado para biometria. Os Bio Cards vêm programados de fábrica para suportar biometria.

© NXP Semiconductors N.V. 2016. Todos os direitos

# 6.2.1 Formatação de um Bio Card

#### Para formatar um Bio Card:

- Selecione o perfil de formatação necessário na lista de rolagem Profile (ver <u>Figura</u> <u>20</u>) e certifique-se de que o tipo de verificação (ver <u>Figura 23</u>) esteja definido como **Biometric**.
- 2. Clique no botão Format.
  - Nota: ao reformatar um cartão formatado anteriormente, um prompt é exibido para inserir o Admin PIN (00000000 é o padrão). O perfil MDDefault utiliza a chave 3DES 3030303030303030 como padrão.
- 3. Cadastre as digitais quando solicitado (ver Figura 29).
- 4. Espere pela mensagem "Success".

Para revisar, adicionar, remover ou editar qualquer perfil de formatação, clique no botão File -> Manage Profiles...

A janela **Profile List** é exibida (ver Figura 21).

Após selecionar um perfil da lista de perfis, há 4 seleções possíveis:

Profil	es List
	Profiles ASEDefault.ppf MDDefault.ppf
	Remove New Modify
Fig 21 Lists de porti UD	Close aaa-020960
Modify para modifica	r ou revisar os parâmetros de formatação
New – para criar um pe	ərfil
<b>Remove</b> – para excluir u	m perfil selecionado
Close – para encerrar ur	n processo
icar em <b>Modify</b> ou <b>Ne</b>	© NXP Semiconductors N.V. 2016. Todos os direi

# 6.3 Gestão de perfis

A janela **Manage Profile** é onde a política de segurança é definida e os parâmetros relevantes dos cartões a serem formatados são configurados. A janela **Manage Profile** contém 4 abas separadas - **General**, **User PIN**, **Admin PIN** e **Digital Signature**.

General	User PIN	Admin PIN	Digital Signature	e
Prof	ile Name			
AS	EDefault.pp	f		
Ca	rd Info			_
C	ard label			
	Change user	PIN at first	use	
	Must change	user PIN af	ter unblock	
	Stays valid f	or 60	Min	
E	Expires after	r 30	Days	
V F	Remember la	ast 1	PINs	
Cana			<b></b>	
Cance	=		Sav	/e

### 6.3.1 Aba Geral

**Profile Name:** Use para definir um nome para o novo perfil ou modificar o nome de um perfil existente.

#### Card Info:

**Card Label** - O Card Label é usado para ajudar a identificar os cartões a serem formatados. O rótulo não possui efeito sobre quaisquer serviços de smart card do Windows. Ele equivale ao PKCS#11 Token Label. Se o rótulo não for definido, é definido automaticamente o padrão "IDProtect + número de série do cartão" ou "CNS + número de série do cartão", dependendo do tipo de cartão usado.

**Change user PIN at first use** – O usuário é solicitado a alterar o PIN do usuário quando o cartão é usado pela primeira vez. Além de mudar o PIN, nenhuma outra ação habilitada por smart card protegido por PIN é permitida até que o PIN seja alterado para um novo valor. O PIN pode ser alterado durante o procedimento de Logon do Windows. No Logon do Windows Vista, é suportado apenas com o IDProtect Credential Provider.

© NXP Semiconductors N.V. 2016. Todos os direitos

Must change user PIN after unblock – Durante o procedimento de desbloqueio, um novo valor de PIN é selecionado. Escolher esta opção exigirá que o usuário mude o User PIN novamente durante o próximo uso do cartão.

**Stays valid for** – Define o tempo de duração da validade do PIN do usuário. Quando o número de minutos inserido passar, o usuário é solicitado a verificar o PIN.

O PIN é sempre exigido. Quando um PIN de usuário for exigido para todas as operações de chave privada, insira um valor de 0 minutos.

Expires after – Força o usuário a mudar o PIN após um número de dias especificado.

**Remember last** – Aplica uma política pela qual um novo PIN não pode ser igual a um dos últimos X valores de PIN utilizados. Até 16 valores podem ser armazenados no cartão. Por motivos de segurança, apenas um HASH do PIN antigo é armazenado.

### 6.3.2 Aba User PIN para Bio Cards

General U	ser PIN A	dmin PIN	Digital Sig	nature	
PIN va	alue ult 👻	11111	1111		
Verific	ation Policy ation type	Biomet	tric	•	
Biome Maxir	tric setting: num finger:	Biomet Biomet s to Biomet	ric or PIN ric or PIN ric and PIN		
Image 51	e quality ▼	FAR 1:1000	0	•	
Com	lexity rule	s			
Cancel			C	Save	

#### Verification Policy

Para escolher o tipo de verificação necessário, selecione uma das 4 opções mostradas na Figura 24 (para PIN Cards, ver a Seção 5).



User PIN – Apenas verificação PIN é suportada (mesma que o PIN card, ver Seção 5)

Biometric – O cartão suporta apenas uma verificação de digitais.

**Biometric or PIN** – Um PIN ou uma combinação de digital pode ser usada para a verificação.

**Biometric and PIN** – Um PIN e uma verificação de digital devem ser usados, implementando autenticação verdadeira de 3 fatores.

#### **Biometric settings**

**Maximum fingers to enroll** – Entre 1 e 10 dedos podem ser cadastrados para cada cartão. Enquanto a seleção está sujeita à política de segurança da organização, é recomendado que um mínimo de 2 dedos sejam usados. Deve ser um de cada mão para oferecer um retorno quando um dedo estiver machucado ou não for lido corretamente pelo sensor biométrico.

**Image quality** – Define o limite mínimo para qualidade de captura de imagem abaixo do qual o cadastro da digital não é tentado. Esta configuração pode ser diferente para cada dedo cadastrado.

**False Acceptance Rate (FAR)** – A medida da probabilidade do sistema biométrico aceitar incorretamente uma tentativa de acesso por um usuário não autorizado. O FAR é declarado como a razão entre o número de aceitações falsas dividido pelo número de tentativas de identificação.

#### **Complexity Rules**

As regras de complexidade habilitam a aplicação de diversas regras ao PIN do usuário. As regras são definidas de acordo com a política de segurança da organização.

### Manual do usuário do IDProtect client

PIN Rules Max attempts 10 -	Max unblocks Unlimit 👻	Min chars	Max chars	
Complexity				
non AlphaNumeri	c 0 🔹	Upper case	0 -	
Alphabetic	0 🔹	Numeric	0 🔹	
Max sequence	16 🔻	Max repeating chars	16 🔻	
			_	
		Cancel	Set	

**Max Attempts** – O número de tentativas de verificação consecutivas mal sucedidas, antes que o PIN do usuário seja bloqueado.

**Max Unblocks** – Número total de desbloqueios do PIN do usuário bem sucedidos, permitidos durante a vida de um cartão. Atingir o número máximo exige que o cartão seja reformatado.

Min and Max chars - define o comprimento exigido do User PIN.

Estes parâmetros podem ser mudados na janela **Manage Profile – User PIN complexity rules** (veja Figura 25) para se adequar à política de segurança. Quando a edição estiver concluída, salve o perfil com o mesmo nome, para substituir o perfil anteriormente salvo ou salve-o com um nome diferente (recomendado). Selecionar Cancel anula e descarta quaisquer alterações feitas ao perfil atual.

Para utilizar um perfil específico para formatação de cartão, selecione-o a partir da lista pop-up Profile na janela principal da Ferramenta de Formatação (veja Figura 8) e clique em Format.

UM10947 Manual do Usuário

Manual do usuário do IDProtect client

General User	PIN Admin PIN	Digital Signature	
PIN value			-
Default	• 0000	0000	
Verificatio Verificatio	n Policy: n type PIN	•	
- 3Des key Use Ad Genera Key value 0000000	<b>policy</b> min Card te random divers 0	sification data	
Complexit	y rules		
Cancel		Save	

# 6.3.3 Aba Admin PIN

O uso da aba Admin PIN é similar ao uso da aba User PIN. Há 2 diferenças principais:

 Definir o máximo de tentativas do Admin PIN tem importantes consequências, pois uma vez que o Admin PIN tenha sido bloqueado, o cartão não pode ser mais usado.

**Atenção:** Após o Admin PIN ter sido bloqueado, o cartão ainda pode ser usado. No entanto, qualquer ação administrativa que exija o Admin PIN, tal como desbloqueio de PIN de usuário e a Formatação ,falhará.

2. O valor do Amin PIN pode também ser definido para o Admin Card. O Admin Card é uma poderosa ferramenta para formatação de cartão segura e desbloqueio de PIN, oferecida separadamente do IDProtect Client. Entre em contato com a NXP ou revendedor NXP para mais informações sobre esta funcionalidade.

# Manual do usuário do IDProtect client

Į	General User PIN Admin PIN Digital Signature	
	PIN value	
	Default   O0000000  Manual	
	Default Random V:	
	Verification type PIN -	
	3Des key policy	
	Use Admin Card	
	Generate random diversification data	
	Key value	
	0000000	
	Complexity rules	
ſ	Cancel	

Ao configurar o Admin PIN para que seja uma chave 3DES, o valor de chave inserido deve ser um valor de chave DES/3DES válido. O valor pode ser uma entrada de 8 bytes, 16 bytes ou 24 bytes h (16, 32 ou 48 dígitos).

## 6.3.4 Aba Digital Signature

A aba Digital Signature define as configurações de assinatura digital do cartão. Nota: nem todos os tipos de cartão suportam todas as opções de assinatura digital. A tentativa de formatar um cartão que não suporte PIN de assinatura digital falhará. Para mais informações sobre assinatura digital, veja a <u>Seção 12 "Assinatura Digital"</u>.

General	User PIN	Admin PIN	Digital Sig	nature
PIN D Un	se Digital Si y properties ix 2048 bit l l value efault Complexity block PIN va efault Complexity	gnature PII eys Mi ( 1111) rules ulue 0000 rules	ax 1024 bit 0 111111 000000	keys
Cance			C	Save

### Use digital signature PIN

Ao marcar a caixa Digital Signature PIN, o cartão com o PIN e PUK de assinatura digital será formatado e posteriormente associado a definições de chaves específicas. Quando esta opção for marcada, as configurações relevantes podem ser definidas.

#### Key properties

**Max 2048-bit Keys** – Define o número máximo de chaves de assinatura digital de 2048 bits que podem ser criadas no cartão formatado.

**Max 1024-bit Keys** – Define o número máximo de chaves de assinatura digital de 1024 bits que podem ser criadas no cartão formatado.

#### **Digital signature PIN value**

Para configurar os PINs durante a formatação, 3 seleções são possíveis a partir do menu pop-up:

© NXP Semiconductors N.V. 2016. Todos os direitos

. Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

**Manual** – Um prompt é mostrado para inserir o PIN do usuário durante o processo de formatação de cada cartão

**Default** – Cada cartão é formatado com o PIN de usuário padrão, conforme especificado no perfil.

**Random** – Um PIN aleatório é gerado e apresentado durante a formatação do cartão.

Importante: Se a geração aleatória de PIN for selecionada, copie o valor do PIN da tela e mantenha-o em local seguro. Não há como recuperar um PIN aleatório perdido.

PINs aleatórios são gerados de acordo com regras de complexidade de PIN pré-definidas.

#### Unblock PIN value

O valor Unblock PIN é similar às configurações Admin PIN do PIN de usuário.

**Atenção:** Após Ublock PIN ter sido bloqueado, o cartão ainda pode ser usado, mas qualquer ação que exija o Unblock PIN, tal como desbloqueio de PIN de assinatura digital, falhará.

Para configurar os PINs durante a formatação, 3 seleções são possíveis a partir do menu pop-up:

**Manual** – Um prompt é mostrado para inserir o Admin PIN durante o processo de formatação de cada cartão.

**Default** – Cada cartão é formatado com o PIN de usuário padrão, conforme especificado no perfil.

Random – Um PIN aleatório é gerado e apresentado durante a formatação do cartão.

Importante: Se a geração aleatória de PIN for selecionada, copie o valor do PIN da tela e mantenha-o em local seguro. Não há como recuperar um PIN aleatório perdido.

# 6.4 Formatação de um Bio Card

A formatação de um Bio Card exige os passos a seguir:

- 1. Instalação de um leitor de smart card biométrico
- 2. Execução da ferramenta IDProtect Format
- 3. Selecionar e modificar, se necessário um perfil biométrico (ver Seção 6.2.1)
- 4. Inserir um Bio Card no leitor de smart card
- 5. Clicar em Format
- 6. Se o cartão já estiver formatado, uma solicitação é feita à chave do Admin PIN (00000000 por padrão)
- 7. A ferramenta IDProtect Format irá sequenciar o cadastro de impressões digitais conforme descrito na <u>Seção 6.4.1</u>

#### 6.4.1 Cadastro de impressões digitais

Após clicar em **Format**, o diálogo IDProtect Enroll é exibido e é feito um prompt. Selecione o primeiro dedo a ser cadastrado e clique em **Enroll** (ver <u>Figura 29</u>).

© NXP Semiconductors N.V. 2016. Todos os direitos

# Manual do usuário do IDProtect client

IDProtect#085000	02523070157			
To enroll, select	the first finge	r and press the En	roll button.	
	0 0		Select biometric read	er
Image Quality :	51 -	False acceptance rate :	1 : 10000	•
			Cancel	Enroll

O diálogo IDProtect Enroll indica o dedo atual sendo cadastrado ao piscar um ponto verde acima do dedo escolhido (ver Figura 30).
### Manual do usuário do IDProtect client

	147		
IDProtect#0A54001235156	147		
Place your finger on the se	nsor		
1	1	Calcot biometric read	
		BSPAPI_0	=
Image Quality : 51 +	False acceptance rate :	1:10000 Cancel	+

#### Fig 30. IDProtect indicando o dedo sendo cadastrado

Selecione um leitor biométrico do menu de rolagem, no caso de mais de um estar instalado.

As instruções são exibidas no canto superior esquerdo do diálogo durante o processo de cadastro.

Após posicionar o dedo correto no sensor, diversas solicitações são feitas para tirar e colocá-lo novamente. Certifique-se de que o dedo seja totalmente removido antes de recolocá-lo sobre o sensor.

### Manual do usuário do IDProtect client

IDProtect#0A54001235156947	
1	
	BSPAPI_0 -
Image Quality : 51 - False	e acceptance rate : 1 : 10000 +
	Cancel

Fig 31. IDProtect mostrando a impressão digital sendo cadastrada

Após posicionar o dedo correto diversas vezes, o estágio de verificação para esta impressão digital é alcançado (ver <u>Figura 31</u>).

IDProtect#0A54001235156947 Place your finger on the sensor	IDProtect#0A54001235156947 Place your finger on the sensor	IDProtect#0A54001235156947 Place your finger on the sensor	
Place your finger on the sensor	Place your finger on the sensor	Place your finger on the sensor	
NI, 11,	Select biometric reader		
	Select biometric reader		
	BSPAPI 0 V	BSPAPI 0	-
BSPAPI_0  Cancel		٨.٥٥٥	020971
BSPAPI_0  Cancel	200.02021	aaa-0.	020977
BSPAPI_0  Cancel aaa-020971	aaa-020971	erificação de impressão digital do IDProtect	NI 1/ 2010

	124	
One finger is enrolled. To e	enroll another one, sele	ect finger and press Enrol
6	5	Select biometric reader
Image Quality 51 🔹	False acceptance rate :	1:10000 -

Após a verificação bem sucedida do primeiro dedo, é solicitado o próximo dedo a ser cadastrado.

O processo continua até que todos os dedos sejam cadastrados, até o número de dedos definidos no perfil de formatação, conforme descrito na <u>Seção 6.3.2</u>. Para pular o cadastro de um ou mais dedos, **Continue** pode ser selecionado a qualquer momento. O cadastro de dedos pode continuar, utilizando-se a ferramenta de cadastro biométrico do IDProtect (ver a <u>Seção 9</u>). O cartão é considerado como **Formatado** mesmo que não seja cadastrado nenhum dedo. A partir deste ponto, o cadastro biométrico ou repersonalização do cartão exige Admin PIN ou Admin Card.

Quando o cadastro de dedos for completado com êxito, a mensagem mostrada na in <u>Figura 34</u> é exibida:

Card was successfully personalized.
ОК

. Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

### 7. Mudança ou desbloqueio do PIN do usuário

Conforme mencionado anteriormente, é possível mudar os PINs de usuário e admin sem reformatar o cartão. Há diversas formas de acessar as ferramentas de Mudança/Desbloqueio de PIN.

# 7.1 Mudança de PIN de usuário a partir do IDProtect Monitor na Bandeja do Sistema

O usuário final pode mudar o PIN de usuário de seu cartão a qualquer momento, conforme descrito a seguir:

Clique com o botão direito do mouse no ícone do IDProtect Monitor

### 

na Bandeja do Sistema e selecione Manage PIN... a partir do menu.

Manager
Manage PIN
Biometric Enrollment
Options
Hide
aaa-020974

A janela IDProtect PIN Tool é exibida:

IDProtect#0A52001	626323124		
PIN Type		Status	
🕂 PIN	0	Valid	Change
Biometric	•	Absent	
Signature	•	Absent	
			Close

Para mudar o PIN de usuário, selecione o link <u>Change</u>. O diálogo IDProtect user PIN é exibido. Insira o PIN de usuário atual e em seguida o novo PIN de usuário.

O PIN de usuário do perfil NXP padrão é: 11111111. . Todas as informações fornecidas neste documento estão sujeitas a isenções legais. © NXP Semiconductors N.V. 2016. Todos os direitos

### Manual do usuário do IDProtect client

IDProtect#0A52	001626323124
Enter your User	PIN
Current User PIN	1
New User PIN	
Confirm new PIN	
·/-	Close Change

Fig 37. Janela de mudança de PIN do IDProtect

Quando concluído, o diálogo mostrado na Figura 38 é exibido.

The PIN was changed	
ОК	

**Nota:** Há um número máximo de tentativas ao inserir um PIN de usuário incorreto. Quando o número for atingido (o número máximo de tentativas padrão é 10), o cartão é bloqueado e não poderá ser mais usado. Para ganhar acesso ao cartão novamente, o PIN de usuário deve ser desbloqueado com o uso do Admin PIN.

# 7.2 Mudança de PIN de usuário a partir da ferramenta de PIN do IDProtect Card Manager

Clique em Start > All Programs > IDProtect Client > IDProtect Manager e selecione Manage

... a partir do menu de PIN

O procedimento é o mesmo descrito na Seção 7.1.

© NXP Semiconductors N.V. 2016. Todos os direitos

Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

Manual do usuário do IDProtect client

### 7.3 Mudança de User PIN a partir do IDProtect Format

Clique em Start > All Programs > IDProtect Client > IDProtect Format e selecione Manage ...

a partir do menu de PIN

O procedimento é o mesmo descrito na Seção 7.1.

**Nota:** O PIN de usuário também pode ser mudado durante a operação normal do cartão, sempre que for apresentada uma nova caixa de diálogo Verify PIN ao usuário. O usuário deve marcar a caixa **Change PIN after verification**. Um prompt solicita a mudança do PIN após a verificação bem sucedida do PIN atual.

### 7.4 Mudança de User PIN a partir da caixa de diálogo IDProtect PIN

Quando uma instalação mínima do IDProtect Client for feita, o usuário ainda pode escolher o PIN do usuário após verificação bem sucedida do PIN. Isso também se aplica quando a ferramenta IDProtect PIN não estiver instalada. Isso é feito a partir da caixa de diálogo IDProtect PIN, marcando-se a caixa **Change PIN after Verification**.

Insira o PIN do usuário, marque a caixa **Change PIN after Verification** e pressione o botão **Verify** (ver Figura 39).

1	DProtect Verification
	IDProtect#0653000450216254
	Enter your User PIN
	Change PIN after verification
	Cancel Verify aaa-020978
Fig 39. Campo de e	ntrada de alteração do IDProtect PIN

Insira e confirme o novo PIN de usuário e em seguida pressione o botão Change (ver Figure 40).

### Manual do usuário do IDProtect client

IDProtect#06530	00450216254
Enter your User	PIN
Current User PIN	*******
New User PIN	
Confirm new PIN	
1	Close Change

Em determinados ambientes, pode ser necessário desabilitar esta funcionalidade. Para desabilitar esta funcionalidade, crie a chave de registro DWORD Flag a seguir com o valor 1:

#### HKLM\Software\AthenaSmartcardSolutions\IDProtect Client\aseHideChangePIN

Em máquinas de 64 bits, uma chave de registro DWORD Flag adicional com o valor 1 deve ser criada no caminho de registro a seguir:

HKLM\Software\Wow6432Node\AthenaSmartcardSolutions\IDProtectclient\aseHideChange PIN

### 7.5 Desbloqueio de um PIN de usuário bloqueado

Quando um PIN de usuário incorreto é repetidamente inserido, ele é bloqueado quando o **parâmetro de Máximo de Tentativas** é alcançado. Este parâmetro é definido durante a formatação do cartão (o padrão é 10 tentativas). O PIN do usuário pode apenas ser desbloqueado com o uso do Admin PIN.

Selecionar **Manage PIN...** a partir da bandeja do sistema ou o menu **IDProtect Manager** abrirá a ferramenta IDProtect PIN.

### Manual do usuário do IDProtect client

IDProtect#0A520	001626323124		
PIN Type		Status	
T PIN	•	Locked	Unlock
Biometric	•	Absent	
[ Signature	•	Absent	
			Close
			Close

O diálogo do IDProtect mostra que o PIN do usuário está bloqueado. Para desbloquear o PIN do usuário, pressione <u>Unlock</u>.

O Administrador deve inserir o PIN do cartão do administrador (PUK).

**Nota:** Um diálogo diferente é apresentado se for utilizado um cartão de administrador ou outro método de desbloqueio.

IDProtect#085	000252C300157
IDProtect User	r PIN
PUK	1
New PIN	
Confirm PIN	
A 1	
	Close OK
	999-02/081

O administrador deve agora inserir e confirmar um novo valor para o PIN do usuário.

Se o PUK for inserido incorretamente, a mensagem mostrada na <u>Figura 43</u> é exibida e revela o número de tentativas restantes.

© NXP Semiconductors N.V. 2016. Todos os direitos



**Nota:** Após 2 tentativas adicionais mal sucedidas (ou conforme definido no parâmetro de máximo de tentativas para o Admin PIN no perfil), o cartão é bloqueado. Uma vez bloqueado, as operações que exijam o Admin PIN não podem ser realizadas, como, por exemplo, desbloquear o PIN de usuário ou reformatar. As operações que exijam o PIN de usuário permanecerão funcionais.

### 7.6 Desbloqueio de um PIN de usuário bloqueado com o uso de um cartão de administrador

Quando um PIN de usuário incorreto é repetidamente inserido, ele é bloqueado quando o parâmetro de Máximo de Tentativas é alcançado. Este parâmetro é definido durante a formatação do cartão (o padrão é 10 tentativas). O PIN do usuário pode apenas ser desbloqueado com o uso do Admin PIN.

Ao utilizar um Admin card para desbloquear um cartão bloqueado, pressione o link <u>Unlock</u> mostrado na <u>Figura 44</u>. A tela de desbloqueio de PIN é aberta (<u>Figura 45</u>) e **Unlock** poderá ser selecionado.

		IDProtect F	PINTool	
I	DProtect#42860	01814064792		
	PIN Type		Status	
井	PIN	•	Locked	Unlock
-	Biometric	•	Absent	
L	Signature	•	Absent	
				Close
				aaa-020
otec	t Card, unlock li	nk		Close

### Manual do usuário do IDProtect client

IDProtect#4286001814064792
Cocked.
To unlock the card using an Admin Card, check the 'Use Admin Card' checkbox and then click 'Unlock'
☑ Use Admin Card
Close Unlock

Quando selecionado, a janela a seguir é apresentada solicitando a inserção de um Admin card no leitor (ver Figura 46). Deve haver 2 leitores conectados.

PIN No Admin card was	The second se	
	found.	
Biometric Or press cancel to ex	ăt.	
/ Signature OK	Cancel	

Após inserir o Admin card no leitor adicional, insira o PIN para o Admin Card (ver Figura <u>47</u>).

### Manual do usuário do IDProtect client



Quando o PIN do Admin Card é autenticado, a janela mostrada na Figura 48 é apresentada. Ela permite que o novo User PIN seja escolhido para o cartão bloqueado.

IDF	IDProtect User PIN
	IDProtect#4286001814064792
PI	Enter your User PIN
H PI	New User PIN
/ 54	New Confirmation PIN data
-	Cancel OK
	Close
	aaa-020

Após a conclusão bem sucedida (ver see <u>Figura 49</u>), uma mensagem de notificação indica que o cartão agora é válido (ver <u>Figura 50</u>) e o uso poderá continuar com o User PIN mudado.

### Manual do usuário do IDProtect client

IDProtect#428	6001814064792	
PIN Type	IDProtect PINTool	×
T PIN	The PIN was unlocked and changed	Unlock
Biometric	<b>U</b>	
/ Signature	ОК	]
		Close

	IDProtect PINTool	×
IDProtect#428600	814064792	
PIN Type	Status	
🕂 PIN	Valid Chan	<u>ae</u>
Biometric	Absent	
/ Signature	Absent	
	Co	se
		aaa-02098

### 8. Mudança de Admin PIN

É possível mudar o Admin PIN ou Signature PUK sem reformatar o cartão. O procedimento é:

Clique em Start > All Programs > IDProtect Client > IDProtect Admin PINTool. Selecione Admin PIN ou Signature PUK, conforme necessário.

IDProtect#0953000	512354326		
PIN Type		Status	
H Admin PIN	ø	Valid	Change
Signature PUK	ø	Valid	Change
			Cancel

Nota: A IDProtect ADMIN PINTool não é instalada por padrão.

Para mudar Current Admin PIN, insira-o no campo mostrado na Figura 52. Agora preencha

New Admin PIN e Confirm new PIN. Pressione Change.

IDProtect#09530	00512354326
Enter your Admir	PIN
Current Admin PIN	
New Admin PIN	
Confirm new PIN	
1	Close Change

Pressione OK para confirmar a mudança bem sucedida do Admin SPI Augustors N.V. 2016. Todos os direitos

UM10947

Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

#### Manual do usuário do IDProtect client



O procedimento para mudar o **Signature PUK** PIN é idêntico ao procedimento para o novo Admin PIN.

### 9. Ferramenta de cadastro biométrico

O cadastro de impressões digitais é o equivalente do Bio Card à mudança do PIN em um PIN Card. Uma das principais diferenças é que o Administrator PIN deve ser inserido antes do cadastro.

As impressões digitais podem ser cadastradas a partir do **IDProtect Format** via **IDProtect Manager** ou a partir do **IDProtect Monitor**, conforme mostrado a seguir:

O usuário final pode mudar o PIN de usuário de seu cartão a qualquer momento, conforme descrito a seguir:

- Clique com o botão direito no ícone **IDProtect Monitor** na bandeja do sistema.
- Selecione o menu Biometric Enrollment... (ver Figura 54)



O processo de cadastro biométrico é descrito na <u>Seção 6.4</u>. O cadastro de biometria pela segunda vez remove todas as impressões digitais anteriormente armazenadas e salva apenas as impressões digitais recém cadastradas.

### **10. IDProtect Manager**

O **IDProtect Manager** pode ser instalado em PCs de usuários finais ou apenas na estação de trabalho de administradores. Isso é definido nas opções de instalação, conforme descrito na <u>Seção 3</u>.

O **IDProtect Manager** é acessado a partir de **Start** ->**Programs**->**IDProtect Client** ->**IDProtect Manager** ou pelo clique duplo no ícone na bandeja do sistema.

è é e	SØ	
	General Certificates & I	(eys
Athena ASEDr	Card name Card label Card state OS version Serial number Total nemory Total free memory Biometrics enabled	IDProtect IDProtect#0850002523070157 Personalized 4003.0022 0850002523070157 32767 Bytes 23518 Bytes Yes
		Close

O **IDProtect Manager** mostra informações relacionadas ao cartão inserido. Ele permite a gestão do PIN do usuário e a visualização de detalhes relacionados a certificados e chaves armazenados no cartão.

A seleção da aba **Certificates & Keys** mostra informações e habilita a gestão de certificados de PIN de usuário verificado e/ou impressões digitais.

#### Manual do usuário do IDProtect client

	IDProtect#0850002523070157
File Certification	Tana Enter your User PIN
20	
	Change BIN after verification
Athena ASED	Cancel Venity
	OS version 4003.0022
	Serial number         0850002523070157           Total memory         32767 Bytes
	Total free memory 22782 Bytes
	Biometrics enabled Yes
	Close
	Close

Ao trabalhar com IDProtect LASER e smart cards ChipDoc, a jenela abre e exibe uma única área. A área corresponde a ambos os certificados e chaves CAPI e PKCS#11.

Ao clicar uma vez na pasta CAPI ou no sinal "+", a pasta é aberta e o seu conteúdo revelado. Se o Logon do Windows ou um certificado de usuário de smart card já tiver sido baixado no cartão, a pasta CAPI exibe o nome do container associado com o certificado.

### Manual do usuário do IDProtect client

Athena ASEDr	General Certificates & Keys
	Close

Ao clicar no rótulo do container ou no sinal "+", a pasta é expandida e revela o certificado e a chave armazenados. No exemplo mostrado na <u>Figura 58</u>, um certificado foi emitido para o usuário **Administrator.** Uma chave privada é associada a este certificado e armazenada no cartão.

Agora é possível acessar todos os certificados e chaves válidos a partir de qualquer uma das interfaces. Por exemplo, um certificado pode ser importado usando Firefox e usado em aplicações CAPI.

Alternativamente, um certificado pode ser cadastrado usando CAPI, através do Athena CSP ou Microsoft Base Smart Card CSP. Pode, em seguida, ser usado a partir de aplicações PKCS#11 como o Firefox.

**Nota:** Containers (Certificados & Chaves) criados na área CAPI do cartão também são acessíveis por meio do PKCS#11 API. Ele é usado por aplicações como PGP, Netscape/Mozilla/Firefox, etc.

#### Manual do usuário do IDProtect client

Athena ASEDr	eneral Certificates & Keys CAPT Control Captor Capt
	Close

Fig 58. Aba Certificados & Chaves expandida no IDProtect

Os menus de rolagem, Toolbar Icons ou o menu acionado pelo clique do botão direito podem ser usados para realizar as seguintes operações no cartão:

**Importing certificates** – permite a importação de vários tipos de certificados. Inclui certificados que incluem o próprio certificado sem a chave privada. Também inclui arquivos .P12 e .pfx que incluem o certificado e a chave privada a eles associada.

**Exporting certificates** – permite que um certificado seja exportado usando o formato .cer ou exportado (carregado) no armazenamento de certificados do usuário.

**Deleting objects** – a maior dos objetos pode ser excluída, a menos que eles façam parte de um container padrão CAPI. Partes de um container padrão podem ser excluídas somente após a designação de outro container como "Padrão".

**Viewing certificate information** – clique duas vezes no certificado para abrir a ferramenta de visualização de certificados

Display refresh – atualiza a exibição

### 10.1 Configuração do container padrão

Um container pode também ser definido como o container padrão com o uso dos menus de rolagem ou acionados pelo clique do botão direito. Quando um container é definido como container padrão, o certificado nele armazenado é usado pelo Windows para Smart Card Logon.

UM10947

Rev. 2 – 26 de Setembro de 2016

### Manual do usuário do IDProtect client



© NXP Semiconductors N.V. 2016. Todos os direitos

### 11. Opções do IDProtect

Para abrir a caixa de diálogo **IDProtect Options**, selecione o menu **Options...** a partir do menu de arquivos do **IDProtect Manager**, ou clique com o botão direito no ícone do **IDProtect Monitor** na bandeja do sistema,

As opções são definidas para o "Current User" ou para "Local Machine". Para uma máquina local, as opções definidas se tornam as configurações padrões para todos os usuários, salvo se houver uma configuração específica para o usuário em questão.

A janela IDProtect Options contém 4 abas: General, Technical Support, Digital Signature e Advanced.

### 11.1 Aba Geral

A aba General dá acesso às configurações de certificado e opções de exibição do IDProtect Monitor.

#### Opções de Armazenamento de Certificado

O IDProtect Client automaticamente carrega os certificados encontrados em um cartão inserido em um leitor ao armazenamento de certificado do usuário atualmente logado. Normalmente, os certificados de usuário são carregados ao armazenamento de certificado pessoal (**Personal certificate**). Outros certificados, tais como certificados CA, são armazenados nos armazenamentos **Trusted Root CA** e **Intermediate CA**.

Por padrão, quando um cartão é removido, os certificados carregados quando o cartão foi inserido não são removidos do armazenamento de certificado pessoal. Esta configuração pode ser mudada na caixa de diálogo **Options**.

**Importante:** Ao ativar os certificados de remoção "**Upon card removal**" ou "**After x days from last loading**", apenas o **IDProtect Monitor** deve carregar os certificados ao armazenamento. Ao usar os sistemas operacionais Windows 7 ou Windows 8, o Microsoft Certificate Propagation Service deve ser desabilitado.

() Never	Certificates loaded from the card, will not be removed when the card is removed from the reader. This is the default behavior.
O Upon card removal	Certificates that were loaded when the card was inserted will be removed when the card is removed. <b>Note</b> - this only applies to certificates loaded to the <b>Personal</b> store.
After days from last loading	Certificates that were loaded from a card will be removed from the <b>Personal</b> certificate store <b>X</b> days after the card was last introduced to the reader.

aaa-021000

© NXP Semiconductors N.V. 2016. Todos os direitos

### Manual do usuário do IDProtect client

#### Outras opções

Show IDProtect Monitor in tray	Will toggle between showing and hiding the <b>IDProtect Monitor</b> icon <b>IDProtect Monitor</b> icon <b>IDProtect Monitor</b> icon <b>IDProtect</b> and <b>IDProte</b>
Dispaly a warning when a non-personalized card is inserted	Will toggle between showing and hiding the "non- personalized card" warning.
Clear Current User settings Will rest	ore the settings for the Current User to those of al Machine.
	aaa-02100

Ao selecionar "Manage IDProtect Settings" para Local Machine, o botão "Current User settings" é mudado para

Force Local Machine setting	15
aaa-021	002

e as configurações substituem as outras configurações do usuário.

### 11.2 Aba de Suporte Técnico

Esta aba habilita a geração e limpeza de arquivos de log.

O IDProtect Client suporta dois tipos de arquivo de log, Current User e Local Machine.

O log **Current User** é usado para registrar a atividade do smart card realizada pelo usuário após o usuário ter feito o logon no sistema.

O log **Local Machine** é usado para registrar atividade de smart card antes do usuário fazer logon no sistema. Ele também registra atividade de smart card realizada por um processo como aplicações publicadas por RDP ou Citrix.

### Manual do usuário do IDProtect client

Manage II	Protect settings as	Current User		-
General	Technical Support	Digital Signature	Advanced	
Log file				
	Generate log file			
Log	file name			
G	Users\user1\AppDat	a VLocal' Br	owsen	
	Clear Log File	Ð.		
	E	-		
	Email Log File			
			-	
Cle	ar Current User setti	ngs	ОК	
			Cancel	

Generate log file	Will generate a log file of the <b>IDProtect Client</b> events in the designated location.
Clear Log File	Clears the log file, if exists.
	aaa-02162

**Nota:** Os arquivos de log devem ser criados apenas se assim for instruído pelo representante do suporte técnico. Após criar o arquivo de log, remova a marcação da caixa de verificação.

### 11.2.1 Arquivos de log

#### Current User - arquivos de log

Para capturar eventos que ocorrem para o usuário atual, selecione Current User a partir de **Manage IDProtect as** em **IDProtect Options** (ver <u>Figura 61</u>).

Manage II	Protect settings as	Current U	lser	-
General	Technical Support	Digital Signat	ure Advanced	
Log file				_
Log	Generate log file file name			
C:	Users\username\Ap	pData\L	Browse	]
	Clear Log File			
	Email Log File			
Cle	ar Current User sett	ngs		
	OK	Cancel	Apply	

Para salvar um arquivo de log a um destino desejado usando o botão **Browse**, marque a caixa **Generate log file**. Alternativamente, salve um arquivo de log em seu caminho padrão.

Caminho padrão para arquivos de log (para Vista e posteriores): C:\Users\username\AppData\Local\Athena\AthenaCSPLog.txt

Caminho padrão de para arquivos de log (para Windows XP): C:\Documents and Settings\username\LocalSettings\ApplicationData\Athena\AthenaCSP Log.txt

#### Manual do usuário do IDProtect client

#### Local Machine – Arquivos de log

Para capturar eventos que ocorrem na máquina local, selecione Local Machine a partir de Manage IDProtect settings as em IDProtect Options.

Manage IC	Protect settings as	Local Machine	0	۷
General	Technical Support	Digital Signature	Advanced	
Log file				
Log	Generate log file file name	Debug	Level	
C:	Windows\Temp\Athe	enaCSPL Br	owse	
	Clear Log File			
	Email Log File			
Force L	ocal Machine setting	s Cancel	Apply	

Para salvar um arquivo de log a um destino desejado usando o botão **Browse**, marque a caixa **Generate log file**. Alternativamente, salve um arquivo de log em seu caminho padrão.

A entrada **Debug Level** está disponível para registro avançado pela equipe de suporte. Caso seja solicitado, a equipe de suporte pode fornecer a entrada exata a ser usada.

Caminho padrão de para arquivos de log (para todos os sistemas operacionais Windows): C:\Windows\Temp\AthenaCSPLog.txt

Certifique-se de que os arquivos de log sejam salvos em uma pasta com permissão de gravação.

#### Desativação dos arquivos de log

Os arquivos de log são desativados quando a caixa na aba **Technical Support** de IDProtect Options é desmarcada.

Também é possível limpar os arquivos de log ao clicar em **Clear Log File**. O arquivo de log agora passa a colher informações a partir do momento em que foi limpo.

© NXP Semiconductors N.V. 2016. Todos os direitos

UM10947

Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

### 11.3 Aba de Assinatura Digital

Esta aba especifica as configurações relacionadas ao PIN de assinatura digital. Para mais detalhes, veja <u>Seção 12 "Assinatura Digital"</u>.

Manage ID	Protect settings as	Current User		•
General	Technical Support	Digital Signature	Advanced	
Signatu	are PIN Policy			-1
O Ne	ver cached on the P	-		
ORe	member PIN and ack	nowledge		
O Pe	member PIN	nomeuge		
O Ke	member Pin			
Sy	nchronize Signature I	PIN with User PIN		
Key C	reation Policy			
One	xplicit use	•		
🔽 En	able Strong Key Prot	ection		
				_
Cle	ar Current User setti	ngs	ОК	
			Cancel	
			-	

© NXP Semiconductors N.V. 2016. Todos os direitos

UM10947

Rev. 2 – 26 de Setembro de 2016

Never cached on the PC	Signature PIN is never cached on the PC.
Remember PIN and acknowledge	PIN is cached on the PC but the user needs to acknowledge each time they sign. User needs to enter their DS PIN only once.
C Remember PIN	PIN is cached on the PC; no user action is required for signature. User needs to enter their DS PIN only once.
Synchronize Signature PIN with User PIN	The DS PIN is synchronized with the <b>User PIN</b> Both PIN's must have the same value.
Creation Policy On explicit use	On explicit use – private key is associated with the Signature PIN only if applications explicitly set it. Any signature key – private key is associated with every AT_SIGNATURE key. Container name starts with – it is possible to specify a container name prefix. Please refer to section 9. Digital Signature for more information.
Enable strong key protection	When the 'strong key protection' CAPI flag (CRYPT_FORCE_KEY_PROTECTION_HIGH) is set for a container, and the key is an AT_SIGNATURE key, associated the key with the digital

### 11.4 Aba Avançado

Esta aba habilita o desbloqueio de cartões sem logon ao Windows. Ela suporta **sessão** desconectada de firewall de ponto de verificação mediante a opção de remoção do cartão e define outras funcionalidades (ver Figura 64).

UM10947

Rev. 2 – 26 de Setembro de 2016

### Manual do usuário do IDProtect client

Manage IDProtect settings as	Local Machine
General Technical Support	Digital Signature Advanced
Settings  Show user fingerprint d  Allow logon with any us  Support Check Point VP	uring verification er certificate N session disconnection on card
removal Dynamic PIN Policy Turning on Dynamic PIN Po Unblock the Smart Card be	licy will allow the user to fore Logging on to Windows
<ul> <li>Allow Dynamic Pin</li> <li>Do not allow Dynamic P</li> </ul>	IN
Force Local Machine setting	js OK Cancel

### 11.4.1 Configurações

You can choose to display a "dummy" fingerprint figure or the real fingerprint image captured. Please note that when using biometric readers that utilize Match-on- Reader only a "dummy" fingerprint image can be displayed.
Allows any valid logon certificate present on the card to be used for smartcard logon
Disconnects Checkpoint VPN session when a
card is removed.

### Política de Desbloqueio Dinâmico

Uma das situações paradoxais com um logon de smart card do Windows é quando o PIN do usuário é bloqueado após muitas tentativas falhas. Nesta situação, o Windows não poderá ser acessado para usar as ferramentas de PIN para desbloqueá-lo.

O IDProtect Client oferece uma ferramenta única que exibe uma caixa de diálogo de desbloqueio de PIN sempre que um cartão bloqueado é inserido em um leitor durante tentativa de logon no Windows.

UM10947

. Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

### Manual do usuário do IDProtect client

C Allow Dynamic Pin	Shows the PIN Unlock dialog whenever an attempt is made to use a locked User PIN.
Do not allow Dynamic PIN	Does not show the PIN Unlock dialog whenever an attempt is made to use a locked User PIN.
	aaa-02101

Quando uma tentativa de logon é feita no Windows com um cartão bloqueado e a opção de desbloqueio dinâmico é permitida, a caixa de diálogo a seguir é exibida.



Para prosseguir com o processo de desbloqueio de PIN, clique em OK (ver Figura 66).



O PIN do administrador do sistema é necessário para prosseguir

(ver Figura 67). Quando solicitado, insira o Admin PIN e clique em

. Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

Verify para continuar.

© NXP Semiconductors N.V. 2016. Todos os direitos

### Manual do usuário do IDProtect client





Insira e confirme o novo User PIN e clique em OK para continuar (ver Figura 68).

	IDProtect User PIN
	IDProtect#0953000512334326
	Enter your User PIN
	New User PIN
	New Confirmation PIN data
	Cancel OK
	aaa-021015
68. Opcões do	IDProtect - Tela de solicitação de novo PIN de usuário e confirmaçã

O novo PIN agora pode ser usado para ativar o login do Windows.

#### Manual do usuário do IDProtect client



#### Política de desbloqueio dinâmico para cartões do tipo BIO OU PIN

A política de desbloqueio dinâmico atua em cartão do tipo BIO OU PIN da seguinte forma:

**Both biometric and user PINS are locked** – desbloqueie o PIN e defina um novo, em seguida, desbloqueie apenas a opção biométrica.

**Only user PIN locked** – desbloqueie o PIN de usuário e defina um novo. Se o desbloqueio falhar, continue o login com o PIN biométrico.

**Only biometric PIN locked** – faça o log in com o PIN de usuário. Após fazer o log in no sistema, o usuário pode desbloquear o PIN biométrico utilizando a ferramenta de cadastro biométrico do IDProtect (ver <u>Seção 9</u>).

Uma sinalização de registro DWORD adicional **aseUnlockPinOnOr**, controla o comportamento. Ela tenta desbloquear o PIN em um cartão do tipo Bio OU PIN por padrão. No entanto, se definida como 0, não é realizado desbloqueio dinâmico no PIN do usuário e o usuário tem de usar o PIN biométrico para fazer logon.

#### Política de Desbloqueio Dinâmico ao utilizar configuração do Microsoft Base CSP

Quando o Microsoft Base CSP for usado como provedor padrão, a Microsoft oferece um mecanismo incorporado para desbloquear um cartão. Este mecanismo é oferecido na tela de logon do Windows 7 e sistemas operacionais posteriores e Server 2008R2 e sistemas operacionais de servidor posteriores.

**Nota:** Esta configuração funciona apenas se o Admin PIN for definido como um valor 3DES. Para explicação detalhada, consulte as opções da ferramenta IDProtect Format na <u>Seção 5</u>.

© NXP Semiconductors N.V. 2016. Todos os direitos

Se, durante o logon pela tela de logon (ver <u>Figura 70</u>), um PIN de smart card incorreto for inserido, o smart card será bloqueado. A tela mostrada na <u>Figura 71</u> é exibida.





	The system could not log you on. The smart card is blocked. Please contact your administrator for instructions on how to unblock your smart card.
	OK
	aaa-021017
71 Onc	ções do IDProtect - Tela de Smart Card Bloqueado

Clique no botão OK e a tela mostrada na in <u>Figura 72</u> é exibida. Ela habilita uma resposta ao código de desafio-resposta a ser dado. Insira um novo PIN de usuário para o smart card e confirme-o.

© NXP Semiconductors N.V. 2016. Todos os direitos

### Manual do usuário do IDProtect client

<image/>	
aaa-021016	
rig / 2. Opções do iDProtect - Tela de Desploquelo de Smart Card	

**Nota:** Quando o smart card foi personalizado, uma chave 3DES foi usada. Uma resposta deve ser calculada a partir do desafio oferecido pela chave.

### **12.** Assinatura Digital

### 12.1 PINs Adicionais

Alguns smart cards, como o cartão NXP IDProtect, suportam assinatura digital. Um cartão formatado com a opção de assinatura digital é criado com 2 PINs adicionais para usuários de assinatura digital.

**Signature PIN** – Este PIN deve ser verificado sempre que uma operação de assinatura digital ocorra em um container de assinatura digital.

Signature PUK – O PIN de desbloqueio para o PIN de assinatura.

Para detalhes, veja a **aba Digital Signature** da ferramenta de formatação na <u>Seção 5.3.4</u> e <u>Seção 6.3.4</u>.

O PIN de assinatura pode ser associado a credenciais de usuário específico, tais como container de chave privada e certificado. Quando associada a uma chave privada, o PIN de assinatura é necessário para cada uso da chave. Ele evita uso não autorizado da chave privada de assinatura digital.

Ao formatar cartões com um PIN de assinatura e PUK, o número máximo de chaves privada para cada tamanho de chave (1024 e 2048) é determinado durante a formatação. Um cartão não pode ter mais do que o número máximo especificado de chaves privadas de assinatura digitais para aquele cartão.

### 12.2 Associação de uma chave privada com um PIN de assinatura digital

Um PIN de assinatura digital pode ser associado apenas a uma chave privada que tenha sido criada especificamente para operações de assinatura. Ele não pode ser associado a uma chave privada que foi criada por criptografia. No CAPI, isso significa que a chave deve ser uma chave AT\_SIGNATURE. Ao usar a interface PKCS#11, a chave deve ter o atributo CKA\_SIGN definido como CK\_TRUE, e o atributo CKA\_DECRYPT definido como CK\_FALSE.

#### Política de Criação de Chaves

A política de criação de chaves no aplicativo de opções do IDProtect, a aba **Digital Signature** (ver <u>Seção 5.3.4</u> e <u>Seção 6.3.4</u>), determina a política para associar uma chave privada com um PIN de assinatura. As seguintes regras de política podem ser definidas:

**On Explicit Use** – Quando definida, uma chave privada é apenas associada ao PIN de assinatura, se as aplicações definirem o atributo PKCS#11 2.20 CKA\_ALWAYS\_AUTHENTICATE.

**Any Signature Key** – Quando esta opção é definida, a chave privada é associada com todas as chaves AT\_SIGNATURE.

**Container name starts with** – Quando definida, é possível especificar um prefixo do nome do container. Qualquer chave de assinatura com um nome de container que seja iniciado com este prefixo é automaticamente associada ao PIN de assinatura. Para aplicações PKCS#11, se o atributo CKA\_ID inicia com o prefixo especificado, a chave é associada ao PIN de assinatura. A associação ocorre independentemente do valor do atributo CKA\_ALWAYS\_AUTHENTICATE.

© NXP Semiconductors N.V. 2016. Todos os direitos

**Enable Strong Key Protection** – Quando definida, qualquer container CAPI criado com a sinalização

strong key protection definida é automaticamente associado ao PIN de assinatura

O administrador do cartão marca chaves privadas que são associadas com o PIN de assinatura com o string **SSCD**. Isso ajuda a verificar se uma chave privada específica está associada ou não ao PIN de assinatura.

### 12.3 Sincronização de um PIN de usuário com um PIN de assinatura

Um PIN de usuário e um PIN de assinatura são 2 PINs diferentes no cartão. Para facilidade de uso, os usuários podem desejar ter o mesmo valor de PIN para ambos. O IDProtect Client pode ser configurado para sincronizar o PIN de usuário e o PIN de assinatura. Esta opção pode ser definida usando a aba **Digital Signature** (ver <u>Seção 5.3.4</u> e <u>Seção 6.3.4</u>). Quando a sincronização estiver ativa, o IDProtect Client automaticamente muda o PIN de assinatura e o PIN de usuário para o mesmo valor para manter sincronização.

Quando o tipo do Admin PIN não for uma chave simétrica usada com sequência de resposta de desafio, a sincronização é mantida entre o Admin PIN e o PUK signatário. Neste caso, o IDProtect também é capaz de manter a sincronização entre o PIN de usuário e o PIN signatário durante a operação de desbloqueio. Isso garante que o novo valor de PIN seja definido para o PIN de usuário e o PIN de assinatura.

**Nota:** Quando a opção **Synchronize Signature PIN with User PIN** é definida, o mesmo valor deve ser usado para o PIN de usuário e o PIN de assinatura. Caso contrário, o IDProtect Client pode bloquear o PIN de usuário ou o PIN de assinatura.

### 12.4 Armazenamento em cache do PIN de assinatura

O IDProtect Client oferece 3 modos de cache para o PIN de assinatura, acessados via aplicação IDProtect Options.

**Never cached on the PC** – Este modo é a opção padrão. Quando definido, o usuário deve inserir o PIN de assinatura sempre que a chave privada associada for usada.

**Remember PIN and acknowledge** – Quando esta opção é definida, o usuário é solicitado toda vez que a chave privada do usuário é usada. No primeiro uso da chave privada, o usuário deve inserir o PIN signatário. Para usos subsequentes, o usuário apenas terá de pressionar o botão OK. O PIN é armazenado em cache, por aplicação, para a sessão de cartão atual apenas. Consequentemente, se o cartão é removido e reinserido, ou se a aplicação é aberta novamente, o PIN deve ser reinserido.

**Remember PIN** – Quando esta opção é definida, o usuário deve inserir o PIN apenas uma vez. Nenhuma outra solicitação é feita parar inserir o PIN durante usos subsequentes da chave privada. O PIN signatário é armazenado em cache, por aplicação, para a sessão de cartão atual apenas. O usuário deve inserir o PIN após inserir o cartão ou quando a aplicação é executada.

UM10947

Rev. 2 – 26 de Setembro de 2016

### 13. Cadastro de Certificado de Usuário/Logon de Smart Card

Após os cartões ChipDoc e IDProtect LASER terem sido personalizados, eles estarão prontos para serem cadastrados para os certificados Smart Card Logon ou Smard Card User. Este capítulo assume que uma estação de cadastro de smart cards tenha sido configurada conforme descrito em

IDProtect for Windows Integration Guide.pdf.

Nota: Para cadastrar usuários de smart card, um leitor de smart card e o IDProtect Client devem ser instalados na estação de cadastro. O IDProtect Client inclui as funcionalidades Athena CSP ou Athena Minidriver.

Para cadastrar um usuário para um certificado de usuário de smart card ou logon de smart card, siga os passos a seguir. Assume-se que a estação de cadastro seja um host do Windows 7.

- 1. Faça o logon no computador da estação de cadastro como Administrador
- 2. Clique em Start, clique em Run, digite certmgr.msc e clique em OK
- 3. Na árvore do console, clique em Personal
- 4. No menu Action, vá para All Tasks > Advanced Operations > Enroll On Behalf Of...
- 5. No assistente Certificate Request, clique em Next na tela Before You Begin
- 6. No assistente Certificate Request, clique em Next na tela Select Certificate **Enrollment Policy**
- 7. Na tela Select Enrollment Agent Certificate, clique em Browse e selecione o certificado de assiantura (ver Figura 73), pressione OK e Next

Select Enrollment Agent Certificate	
You need an enrollment agent certificate in order to sign a certificate reque	st on behalf of other users. Click
browse to locate a signing certificate, and then click Next.	
Signing certificate	Browse
Windows Security	
Confirm Certificate	
Confirm this certificate by clicking OK. If this is not the correct certificate, click Cancel.	
SmartEnroll Issuer: FIMCA	
Valid From: 5/2/2011 to 5/1/2013 Click here to view certificate prope	
	Cancel
OK Cancel	
	aaa-021019

Na página Request Certificates, selecione o modelo de certificado Smart Card User ou Smart Card Logon

e expanda a opção **Details** e pressione Properties (ver Figura 74).

Request Certificates			
You can request the following click Next.	types of certificates. Select the certific	rates you want to request, and then	
1			-
QA FIM SCU 2048	i) STATUS: Availab	Details A	
The following options de	cribe the uses and validity period that	t apply to this type of certificate:	
Key usage:	Digital signature		
Application policies:	Smart Card Logon		
. Francis Francis	Client Authentication		-
	Secure Email		=
Validity period (days):	365	[] Descutors	
		Properties	+
Show all templates			
Learn more about certificates			
		Next Car	- Insu
			ica

Na página **Certificate Properties** na aba **Private Key**, expanda **Cryptographic Service Provider**. Se o **Athena CSP** estiver em uso, selecione **Athena CSP (Encryption)** e pressione **OK** e **Next** (ver <u>Figura 75</u>). Se o **Athena Minidriver** estiver em uso, selecione **Microsoft Base Smart Card Cryptographic Service Provider** e pressione **OK** e **Next**
### Manual do usuário do IDProtect client

	Certification Authority	
Cryptog	raphic Service Provider	^
A CSP is a certificate Select cry	a program that generates a public and private key pair used in many e-related processes. ptographic service provider (CSP):	
Micro	soft Strong Cryptographic Provider (Encryption)	*
Athen	a ASECard Crypto CSP (Encryption)	
Micro	soft Base Cryptographic Provider v1.0 (Encryption)	m
Micro	soft Base DSS and Diffie-Hellman Cryptographic Provider (Encryption)	
Micro	soft Base Smart Card Crypto Provider (Encryption)	
Micro	soft DH SChannel Cryptographic Provider (Encryption)	-
Eearn mor	e about <u>private key</u>	
	OK Cancel A	pply

Na tela **Select User**, clique em **Browse** e selecione o usuário que necessite de um smart card (ver <u>Figura 76</u>). Pressione **OK** e **Enroll**.

© NXP Semiconductors N.V. 2016. Todos os direitos

### Manual do usuário do IDProtect client

Select a user		
-		
To request a certificate on behalf of another us example, Firstname Lastname, username, or do	er, enter the formal name or domain na main\username.	ame of that user. For
User name or alias:		
		Browse
Select User	2 ×	
Select this object type:		
User	Qbject Types	
From this location:		
Athenadom2.com	Locations	
Enter the object name to select (examples):		
Bob Gordon (bob@Athenadom2.com)	Qheck Names	
		Cancel
	the second se	cance

Quando solicitado (ver Figura 77), insira o smart card.

card reader to save the new certi	ificate.
If the smart card is already in the reader, re smart card and insert it again.	move the
Note: This certificate cannot be saved on the card used to sign the certificate request.	he smart
(	Cancel

O diálogo **IDProtect PIN Entry** ou **Fingerprint Verification** é exibido. Insira o PIN quando solicitado e pressione **Verify**. O User PIN padrão para cartões NXP é **111111.** Alternativamente, posicione o dedo sobre o sensor e prossiga com a verificação biométrica. No caso de um cartão PIN, utilize o diálogo exibido (ver <u>Figura 78</u>).

### Manual do usuário do IDProtect client

IDProtect#08500003	2D1E2340		
Enter your User PIN			-
6			
KNEMER KN	_		
			2
Change PIN after verifica	tion		
	Cancel	Verify	
THE	100 C		

Dependendo de qual política **Change PIN at first use** tiver sido seleciona em **Format Profile**, o diálogo **IDProtect PIN Entry** poderá ser exibido. O usuário é solicitado a inserir e confirmar o novo **User PIN**. Para formatações padrão, consulte a <u>Seção 4</u> <u>"Parâmetros de formatação padrão"</u>.

O usuário também pode marcar a caixa **Change PIN after verification** para que receba uma solicitação de mudança de PIN. Em ambos os casos, o diálogo mostrado na <u>Figure</u> <u>79</u> é exibido.

IDProtect#0A54	001235156947
Enter your User	PIN
Current User PIN	****
New User PIN	
Confirm new PIN	
1	Close Change
	aaa-021025

Insira o novo PIN e confirme-o, e o cadastro será iniciado.

Para emitir um smart card para um usuário adicional ou **Fechar** para sair do assistente de cadastro, selecione **New User**.

© NXP Semiconductors N.V. 2016. Todos os direitos

### Manual do usuário do IDProtect client

Certificat	e Installation Resul	enrolled and installed on this computer.	
Active Di	irectory Enrollment Poli	cy .	
@ Smarte	card User	STATUS: Succeeded	Details 🛩
		Nex	t user Close

© NXP Semiconductors N.V. 2016. Todos os direitos

### Manual do usuário do IDProtect client

### 14. Fazendo Logon com um NXP PIN smart card

Para habilitar o logon às plataformas a seguir usando um smart card e um PIN de usuário, registre um cartão na estação de cadastro de certificados para smart card. O cadastro é descrito na <u>Seção 13</u>:

Windows XP Windows Vista Windows 7 Windows 8 Windows 8.1 Windows 10 Server 2003 Server 2008 Windows Server 2008 R2 Windows Server 2012 R2

Se o PC do cliente tiver sido devidamente configurado com um leitor de smart card, a caixa de diálogo Welcome to Windows exibe a tela de logon do smart card (ver Figura <u>81</u>). Este é o provedor de credenciais para smart card padrão da Microsoft.



Para logon com smart card, insira o smart card no leitor. Quando solicitado, insira o User PIN para fazer o logon ao PC e à rede (ver <u>Figure 82</u>).

### Manual do usuário do IDProtect client



Ao usar o Windows 8, Windows 8.1, Windows 10 ou Windows Server 2012/2012 R2, os ícones do provedor de credenciais de smart card são diferentes (ver Figura 83).



© NXP Semiconductors N.V. 2016. Todos os direitos

### 15. Fazendo logon com o smart card habilitado com biometria NXP

Ao usar um cartão NXP habilitado com biometria para fazer logon ao Microsoft Windows, o diálogo mostrado na in <u>Figura 84</u> será exibido. Para fazer logon à estação de trabalho, o usuário deverá fornecer a impressão digital correta.

Place your finger on the sensor	
*	Select biometric reader BSPAPI_0
)r enter your User PIN :	Change PIN after verification
	Cancel Verify

# 16. Configurações de política para comportamento de remoção de smart card

É possível definir diferentes políticas para definir o comportamento de remoção de smart card. Para definir as políticas, políticas de segurança de domínio devem ser definidas no controlador de domínio.

Clique em Start > Settings > Control Panel >> Administrative Tools >> Domain Security Policy. A caixa de diálogo mostrada na <u>Figura 85</u> é exibida.



Fig 85. Seleção de opções de segurança de domínio

Expanda Local policies e selecione Security options. Escolha smart card removal behavior na janela à direita. Selecione e escolha Properties para acessar a caixa de diálogo mostrada na Figura 86.

Há três opções disponíveis. Escolha uma das opções e clique em **OK** para definir o comportamento de remoção do smart card para o domínio.

### Manual do usuário do IDProtect client

Security Policy Setting			1
Interactive logon: Sr	mart card remov	al behavior	
Define this policy setting			
No Action Lock Workstation Force Logoff			
	OK	Cancel	
-			aaa-021031

Ao usar o Windows 8 (ou posterior) ou Windows Server 2012 (ou posterior), a política de remoção de smart card deve ser definida usando GPO em:

Computer configuration>Windows settings>Local policies>Security options>Smart card removal behavior.



UM10947 Manual do Usuário

Manual do usuário do IDProtect client

Habilite o serviço **Smart Card Removal Policy** também no console de gestão de serviços (Services.mmc).

Smart Card Removal Policy	Name	Description	Status	Startup Type	Log On As	
Start the service Description: Allows the system to be configured to lock the user desktop upon smart card removal.	Secondary Logon Secury Socket Tunneling Protocol Ser- Secury Socket Tunneling Secury Center Senor Monitoring Service Server Shall Handware Detection Skype Updater	Enables starting processes under alternate credentials. If this ser- Provides support for the Secure Socket Tunneling Protocol (SS- The starturg of this service signals of the services that the Securit, The WSCSVC (Windows Security Centrel) service monitors and r Monitors various services in order to expose data and adapt to i Supports file, print, and named-pipe sharing over the adapt to i Provides notifications for AuxoPlay hardware events: Enables the detection, download and installation of updates for-	Running Running Running Running Running	Manual Manual Automatic Automatic (D., Manual (Trig., Automatic Automatic Automatic	Local Syste Local Service Local Syste Local Service Local Service Local Syste Local Syste Local Syste	
	G Smart Card	Manages access to smart cards read by this computer. If this se	Running	Automatic (T	Local Service	
	Smart Card Removal Policy	Allows the system in be configured to tock the user desktop up-		Manual	Lincel System	
	SNMP Trap Software Protection Spot Verifier SSDP Discovery Soll Image Acquisition Events Storage Service	Receives tap messages generated by local or remote Simple NL- Enables the download, initialition and enforcement of digital 6 Virifies potential file system comptions. Discovers networked devices and services that use the SSDP dis. Laurches applications associated with thil image acquisition e Enforces group policy for storage devices:	Running	Manual Automatic (D., Manual (Trig., Manual Manual Manual (Trig.,	Local Service Network S Local Syste Local Service Local Syste Local Syste	
						222-02103

**Nota:** Se a Política de Segurança não for definida no domínio, o usuário individual poderá fazer a escolha em base local de estação de trabalho a estação de trabalho.

© NXP Semiconductors N.V. 2016. Todos os direitos

UM10947

Rev. 2 – 26 de Setembro de 2016

### 17. Bloqueio e desbloqueio de um PC após remoção do cartão

### Para bloquear um computador com Windows:

Se definido corretamente, conforme descrito na <u>Seção 16</u>, a remoção do cartão do leitor bloqueia um computador com Windows. A tela de indicação de bloqueio mostrada na <u>Figura 89</u> é exibida.



### Para desbloquear um computador com Windows:

Pressione **ALT+CTRL+DeI**, selecione o provedor de credenciais NXP ou provedor de credenciais de smart card da Microsoft. Reinsira o smart card. Insira o **User PIN** e clique em **OK** para tornar a fazer logon.



**Nota:** No **Windows Vista e versões posteriores**, pode ser necessário iniciar o serviço Smart Card Removal Policy para ativar a tela de bloqueio após remoção do cartão.

© NXP Semiconductors N.V. 2016. Todos os direitos

### 18. Opções avançadas de instalação por linha de comando

### 18.1 Parâmetros de instalação

### IBOOT

Valor padrão: 0 – Reinicialize se necessário após a instalação. Por exemplo, quando suporte Gina estiver instalado.

Quando definido em 1 - não há reinicialização após a

instalação. Linha de comando: Boot de instalação - Não

reinicializar após instalação siexec.exe /i

"[PathToMsi]\IDProtectClient.msi" UBOOT=1 UBOOT

Valor padrão: 0 - Reinicialização após instalação.

Quando definido em 1 – não há reinicialização após a instalação. Esta opção oferece uma oportunidade de instalar um novo cliente IDProtect antes da reinicialização. Também permite logon por smart card com o cliente IDProtect instalado na próxima inicialização.

Linha de comando: Boot de Desinstalação - Não reinicializar após desinstalação.

msiexec.exe /i "[PathToMsi]\IDProtectClient.msi" UBOOT=1

### 18.2 Instalação dos componentes do IDProtect

### **NSTALLMANGEPIN**

Valor padrão: 1

Parâmetro opcional que define se o IDProtect Manage PIN será instalado. Quando

definido como 0 - não instalar

Quando definido como 1 - instalar

Linha de comando: Não instalar o IDProtect Manage PIN.

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " INSTALLMANGEPIN=0

### INSTALLMONITOR

Valor padrão: 1

Parâmetro opcional que define se o IDProtect Monitor será instalado. Quando

definido como 0 - não instalar

Quando definido como 1 - instalar

Linha de comando: Instalar ASECard Monitor.

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " INSTALLMONITOR=1

© NXP Semiconductors N.V. 2016. Todos os direitos

### Manual do usuário do IDProtect client

#### **INSTALLRDPSERVER**

Valor padrão: 0

Executar o setup sem instalar os dois serviços que habilitam suporte ao servidor RDP.

#### Linha de comando:

Executar setup sem instalação do servidor RDP.

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " INSTALLRDPSERVER=0

#### **INSTCITRIXCLIENT**

Valor padrão: 0

Quando é definido como 1 - O cliente Citrix é instalado, os componentes do Citrix são instalados.

Linha de comando: Instalar componentes do Citrix.

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " INSTCITRIXCLIENT=1

### **SHOWICONTRY**

Valor padrão: 1

Definir a entrada de registro para controlar a aparência do ícone da bandeja do sistema. Por padrão é instalado e definido como 1.

Linha de comando: Não mostrar o ícone na bandeja.

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " SHOWICONTRY=0

#### **INSTALLPERSO**

Valor padrão: 1

Parâmetro opcional que define se o IDProtect Format será instalado.

Quando definido como 0 - não instalar

Quando definido como 1 - instalar

Linha de comando: Não instalar o IDProtect Format.

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " INSTALLPERSO=0

#### **INSTALLMANAGER**

Valor padrão: 1

Parâmetro opcional que define se o IDProtect Manager será instalado. Quando

definido como 0 - não instalar

Quando definido como 1 - instalar

Linha de comando: Não instalar o IDProtect Manager.

Todas as informações fornecidas neste documento estão sujeitas a isenções legais.

© NXP Semiconductors N.V. 2016. Todos os direitos

### Manual do usuário do IDProtect client

### Valor padrão: 1 Parâmetro opcional que define se o IDProtect Options será instalado. Quando definido como 0 - não instalar Quando definido como 1 - instalar Linha de comando: Não instalar o IDProtect Options. msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " INSTALLOPTIONS=0 MOZILLASUPPORT

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " INSTALLMANAGER=0

Quando definido como 0 – Não adiciona suporte PKCS#11 ao Firefox. Quando definido como 1 – Adiciona suporte PKCS#11 ao Firefox.

### Linha de comando:

**INSTALLOPTIONS** 

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " MOZILLASUPPORT=1

### DEFNXPCSP

Valor padrão: 0

Quando definido como 1 – Athena CSP é o provedor CAPI padrão.

Quando definido como 0 – Microsoft Base CSP é o provedor CAPI padrão.

### Linha de comando:

Definir Microsoft como provedor CAPI padrão msiexec.exe /i "<msi-

name>" DEFNXPCSP=0

### INSTALLDOC

Valor padrão: 1

Executar setup sem instalar documentos.

### Linha de comando:

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " INSTALLDOC=0

### INSTADMINPINTOOL

Valor padrão: 0.

Parâmetro opcional que define se o IDProtect Admin PINTool será instalado.

 $\ensuremath{\textcircled{}^{\circ}}$  NXP Semiconductors N.V. 2016. Todos os direitos

### Manual do usuário do IDProtect client

Quando definido como 0 - Não instala o IDProtect Admin PINTool.

Quando definido como 1 – Instala o IDProtect Admin

PINTool.

Linha de comando:

Instalar IDProtect Admin PINTool msiexec.exe /i "<msi-

name>" INSTADMINPINTOOL=1

#### **INSTBIOCOMP**

Valor padrão: 0.

Quando definido como 1 - Instala os componentes biométricos.

Quando definido como 0 - Não instala os

componentes biométricos.

### Linha de comando:

Instalar componentes biométricos

msiexec.exe /i "<msi-name>" INSTBIOCOMP=1

### INSTALLBIOTOOL

Valor padrão: 1

Quando definido como 1- Instala ferramenta de cadastro.

Quando definido como 0- Não instala ferramenta de cadastro

biométrico.

### Linha de comando:

Não instala ferramenta de cadastro biométrico

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " INSTALLBIOTOOL=0

### **INSTALLPRECISELIBS**

Valor padrão: 2

Quando definido como 1 - Instala bibliotecas Precise (deve usar

INSTBIOCOMP=1 também). Quando definido como 2- Não instala bibliotecas

Precise.

### Linha de comando:

Não instala bibliotecas Precise

### **ASESENSBSPS**

UM10947

. Todas as informações fornecidas neste documento estão sujeitas a

### Manual do usuário do IDProtect client

msiexec.exe /i "<msi-name>" INSTALLPRECISELIBS=2

### para x64:

msiexec.exe /i "IDProtectClientx64.msi" INSTALLPRECISELIBS=1

#### para x86:

msiexec.exe /i "IDProtectClient.msi" INSTALLPRECISELIBS=1

Padrão: 0x10 (bsapi).

### Valores HEX:

0x01 - precise

0x05 - precise + validity

0x09 - precise + Nitgen

0x10 - bsapi

0x11 - bsapi + precise

0x18 - bsapi + Nitgen

0x0D - precise + Nitgen + validity

### Manual do usuário do IDProtect client

0x15 - bsapi + precise + validity

0x1D - bsapi + precise + validity + Nitgen

Linha de comando: bspapi + precise.

msiexec.exe /i "<msi-name>" ASESENSBSPS=11

### INSTALLCCID

Valor padrão: 0.

Quando definido como 0 - Não instala o driver CCID

Quando definido como 1 - Se não for Windows XP,

instala o driver CCID A instalação do driver CCID é

para o Windows XP apenas. Linha de comando:

msiexec.exe /i "<msi-name>" INSTALLCCID=1

#### Combinação de parâmetros

Os parâmetros podem ser combinados em uma única linha de comando.

Linha de comando: Não instalar IDProtect Options, instalar IDProtect Manager e definir suporte a Check Point.

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " INSTALLOPTIONS=0 INSTALLMANAGER=1 CPSUPPORT=1

### **INSTALLDRIVERS**

Valor padrão: 1

Executar o setup sem opção de instalação de dispositivo de leitor de smart card NXP. As janelas para instalação dos leitores de smart card NXP e tokens não são exibidas.

Linha de comando: Executar setup sem instalação dos drivers.

msiexec.exe /i "<msi-name>" INSTALLDRIVERS=0

### <u>INSTKSP</u>

Valor padrão: 1

Configura a associação de registro Calais para KSP para Athena ou

Microsoft. Quando definido como 0 - Define Microsoft como provedor

KSP

Quando definido como 1 – Define Athena como provedor KSP

Quando definido como 2 – Oculta esta funcionalidade no diálogo de configuração personalizado. (Apenas a partir da versão 6.26.11 em diante)

Linha de comando: Definir Microsoft como provedor KSP padrão

. Todas as informações fornecidas neste documento estão sujeitas a

msiexec.exe /i "<msi-name>" INSTKSP=0

### 18.3 Parâmetros par configuração do IDProtect VERIFICATIONTYPE

Valor padrão: Nenhum – Se o parâmetro não for definido, o tipo de verificação de chave de registro não é instalado.

Quando é definido, a chave de registro é instalada com o valor

definido. Linha de comando: Tipo de verificação - é instalado e

definido como 10 (h) msiexec.exe /i "[PathToMsi]\IDProtectClient.msi"

#### VERIFICATIONTYPE=10 Valores:

Card - 0x10Biometric Only - 0x3PIN Only - 0x1Both - 0x4

### DELCERTSTORE

Valor padrão: 0

Quando é definido como 1, sempre que um cartão certificado for excluído do armazenamento, é excluído do cartão também.

Linha de comando: Se for excluído do armazenamento raiz, define o certificado a ser excluído do cartão.

#### msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " DELCERTSTORE=1

### DELCARDCERT

Valor padrão: 1

Para todos os valores diferentes de 0, sempre que um certificado for excluído do cartão, ele será excluído do armazenamento raiz também.

Linha de comando: Não excluir certificado do armazenamento mesmo se tiver sido excluído do cartão.

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " DELCARDCERT=0

### **LOADROOT**

Valor padrão: 0

Se existir no smart cards, define a entrada de registro para upload do certificado raiz para o armazenamento raiz. Por padrão, não é carregado ao armazenamento do certificado.

Linha de comando: Configurar raiz de carga para fazer upload do certificado no armazenamento raiz.

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " LOADROOT=1

### Manual do usuário do IDProtect client

### **CPSUPPORT**

Valor padrão: 0

Configurar entrada de registro para suportar Check Point. Por padrão, o Check Point não é suportado.

Linha de comando: Definir suporte ao Check Point.

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " CPSUPPORT=1

### **CERTPOLICY**

Valor padrão: NENHUM

Definir uma entrada de registro para controle do número de dias que os certificados são mantidos em um armazenamento de certificado, antes de serem excluídos. Por padrão é instalado e definido string vazio.

Linha de comando: Política de certificado para 5 dias.

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " CERTPOLICY=5

### **ORIGBIOFINGPRINT**

Valor padrão: 1

Definir se uma imagem em tempo real das impressões digitais é mostrada no diálogo ou apenas uma imagem estática de uma impressão digital "padrão".

Linha de comando: Mostrar imagem da impressão digital em tempo real.

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " ORIGBIOFINGPRINT=1

### ALLOWUNLOCK

Valor padrão: 1

Nome do valor de registro: allowUnlock

Quando definido como 1 - não permite

desbloqueio dinâmico. Quando definido

como 2 - permite desbloqueio dinâmico.

Linha de comando: Permitir bloqueio

desbloqueio dinâmico. msiexec.exe /i "<msi-

name>" ALLOWUNLOCK =2 CREATEPUKEY

Valor padrão: 0

Nome do valor de registro: enablePublicCreate

Quando definido como 0 - Não aplicado, criado sem esta

opção.

### Manual do usuário do IDProtect client

Quando definido como 1 - Permite criar uma chave

pública no cartão. Linha de comando:

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " CREATEPUKEY=1

### ENASTROPROT

Valor padrão: 0

Nome do valor de registro: enableStrongProtected

Quando definido como 0 - Não aplicado, criado sem esta opção.

Quando definido como 1 - Permite a criação onde DS é suportado, de outra forma

falhando a operação. Linha de comando: Permite criar onde DS é suportado, de

outra forma falhando a operação. msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi "

### ENASTROPROT =1

### VERIFPOLICY

Valor padrão: 0

Nome do valor de registro:

DSVerificationPolicy Quando definido como

0 - O PIN não é armazenado em cache

Quando definido como 1 – O PIN é

armazenado com prompt. Quando

definido como 2 - PIN armazenado

Linha de comando: PIN armazenado.

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " VERIFPOLICY =2

### DSSYNCPOLICY

Valor padrão: 0

Nome do valor de registro: DSSynchOption

Quando definido como 0 - Não sincroniza o usuário e

DS PINs. Quando definido como 1 - Sincroniza o

usuário e DS PINs.

Linha de comando: Sincroniza o usuário e DS PINs.

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " DSSYNCPOLICY =1

### Manual do usuário do IDProtect client

### **DNSPREFIXNAME**

Valor padrão: Nenhum.

Nome do valor de registro: DSNamePrefix

Linha de comando: DS name Prefix

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " DNSPREFIXNAME ="DS Name.."

### DSCREATIONPOLICY

Valor padrão: 0

Nome do valor de registro:

DSCreationPolicy Quando definido

como 0 - Política explícita.

Quando definido como 1 – Política de assinatura

Linha de comando: Política de assinatura

msiexec.exe /i "[PathToMsi]\ IDProtectClient.msi " DSCREATIONPOLICY =1

### **CERTPROP**

Valor padrão: 2

Quando definido como 0 – Desabilita

propagação do certificado. Quando definido

como 1 - Habilita propagação do certificado.

Quando definido como 0 – Não define nenhum valor para propagação de certificado – deixa a propagação do certificado como está.

Linha de comando: Habilita propagação do

certificado . msiexec.exe /i "<msi-name>"

CERTPROP=1 Chaves de registro relacionadas

ao parâmetro CERTPROP:

- Windows XP e Windows Server 2003.
  - [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\ScCertProp]"Enabled"=dword:[CERTPROP]
- Windows Vista e versões posteriores:
  - [HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CertProp]"CertPropEna bled"=dword:[CERTPROP]

### Manual do usuário do IDProtect client

### USEAUTOPIN

Valor padrão: 0.

Quando definido como 1 – O uso do modo de PIN de usuário automático tira o valor de PIN de IPSEC\_P Quando definido como 0 – Não usa o

modo de PIN de usuário automático.

Linha de comando: Definir senha como

1111 msiexec.exe /i "<msi-name>"

### USEAUTOPIN=1111 AUTOPASSWORD

Valor padrão: Vazio.

Quando UseP11AutoPIN == 1, é o valor de PIN do usuário usado no modo automático. Quando UseP11AutoPIN == 0, este valor não é usado.

### Linha de comando: Definir senha como 1111

msiexec.exe /i "<msi-name>" AUTOPASSWORD=1111

### **LIFTFINGER**

Valor padrão: 0.

Quando definido como 0 - Não força o usuário a levantar o dedo antes de autenticá-lo. Quando definido como 1 - Força o usuário a levantar o dedo antes de autenticá-lo.

Linha de comando: Força o usuário a levantar o dedo antes de autenticá-lo.

msiexec.exe /i "<msi-name>" LIFTFINGER=1

### **MNGRHIDEDEL**

Valor padrão: 0.

Quando definido como 0 - Não oculta opção Delete do

administrador. Quando definido como 1 - Oculta opção

Delete do administrador.

Linha de comando: Ocultar opção Delete do administrador

msiexec.exe /i "<msi-name>" MNGRHIDEDEL=1

### Manual do usuário do IDProtect client

### FRIENDNAMEMON

Valor padrão: 0.

Quando definido como 0 – Não adiciona atributo de nome amigável ao armazenamento do CKA\_LABEL. Quando definido como 1 – Adiciona atributo de nome amigável ao armazenamento do CKA\_LABEL. **Linha de comando:** Monitor adiciona nome amigável.

msiexec.exe /i "<msi-name>" FRIENDNAMEMON=1

#### FRIENDNAMECSP

Valor padrão: 0.

Quando definido como 0 – Não Grava o nome amigável como o label (CKA\_LABEL) Quando definido como 1 – Grava o nome amigável como o label (CKA\_LABEL)

Linha de comando: CPS grava o nome amigável como label.

msiexec.exe /i "<msi-name>" FRIENDNAMECSP=1

### **CERTMONLOAD**

Valor padrão: 0. Esta sinalização é apenas para Windows

Vista e sistemas operacionais posteriores. Quando

definido como 0 – O monitor não carrega certificados

para armazenar. Quando definido como 1 - O monitor

carrega certificados para armazenar.

Linha de comando:

msiexec.exe /i "<msi-name>" CERTMONLOAD=1

#### **HIDEADMINCARD**

Valor padrão: 0.

Quando definido como 0 – Não oculta a opção do

cartão Use Admin Quando definido como 1 -

Oculta a opção do cartão Use Admin

Linha de comando: Ocultar opção do cartão

Use Admin msiexec.exe /i "<msi-name>"

### HIDEADMINCARD=1 DISDSCHA

### Manual do usuário do IDProtect client

Valor padrão: 0.

Quando definido como 0 – Não desabilita a opção **change ds pin** no IDProtect PINTool. Quando definido como 1 – Desabilita a opção **change ds pin** no IDProtect PINTool.

Linha de comando: Desabilita a opção change ds pin no IDProtect PINTool.

msiexec.exe /i "<msi-name>" DISDSCHA=1

### DISABLELABEL

Valor padrão: 0.

Quando definido como 0 – Não desabilita a opção change label no IDProtect Manager. Quando definido como 1 – Desabilita a opção label no ASECard Manager.

Linha de comando: Desabilita a opção label no ASECard Manager.

msiexec.exe /i "<msi-name>" DISABLELABEL=1

### **KEEPARCVCERT**

Valor padrão: 0

Nome do valor de registro: KeepArchivedCerts

Quando é definido como 1 – sempre que um certificado for marcado como arquivado, ele é marcado como arquivado no cartão também. Caso contrário, é excluído do cartão.

Linha de comando: Definir certificado como

arquivado msiexec.exe /i "<msi-name>"

### KEEPARCVCERT=1 USESYSDEF

Valor padrão: 0

Quando definido como 1 – significa que o uso dos parâmetros de LOCAL\_MACHIN serão forçados.

Quando definido como 0 – usa os parâmetros de CURRENT\_USER e se não forem encontrados, usa os parâmetros de LOCAL\_MACHINE.

Linha de comando: Força o uso de

LOCAL\_MACHINE msiexec.exe /i "<msi-name>"

### USESYSDEF=1 ASEHIDECHANGEPIN

### Manual do usuário do IDProtect client

Valor padrão: 0

Quando definido como 0 – Muda o PIN após a caixa de verificação ser exibida. Quando definido como 1 – Muda o PIN após a caixa de verificação ser ocultada. **Linha de comando:** Ocultar caixa de verificação de mudança de pin.

msiexec.exe /i "<msi-name>" ASEHIDECHANGEPIN=1

#### SHOWAPPVER

Valor padrão = 0

Quando é definido como 0 – Nenhuma versão applet exibida no Manager Tool.

Quando é definido como 1 – No caso de Java card, exibe a versão do applet no Manager Tool.

Linha de comando: Exibe versão do applet.

msiexec.exe /i "<msi-name>" SHOWAPPVER=1

#### **FORMATYPE**

Controla o tipo de mensagem seguro (com base em RSA ou ECC) para Laser cards. Se for 0, é com base em RSA (padrão). Se for um, com base em ECC.

Valor padrão: 0

Quando é definido como 0 -

com base em RSA Quando é

definido como 1 - com base em

ECC Linha de comando:

msiexec.exe /i "<msi-name>" FORMATYPE=1

### 18.4 Parâmetros MSIEXEC

#### GUI em japonês

msiexec.exe /i "<msi-name>" TRANSFORMS=1041.mst

#### **GUI em inglês**

msiexec.exe /i "<msi-name>" TRANSFORMS=1033.mst

gb – interface básica apenas.

gn – nenhuma interface. Se inicialização for necessária, não há implicações.

### Manual do usuário do IDProtect client

### Linha de comando:

msiexec.exe /i "<msi-name>" /qb INSTALLOPTIONS=0 INSTALLMANAGER=1 CPSUPPORT=1

msiexec.exe /i "<msi-name>" /qn INSTALLOPTIONS=0 INSTALLMANAGER=1 CPSUPPORT=1

### 18.5 Usando privilégios elevados para não administradores

Para instalar em uma máquina que não seja parte do grupo administrativo, a máquina deve ser configurada para executar instalações com privilégios elevados. Três sinalizações devem ser configuradas por meio do gpedit.msc: Sempre instalar com privilégios elevados (máquina e seções de usuário) e habilitar controle de usuário sobre instalações na seção da máquina. A última sinalização é necessária para permitir que o usuário utilize sinalizações com as configurações.

### Manual do usuário do IDProtect client

### 19. Informações Legais

### 19.1 Definições

Rascunho 0 O documento é uma versão de rascunho apenas. O conteúdo ainda sob revisão interna e sujeito a aprovação formal, que pode resultar em modificações ou adições. A NXP Semiconductors não dá quaisquer representações ou garantias quanto à precisão ou completude das informações aqui inclusas e não se responsabilizará pelas consequências do uso de tais informações.

### 19.2 Renúncia

Garantia e responsabilidade limitada – Acredita-se que as informações neste documento sejam precisas e confiáveis. No entanto, a NXP Semiconductors não dá quaisquer representações ou garantias, expressas ou implícitas quanto à precisão ou completude de tais informações e não se responsabilizará pelas consequências do uso de tais informações. A NXP Semiconductors não se responsabiliza pelo conteúdo deste documento se disponibilizada por uma fonte de informações fora da NXP Semiconductors.

Em nenhum caso a NXP Semiconductors se responsabilizará por danos indiretos, incidentais, punitivos, especiais ou consequenciais (incluindo – sem se limitar a – lucros perdidos, economias pedidas, interrupção de negócios, custos relacionados à remoção ou substituição de produtos ou taxas de retrabalho), sejam ou não causados por negligência, garantia, violação contratual ou qualquer outra teoria legal.

Não obstante quaisquer danos que o cliente possa incorrer por qualquer motivo, a responsabilidade agregada e cumulativa da NXP Semiconductors para com o cliente pelos produtos descritos aqui se limitará de acordo com os Termos e condições de venda comercial da NXP Semiconductors.

**Direito de fazer mudanças** – A NXP Semiconductors se reserva ao direito de fazer alterações à informações publicadas neste documento, incluindo sem limitação especificações e descrições de produtos, a qualquer momento, sem notificação prévia. Este documento se sobrepõe e substitui todas as informações disponibilizadas antes de sua publicação.

Adequação de uso – Os produtos da NXP Semiconductors não são projetados, autorizados ou garantidos como ideais para uso no suporte à vida, sistemas críticos À vida ou de segurança à vida, ou equipamentos com o mesmo propósito, nem em aplicações onde falha ou mau funcionamento de um produto da NXP Semiconductors possa resultar em lesões, morte ou danos à propriedade ou ao meio ambiente. A NXP Semiconductors e seus fornecedores não aceitam responsabilização pela inclusão e/ou uso dos produtos da NXP Semiconductors em tais equipamentos ou aplicações e, portanto, tal inclusão e/ou uso é de risco do cliente.

**Aplicações** – As aplicações aqui descritas para qualquer um destes produtos têm propósito meramente ilustrativo. A NXP Semiconductors não faz representação ou garantia de que tais aplicações serão ideais para o uso especificado sem testes ou modificações adicionais.

Os clientes são responsáveis pelo projeto e operação de suas aplicações e produtos que usam os produtos da NXP Semiconductors, e a NXP Semiconductors não aceita responsabilidade por qualquer assistência com aplicações ou projeto do produto do cliente

É responsabilidade do cliente determinar se o produto da NXP Semiconductors é ideal e está de acordo com as aplicações e produtos planejados, assim como aplicação e uso planejado de terceiros. Os clientes devem oferecer salvaguardas apropriadas de design e operação para minimizar os riscos associados às suas aplicações e produtos.

A NXP Semiconductors não aceita responsabilidade relacionada a qualquer defeito, dano, custos ou problemas que possam ocorrer devido a fraqueza ou defeito nas aplicações ou produtos do cliente, ou a aplicação ou uso por terceiros. O cliente é responsável por fazer todos os testes necessários para as aplicações e produtos do cliente que utilizam produtos da NXP Semiconductors, a fim de evitar defeito de aplicações e produtos ou na aplicação ou uso por terceiros. A NXP não aceita responsabilidade a este respeito.

**Controle de exportação** – Este documento, assim como os itens descritos aqui, podem estar sujeitos a regulamentações de controle de exportação. A exportação pode exigir autorização prévia das autoridades competentes.

**Produtos de avaliação** – Este produto é disponibilizado da forma como é e sem falhas para fins de avaliação apenas. A NXP Semiconductors, seus afiliados e fornecedores expressamente se isentam de todas as garantias, sejam elas expressas, implícitas ou estatutárias, incluindo, mas não se limitando a garantias implícitas de

não infração, comercialização e adequação a um propósito particular. Todo o risco relacionado a qualidade ou proveniente do uso ou desempenho deste produto permanece por conta do cliente.

Em nenhum caso a NXP Semiconductors, suas afiliadas ou fornecedores serão responsáveis por quaisquer danos especiais, indiretos, consequenciais, punitivos ou incidentais (incluindo, mas não se limitando a danos por perda de negócio, interrupção de negócios, perda de uso, perda de dados ou informações, e similares) resultantes da incapacidade de uso do produto, seja com base em negligência, responsabilidade estrita, violação contratual, violação de garantia ou qualquer outra teoria, mesmo se aconselhado sobre a possibilidade de tais danos.

Não obstante quaisquer danos que o cliente possa incorrer por qualquer motivo (incluindo, mas nãose limitando a todos os danos mencionados acima e todos os danos diretos ou gerais), toda a responsabilidade da NXP Semiconductors, suas afiliadas e seus fornecedores e remediação exclusiva do cliente de todos eles devem se limitar a danos incorridos pelo cliente com base em confiança razoável até maior que a quantia paga pelo cliente pelo produto ou cinco dólares (US\$ 5). As limitações, exclusões e isenções se aplicam ao máximo permitido pela lei aplicável, mesmo se qualquer remediação falhar seu propósito essencial.

**Traduções** – Uma versão que não esteja em inglês do documento serve apenas como referência. A versão em inglês prevalecerá em caso de discrepância entre as versões traduzidas e em inglês.

### 19.3 Marcas registradas

Aviso: Todas as marcas, nomes de produtos, nomes de serviços e marcas registradas aqui mencionadas são propriedade de seus respectivos proprietários.

### 20. Tabelas

Tabela 1 Parâmetros pricipais ASEDefault e MDDefault.8

### 21. Figuras

Fig 1.	Configuração do IDProtect Client5
Fig 2.	Assistente de instalação do IDProtect Client5
Fig 3.	Seleção de funcionalidade de instalação do
•	IDProtect Client6
Fia 4.	Janela do IDProtect Format11
Fig 5	Aviso do IDProtect Monitor 12
Fig 6	lanela do IDProtect Format – detalhes
rig ö.	do cartão
Eia 7	lanala da IDProtect Format, gostão do
Fig 7.	partil
	Janala da IDDrataat Farmat Lista da parfia 14
FIQ 0.	Janeia do IDProtect Format – Lista de peris 14
Fig 9.	Manage Profile – aba General
Fig 10.	Manage Profile – aba User PIN
Fig 11.	Valor do User PIN17
Fig 12.	Regras de complexidade de User PIN17
Fig 13.	Manage Profile – perfil Admin PIN gestão
Fig 14.	Valor padrão de Admin PIN19
Fig 15.	Tipo de verificação Admin PIN20
Fig 16.	Manage Profile – assinatura digital21
Fig 17.	Janela do IDProtect Format24
Fig 18.	Aviso do IDProtect Monitor24
Fig 19.	Detalhes do cartão IDProtect ISO MoC
Fig 20.	Detalhes do cartão IDProtect Precise MoC25
Fig 21	Lista de perdis IDProtect 26
Fig 21.	Manage Profile – aba General 27
Fig 22.	Manage Profile and User DIN 29
Fig 23.	Managa Profile – aba User FIN
Fig 24.	Degree de esterilevide de DIN
Fig 25.	Regras de complexidade PIN
Fig 26.	Manage Profile – perfil Admin PIN gestao
Fig 27.	Valor padrao de Admin PIN
Fig 28.	Manage Profile – assinatura digital
Fig 29.	Cadastro do primeiro dedo no IDProtect
Fig 30.	Indicação de dedo sendo cadastrado
	no IDProtect
Fig 31.	IDProtect exibindo impressão digital sendo
	cadastrada37
Fig 32.	Verificação de impressão digital IDProtect
Fig 33.	Cadastro do próximo dedo no IDProtect
Fig 34.	Cadastro biométrico realizado com sucesso
0	no IDProtect
Fia 35.	IDProtect Manage PIN
Fig 36.	Janela da ferramenta IDProtect PIN
Fig 37	Janela de mudanca do IDProtect PIN 40
Fig 38	Diálogo de confirmação de mudança
i ig 50.	do IDProtect PIN 40
Eia 20	Compo do entrado do mudenco do
FIG 39.	DProtect DIN
F:- 40	IDPIOLECLIPIN
Fig 40.	Campo de entrada de novo PIN de
	usuario no IDProtect42
Fig 41.	Ferramenta IDProtect PIN43
Fig 42.	Campo de entrada de IDProtect PUK43
Fig 43.	Aviso de entrada incorreta no IDProtect44
Fig 44.	Link de desbloqueio do IDProtect Card44
Fig 45.	Desbloquear cartão bloqueado no IDProtect45
Fig 46.	Solicitação de Admin Card no IDProtect45
Fig 47.	Solicitação de PIN de Admin Card46
Fig 48	Solicitação de novo PIN de usuário no IDProtect 46
Fig 49	Verificação de novo PIN de usuário no IDProtect47
	,

Fig 50.	Novo PIN de usuário válido no IDProtect	17
Fig 51.	IDProtect Admin PINTool	18
Fig 52.	Mudança de Admin PIN no IDProtect	18
Fig 53.	Confirmação de mudanca de PIN no IDProtect4	19
Fig 54.	Ferramenta de cadastro biométrico IDProtect4	19
Fig 55.	IDProtect Manager	50
Fig 56	Verificação do IDProtect	51
Fig 57	Certificados e Chaves do IDProtect Manager	52
Fig 58	Certificados e Chaves Expandidas do IDProtect 4	53
Fig 50.	Container padrão de config. do IDProtect	50
Fig 60	Tola de IDProtect Options	57
Fig 60.	Configuração do orguivo do log Current Lloor do	זכ
FIG 61.	Deroto et	- 0
	Oppfigure a final de la gravita de la gravit	00
FIG 62.	Configuração de arquivo de log Local Machine do	)
<b>-</b> :	IDProtect	59
Fig 63.	IDProtect Options – aba Digital Signature	50
Fig 64.	IDProtect Options – aba Advanced	52
Fig 65.	IDProtect Options – login de Adminstrador - diálo	go
	Tela inicial6	53
Fig 66.	IDProtect Options – Tela de solicitação	
	de Admin PIN	53
Fig 67.	IDProtect Options – Tela de entrada de	
-	Admin PIN	54
Fig 68.	IDProtect Options – Solicitação de novo	
0	User PIN e Tela de confirmação	64
Fia 69.	IDProtect Options – login de Adminstrador -	
	diálogo tela de fechamento	35
Fig 70	IDProtect Options – tela de logon do	
i ig 70.	Administrador	36
Fig 71	IDProtect Options – Tela de bloqueio	
i ig 7 i.	de smart card	36
Fig 72	IDProtect Options – Tela de desbloqueio	0
1 19 72.	de smart card	37
Eia 72	Tolo do confirmação do codostro do cortificado	70
Fig 73.	Tela de collinimação de caudstro de certificado	74
FIG 74.		70
Fig 75.	Tela de seleção CSP	2
Fig 76.		13
Fig //.	Tela de solicitação de inserção de smart card	/3
Fig 78.	l ela de verificação de PIN de usuario	
	de smart card	74
Fig 79.	Tela de entrada de novo PIN de usuário	
	de smart card	74
Fig 80.	Tela de status de cadastro de certificado	
	em smart card	75
Fig 81.	Tela de boas vindas de logon por smart card7	76
Fig 82.	Tela de logon por smart card	77
Fig 83.	Tela de entrada por smart card	77
Fig 84.	Tela de verificação de logon por smart card	78
Fig 85.	Seleção de opção de segurança de domínio	79
Fig 86.	Configurações de política de seguranca	-
	de domínio	30
Fig 87.	Editor de política de grupo local	30
Fig 88	Console de gestão de servicos	31
Fig 89	Indicação de sistema bloqueado	32
Fig 90.	Logon do sistema	32
- ig 30.	Logon do sistema	

### Manual do usuário do IDProtect client

### 22. Conteúdo

1	Introdução 3	
2	Pré-requisitos 3	
3	IDProtect cliente for Windows 4	
3.1	Instalação	
3.1.1	Instalação do IDProtect client para suporte de PIN cards	4
3.1.2	Instalação do IDProtect client para suporte 6 de BIO cards	
3.1.3	Instalação do cliente IDProtect em Citrix e ambiente de servidor terminal Windows	
4	Parâmetros de formato padrão	
41	Formatação rápida do IDProtect card 9	
4.2	Cartões habilitados com RSA 4096	
5	Uso da ferramenta de formatação IDProtect em	
-	PIN cards	
5.1	Descricão geral1	1
5.2	Uso da ferramenta IDProtect Format	1
521	Formatação de um cartão PIN .	3
5.3	Gestão de Perfi.	ĺ
5.3.1	Manage Profile - aba General .	5
5.3.2	Manage Profile - User PIN tab 16	3
5.3.3	Manage Profile – aba Admin PIN	
5.3.4	Manage Profile – aba Digital Signature	
6	Uso da ferramenta de formatação IDProtect em	
-	Bio Cards23	
6.1	Descrição geral23	
6.2	Uso da ferramenta IDProtect Format	
6.2.1	Formatação de um Bio Card	;
6.3	Gestão de perfis27	,
6.3.1	Aba General27	,
6.3.2	Aba User PIN para Bio Cards	
6.3.3	Aba Admin PIN	
6.3.4	Aba Digital Signature	
6.4	Formatação de um Bio Card	
6.4.1	Cadastro de impressões digitais	
7	Mudanca ou desbloqueio do PIN do usuário39	
7.1	Mudanca de PIN de usuário a partir	
	do IDProtect Monitor na Bandeia do Sistema39	
72	Mudanca de PIN de usuário a partir da	
	ferramenta de PIN no IDProtect Card Manager40	)
7.3	Mudanca de User PIN a partir do IDProtect	
	Format	
7.4	Mudança de User PIN a partir da caixa de	
	diálogo IDProtect PIN41	
7.5	Desbloqueio de um PIN de usuário bloqueado 42	
7.6	Desbloqueio de um PIN de usuário bloqueado	
	com o uso de um cartão de administrador44	
8	Mudanca de Admin PIN48	;
-	,	

9 10	Ferramenta de cadastro biométrico	49 50
10 1	Configuração do recipiente padrão	53
11	Opcões do IDProtect	55
11.1	Aba General	55
11.2	Technical Support tab	56
11.2.1	Arquivos de log	58
11.3	Aba Digital Signature	60
11.4 11.4	Aba Avançado	61
11.4.1 12		62
12 12 1	PINs Adicionais	68
12.2	Associação de uma chave privada com	00
	um PIN de assinatura digital PIN de assinatura	.68
12.3	Sincronização de um PIN de usuário	
	com um PIN de assinatura PIN	. 69
12.4	Armazenando o PIN de assinatura em cachê	69
13	Certificado de Usuário/Logon de Smart Card Cadastro	70
14	Fazendo logon com um smart card de PIN NXP	76
15	Fazendo logon com o smart card habilitado	
	com biometria NXP	.78
16	Configurações de política para comportamer de remoção de smart card	nto .79
17	Bloqueio e desbloqueio de um PC	
	após remoção do cartão	.82
18	Opções avançadas de instalação por linha de comando	e .83
18.1	Parâmetros de instalação	.83
18.2	Instalação dos componentes do IDProtect	.83
18.3	Parâmetros par configuração do IDProtect	.88
18.4	Parâmetros MSIEXEC	.95
18.5	Utilização de privilégios elevados para	05
10		
101	Dofiniçãos	.90
19.1	Renúncia	96
19.3	Marcas registradas	.96
20	Tabelas	97
21	Figuras	.97
22	Conteúdo	.98

Tenha em atenção que os avisos importantes relativos a este documento e produtos aqui descritos foram incluídos na secção "Informações legais".

© NXP Semiconductors N.V. 2016. Todos os direitos reservados.

Para mais informações, visite: http://www.nxp.com Para endereços dos escritórios de vendas, enviar e-mail para salesaddresses@nxp.com

s, enviar e-mail para salesaddresses@nxp.com Data de emissão: 26 de setembro de 2016. Identificador do

documento: UM10947