

# WatchKey

WatchKey USB PKI Token  
Manual de Instalação e Operação

Versão Windows

**Watchdata**

Copyright 2011 Watchdata Technologies.

Todos os direitos reservados.

É expressamente proibido copiar e distribuir o conteúdo presente neste manual sem prévia autorização escrita da Watchdata Technologies.

Microsoft, Windows, ActiveX, Word, PowerPoint, Internet Explorer, IE, Windows NT, Windows XP, e .NET são marcas registradas ou marcas da Microsoft Corporation.

Apple, Macintosh e são marcas da Apple Computer.



# Introdução

À medida que o desenvolvimento da tecnologia de redes permite que mais e mais pessoas possam se comunicar on-line, a segurança relacionada ao sigilo e a autenticação dessa comunicação torna-se mais relevante.

O WatchKey garante a segurança em transações online ao utilizar uma solução baseada em chip criptográfico de última geração, garantindo portabilidade, segurança, interoperabilidade e integração com diversos softwares e plataformas existentes.

A segurança proporcionada pelo WatchKey é baseada em certificados digitais e chaves criptográficas assimétricas, garantindo facilidade de uso e os mais altos níveis de segurança para assinatura digital. O WatchKey é usado como portador de chaves e certificados, além de processar o algoritmo de criptografia através de seu processador interno.

A comunicação com o computador através da interface USB garante suporte a aplicações que incluem internet banking, assinatura digital, assinatura de emails, certificados, entre outros.

Este manual descreve a instalação e a operação básica do WatchKey.

Maiores detalhes podem ser obtidos em:

<http://www.watchdata.com/brazil/watchkey/index.htm>

# Plataformas suportadas pelo WatchKey

Sistemas operacionais suportados pelo WatchKey:

## **Windows**

- |                               |                    |
|-------------------------------|--------------------|
| • Windows 2000 SP4            | Português / Inglês |
| • Windows XP SP2 e superiores | Português / Inglês |
| • Windows Vista 32/64         | Português / Inglês |
| • Windows 7 32/64             | Português / Inglês |
| • Windows 8 32/64             | Português / Inglês |

## **Linux (Kernel 2.4 e 2.6)**

- |                |                    |
|----------------|--------------------|
| • OpenSuse     | Português / Inglês |
| • Ubuntu       | Português / Inglês |
| • Debian 32/64 | Português / Inglês |
| • Fedora 32/64 | Português / Inglês |

## **MacOS**

- |                             |                    |
|-----------------------------|--------------------|
| • MacOS X 10.5              | Português / Inglês |
| • MacOS X 10.6 e superiores | Português / Inglês |
| • MacOS X 10.7 e superiores | Português / Inglês |
| • MacOS X 10.8 e superiores | Português / Inglês |

# Instalação do WatchKey

## COMO INSTALAR O WatchKey

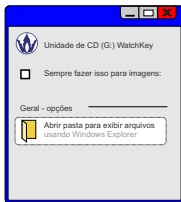
Ao inserir o WatchKey, o computador irá reconhecer o dispositivo e instalará seus drivers automaticamente.

No Windows Vista, Windows 7 e Windows 8, uma janela se abrirá automaticamente com a opção de abrir as pastas que contém o software do WatchKey. No Windows XP e Windows 2000, a janela com as pastas será aberta diretamente.

Esta versão do WatchKey está disponível para Windows, Mac e Linux.

Os drivers também podem ser encontrados para download no endereço:

<http://www.watchdata.com/brazil/watchkey/index.htm>

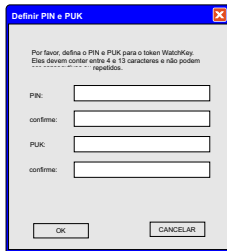


# Ferramentas de Administração do WatchKey

## MODIFICAR PIN E PUK PADRÃO

De forma a preservar a segurança dos dados armazenados no dispositivo, o token WatchKey irá solicitar que o PIN e o PUK padrão, respectivamente '88888888' e '12345678', sejam modificados.

Assim, enquanto os valores não forem modificados, não será possível utilizar as funções do token WatchKey.



The image shows a Windows-style dialog box titled "Definir PIN e PUK" (Set PIN and PUK). The title bar is blue with a red close button on the right. The main area has a light gray background. At the top, there is a small text block: "Por favor, defina o PIN e PUK para o token WatchKey. Eles devem conter entre 4 e 13 caracteres e não podem ser iguais." Below this, there are four input fields arranged in two pairs. The first pair is for the PIN, with labels "PIN:" and "confirma:" to the left of the respective text boxes. The second pair is for the PUK, with labels "PUK:" and "confirma:" to the left of the respective text boxes. At the bottom of the dialog, there are two buttons: "OK" and "CANCELAR" (Cancel).

# Ferramentas de Administração do WatchKey

## VISÃO GERAL

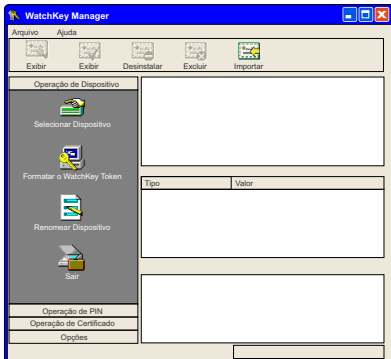
As Ferramentas de Administração do WatchKey são utilizadas para realizar as seguintes operações:

**Dispositivo:** Seleção, inicialização e mudança de nome do dispositivo.

**PIN:** Verificação, modificação e desbloqueio de PIN.

**Certificado:** Visualização, instalação, remoção e importação de certificados.

**Opções:** Informações sobre o dispositivo



# Ferramentas de Administração do WatchKey

## VISÃO GERAL

### Dispositivo



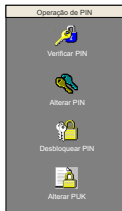
Permite selecionar outro dispositivo quando há mais de um WatchKey presente.

Permite inicializar o dispositivo para uso com certificados.

Permite modificar o nome do dispositivo.

Encerra o programa.

### Gerenciamento de PIN



Permite a verificação de PIN para impedir o acesso e o uso do dispositivo por usuários não autorizados.

Modificar o PIN.

Desbloquear o PIN através do PUK.

Modificar o PUK.



# Ferramentas de Administração do WatchKey

## VISÃO GERAL

### Certificados



Visualizar os certificados do WatchKey.

Instalar o certificado selecionado.

Desinstalar o certificado selecionado.

Remover o certificado do WatchKey.

Permite a importação de um certificado para o WatchKey.

### Opções



Apresenta informações do dispositivo como Nome, ATR, versão e espaço disponível.

Apresenta relatório de instalação.

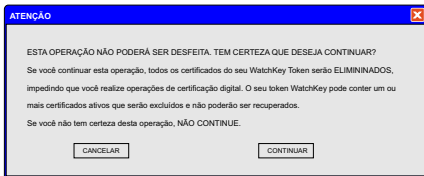
Restaura o dispositivo para o estado original de fábrica. Todos os certificados e chaves são apagados.

# Ferramentas de Administração do WatchKey

## DISPOSITIVO

### Formatar e Inicializar Dispositivo

Esta opção permite apagar o WatchKey, retornando-o a seu estado inicial, e removendo todos os certificados, PIN e PUK nele armazenados.



**Passo 1:** Selecione o dispositivo, clique Formatar. É necessário fornecer o PUK do WatchKey. Atenção: Esta operação não pode ser desfeita.

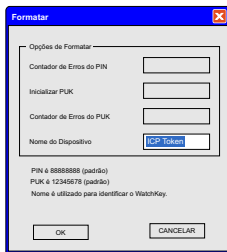


# Ferramentas de Administração do WatchKey

## DISPOSITIVO

### Inicializar Dispositivo

**Passo 2:** Se o PUK for autenticado, o dispositivo será inicializado. Digite o novo nome do dispositivo.



The image shows a Windows-style dialog box titled "Formatar" (Format) with a red 'X' icon in the top right corner. The dialog has a tab labeled "Opções de Formatar" (Formatting Options). Inside the tab, there are four input fields: "Contador de Erros do PIN" (PIN Error Counter), "Iniciar PUK" (Start PUK), "Contador de Erros do PUK" (PUK Error Counter), and "Nome do Dispositivo" (Device Name). The "Nome do Dispositivo" field contains the text "ICP Token". Below the input fields, there is a section with default values: "PIN é 88888888 (padrão)" (PIN is 88888888 (default)), "PUK é 12345678 (padrão)" (PUK is 12345678 (default)), and "Nome é utilizado para identificar o WatchKey." (Name is used to identify the WatchKey.). At the bottom of the dialog are two buttons: "OK" and "CANCELAR" (Cancel).

**Contador de erros de PIN:** Define o máximo de tentativas que podem ser realizadas com o PIN incorreto antes de bloquear o WatchKey.\*

**Contador de erros do PUK:** Define o máximo de tentativas que podem ser realizadas com o PUK incorreto antes de bloquear o WatchKey.\*

**Nome:** Rótulo atribuído ao dispositivo.

\* as opções dos contadores não podem ser alteradas.

# Ferramentas de Administração do WatchKey

## DISPOSITIVO

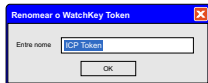
### Inicializar Dispositivo

Após inicializar o dispositivo com sucesso, o WatchKey retorna a seu estado original e todos os certificados são removidos.



### Modificar nome do dispositivo

Permite que o usuário modifique o nome do dispositivo.



# Ferramentas de Administração do WatchKey

## GERENCIAMENTO DE PIN

### Verificar PIN

A verificação do PIN é realizada para confirmar a identidade do usuário do token e impedir o uso não autorizado do dispositivo.



O PIN deve conter no mínimo 4 e no máximo 16 caracteres, podendo incluir letras e / ou números. Os caracteres não podem ser repetidos nem consecutivos.

# Ferramentas de Administração do WatchKey

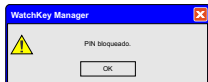
## GERENCIAMENTO DE PIN

### Verificar PIN

Caso o PIN digitado seja incorreto, o sistema irá solicitar que o mesmo seja digitado novamente e irá informar quantas tentativas ainda restam.



Caso o limite máximo de cinco tentativas de PIN seja atingido, o WatchKey irá bloquear o acesso ao PIN.

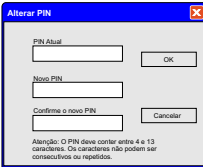


# Ferramentas de Administração do WatchKey

## GERENCIAMENTO DE PIN

### Modificar PIN

Esta função permite modificar e personalizar um PIN de acordo com o usuário.



The dialog box has a blue title bar with the text "Alterar PIN" and a close button. It contains three input fields: "PIN Atual", "Novo PIN", and "Confirma o novo PIN". To the right of the first field is an "OK" button, and to the right of the second and third fields is a "Cancelar" button. At the bottom, there is a warning message in Portuguese: "Atenção: O PIN deve conter entre 4 e 13 caracteres. Os caracteres não podem ser consecutivos ou repetidos."

Alterar PIN

PIN Atual  OK

Novo PIN

Confirma o novo PIN  Cancelar

Atenção: O PIN deve conter entre 4 e 13 caracteres. Os caracteres não podem ser consecutivos ou repetidos.

Por questões de segurança, o usuário deve personalizar um novo PIN imediatamente após a formatação.

Caso o contador máximo de tentativas de PIN seja atingido, o WatchKey irá bloquear o acesso ao PIN.

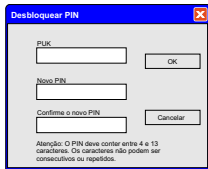
# Ferramentas de Administração do WatchKey

## GERENCIAMENTO DE PIN

### Desbloqueio de PIN

Conforme descrito anteriormente, o WatchKey pode ter seu acesso bloqueado por questões de segurança. Para que ele seja desbloqueado, é necessário utilizar o PUK.

Com o PUK correto, é possível definir um novo PIN.



**Desbloquear PIN**

PUK

Novo PIN

Confirme o novo PIN

Atenção: O PIN deve conter entre 4 e 13 caracteres. Os caracteres não podem ser consecutivos ou repetidos.



# Ferramentas de Administração do WatchKey

## OPERAÇÕES COM CERTIFICADOS

As Ferramentas de Administração do WatchKey permitem ao usuário realizar cinco operações com certificados: visualizar, instalar, desinstalar, excluir e importar.

### **Visualizar certificados**

Ao acessar o Menu de Operações com Certificados, os certificados disponíveis no WatchKeyToken serão listados na janela superior direita. Para acessar informações do certificado selecionado, clique no botão Exibir Certificado.

### **Instalar Certificados**

Selecione o certificado que desejado e clique em 'Instalar Certificado'.

### **Desinstalar Certificado**

Selecione o certificado a ser desinstalado e clique em 'Desinstalar Certificado'. Importante: Esta operação somente pode ser realizada pelo usuário que tenha o registro do certificado.

### **Excluir Certificado**

Esta função permite a remoção de certificados armazenados no WatchKey e associados ao usuário local.

### **Importar Certificado**

Permite a importação de certificados para o token. Caso o certificado esteja criptografado, será necessário digitar a senha de acesso do certificado.

# Ferramentas de Administração do WatchKey

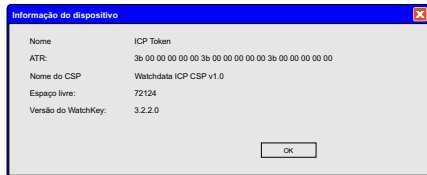
## OPÇÕES

Informações sobre o dispositivo podem ser obtidas em Opções.



Informações relativas ao dispositivo incluem: ATR, nome do provedor do serviço de criptografia, versão de hardware e espaço disponível.

É possível também verificar um relatório com pleto de todos arquivos instalados pelo WatchKey em seu sistema.



### Restaurar o dispositivo as configurações de fábrica

Esta opção permite a inicialização do dispositivo, restaurando todas as configurações originais de fábrica. Todos os certificados, PIN, PUK e parâmetros do token serão reinicializados.

# Ferramentas de Administração do WatchKey

## APENDICE 1: GLOSSARIO

**PKI:** (Public Key Infrastructure (PKI) é um conjunto de hardware, software, políticas e procedimentos necessários para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais. A PKI promove um arranjo que vincula chaves públicas com respectivas identidades de usuários por meio de uma autoridade certificadora (AC). Para cada usuário, a identidade do usuário, a chave pública, a sua ligação, as condições de validade e outros atributos são feitos mais seguros em certificados de chave pública emitidos pela AC.

**AC:** (Autoridade Certificadora) tem a responsabilidade de publicar e gerenciar todos os certificados, sendo o núcleo da PKI e responsável pelo gerenciamento de certificados digitais, distribuição e revogação.

**Digital Certificate:** É uma sequência de códigos digitais que utiliza uma assinatura digital para ligar uma chave pública com informações de identidade a uma chave privada. O Certificado digital é emitido por uma AC confiável e contém: número de série, assunto, algoritmo de assinatura, emissor, tempo de validade, o uso da chave pública, entre outros. Pode ser usado para enviar e-mail seguro, acesso a sites seguros, pagamento online, declaração de impostos e transações eletrônicas seguras..

**Server Certificate:** É um certificado emitido por uma AC e é instalado em um servidor para garantir a autenticidade dos serviços.

# Ferramentas de Administração do WatchKey

## APENDICE 1: GLOSSÁRIO

**Root Certificate:** O certificado raiz é um certificado público não assinado ou um certificado auto-assinado que identifica a AC. O certificado raiz é parte inicial em um esquema de infra-estrutura de chave pública. Os certificados digitais são verificados usando uma cadeia de confiança da AC.

**Client Certificate:** É o certificado emitido por uma AC e é instalado no computador do usuário e acessado pelos serviços de segurança e criptografia.

**SSL:** (Secure Sockets Layer) Protocolo que fornece confidencialidade e integridade na comunicação entre um cliente e um servidor, através do uso de criptografia.

**PKCS#11:** Define uma plataforma independente para tokens criptográficos, tais como Hardware Security Modules (HSM), smart cards e alguns tipos de objeto de criptografia (RSA chaves, X.509 certificados, DES / Triple DES chaves, etc) e todas as funções necessárias para utilizar, criar / gerar, modificar e excluir esses objetos.

**CSP:** Um provedor de serviços de criptografia (CSP) é o programa que executa serviços de autenticação, codificação e criptografia a que aplicativos Windows têm acesso através da interface de programação de aplicativo Microsoft Cryptography (CryptoAPI).

# **Watchdata**

## **Sobre a Watchdata Technologies**

A Watchdata Technologies é uma dos líderes mundiais em soluções para autenticação digital, identificação, e pagamentos para governos e empresas. Com presença em mais de 50 países, a Watchdata atua com projetos de segurança digital nas áreas bancária, de telecomunicações, de transporte, saúde e utilidade pública. Maiores informações no site:

[www.watchdata.com](http://www.watchdata.com)

***Watchdata***