



DATAKEY®

Datakey CIP Integration & Configuration Guide

CIP version 4.7

For Check Point users

Copyright notice

© 2002 Datakey Inc. All rights reserved.

No part of this document may be reproduced or retransmitted in any form or by any means electronic, mechanical, or otherwise, including photocopying and recording for any purpose other than the purchaser's personal use without written permission of Datakey Inc.

Trademarks

Datakey is a registered trademark and Datakey CIP is a trademark of Datakey Inc. Check Point, FireWall-1, VPN-1, VPN-1 SecuRemote, and OPSEC are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. Microsoft is a registered trademark of Microsoft Corporation. Windows and Windows NT are registered trademarks of Microsoft Corporation. Netscape and Netscape product names are trademarks of Netscape Communications Corporation. All other brand names and product names used in this manual are trademarks, registered trademarks, or trade names of their respective holders.

Print history

Date	Software Release	Description
December 2002	Datakey CIP V4.7	Initial release of the Datakey CIP Integration & Configuration Guide: For Check Point users

TABLE OF CONTENTS

Datakey CIP Integration and Configuration Guide	1
Overview	2
Benefits	4
Requirements	4
About your certificate authority	5
About Check Point VPN-1/FireWall-1	5
Configuring your local and remote workstations	6
Install Datakey CIP and a Datakey card reader	6
Enable the Delete On Removal option	6
Install the CA root certificate	7
Requesting and installing a certificate and key pair	8
Configuring and using SecuRemote on remote workstations ...	9
Using Datakey smart cards in a Check Point environment	11
Securing your VPN	11
Securing your email messages	12
Securing your Web transactions	13
Datakey CIP Desktop functions	13
Viewing digital credentials on your smart card	15
Troubleshooting	16
Appendix A	
Configuring a CA for use in a Check Point environment	17
Create a new CA	17
Configure the initial jurisdiction	18
Specify settings for the new CA	19
Create a new extension profile	20
Configure jurisdiction to use new extension profile	21
Configure CRL options	22
Download the CA's root certificate to diskette	23

Appendix B	Configuring your Check Point VPN-1/FireWall-1	25
	Create a workstation object	25
	Create an LDAP Account Unit object	26
	Create a CA instance	26
	Generate a Certificate Signing Request	27
	Approve the request on your local RSA Keon CA	29
	Load the FireWall-1 certificate from diskette	29
	Configure the IKE properties	29
	Define a TCP service	30
	Create an external user group	31
	Configure and install an initial security policy	31

Datakey CIP Integration and Configuration Guide

This document provides a brief overview on how smart cards from Datakey Inc. provide security for digital credentials in a Check Point™ environment. In addition, this document describes the basic steps necessary to use Datakey® smart cards with your Check Point products.

This document contains the following topics:

- “Overview”
- “Benefits”
- “Requirements”
- “About your certificate authority”
- “About Check Point VPN-1/FireWall-1”
- “Configuring your local and remote workstations”
- “Using Datakey smart cards in a Check Point environment”
- “Viewing digital credentials on your smart card”
- “Troubleshooting”

Note: *The integration and configuration portions of this document assume that Datakey CIP™ is already installed on your workstation(s). See the **Datakey CIP User’s Guide** for installation instructions.*

Overview

Datakey Inc. focuses on delivering smart card-based solutions that assure identity and protect the integrity and privacy of data shared over public and private networks. Datakey cryptographic smart cards, client software, desktop applications and card management products enable organizations to reliably identify users and open doors in both the physical and online worlds.

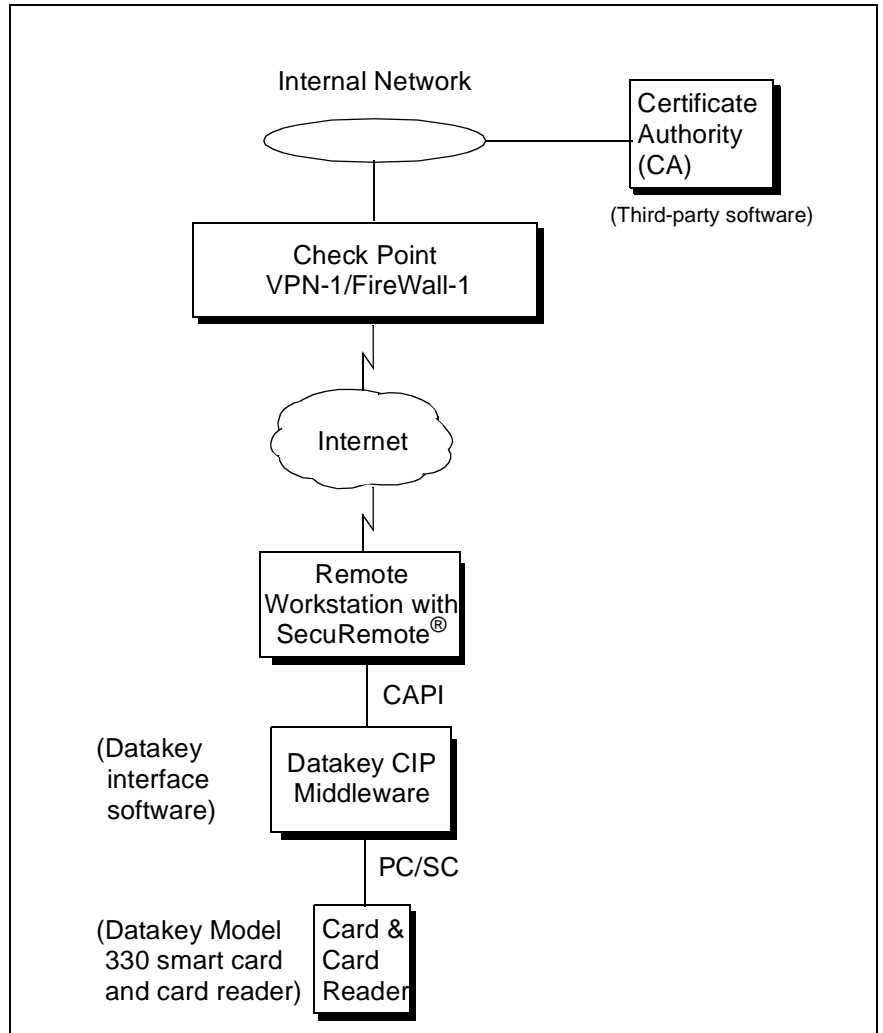
Customers and partners alike rely on Datakey technology in a full range of enterprise applications, including password management, host authentication, Windows log-on, VPN access, Web authorization, desktop security, corporate badge and building access, biometric integration, public key encryption, digital certificates and digital signatures.

One of the systems that can be used in conjunction with Datakey's smart cards is from Check Point. Check Point's FireWall-1® enables enterprises to define and enforce a single, comprehensive security policy that protects all network resources. Its innovative architecture delivers a highly scalable solution that integrates all aspects of network security. Check Point's VPN-1® provides the most comprehensive set of products and technologies for remote access, intranet, and extranet VPNs. VPN-1 software protects the privacy of business communications over the Internet while securing critical network resources against unauthorized access.

While your Check Point software provides ready and trustworthy access to public information, the digital credentials necessary for providing secure connectivity are made more secure with the use of Datakey smart cards. The smart cards enhance your Check Point solution by functioning as portable and secure carriers for your digital credentials. The smart cards protect your digital credentials using *two-factor security*, meaning access to your credentials requires both something that you have (the smart card) and something that is known (a passphrase to access the smart card).

Datakey's smart card technology integrates easily with Check Point software. Once installed and configured, use of the Datakey smart card within a Check Point system is virtually transparent. Figure 1 illustrates how Datakey CIP software and the Datakey smart card/card reader fit seamlessly into your existing Check Point software system.

FIGURE 1. Datakey CIP and Check Point software components



Benefits

Check Point products are able to use public key technology to secure messages and transactions that are exchanged over public data networks. To enhance this security, Datakey smart cards can be used in conjunction with your Check Point software. This enables you to store your unique digital credentials on a Datakey smart card, providing the following benefits:

- Your digital credentials are protected by two-factor security: something that you have (the smart card) and something that is known (a passphrase). The passphrase is entered via an easy-to-use interface.
- Your digital credentials cannot be copied from the smart card as it might from your workstation's hard disk.
- The smart card is much more tamper-resistant than your workstation; the card automatically locks itself after a predefined number of failed access attempts.
- If you misplace your smart card, you know it and can take preventive actions; if someone copies your digital credentials off your computer you won't know it and you won't know to take preventive actions.
- Your digital credentials become portable; they can travel with you.
- You can use the smart card to securely store additional information such as biometric information, etc.
- The smart card can serve other purposes, including providing physical access to buildings, serving as an employee ID card, etc.
- The smart card is extremely easy to use.

Requirements

To use Datakey smart cards in a Check Point environment you need the following:

- Access to a certificate authority (CA) that can be used to generate digital certificates for your firewall and for each individual user
- Check Point firewall and Check Point VPN software that is configured to interact with and support local and remote workstations
- Datakey CIP software installed and configured on your local and remote workstations
- A Datakey card reader installed on each workstation
- Check Point SecuRemote® software on your remote workstations

About your certificate authority

A certificate authority (CA) is used to create and manage digital credentials, including certificates, public keys, and private keys. Digital credentials are mandatory in order to operate securely in today's networked environment. They are used to authorize a user to secure applications before that user is allowed to conduct business. Credentials are also used to encrypt data before it is transmitted across vulnerable public networks or across the Internet.

There are many respected certificate authority vendors available today. It is therefore impossible to provide details on how to configure and use your specific CA. Appendix A, however, does provide some examples of using an RSA Keon CA in a Check Point environment.

The basic tasks associated with a CA in your Check Point environment are:

- Configure your CA
- Download a copy of the CA's root certificate to your Check Point firewall
- Download a copy of the CA's root certificate to your individual workstations
- Generate certificates for your firewall and for each individual user

About Check Point VPN-1/FireWall-1

Check Point's VPN-1/FireWall-1 provides the framework for one of the most widely used security platforms available today. FireWall-1 is a stateful inspection firewall that protects your enterprise. It enables you to define and enforce a single, comprehensive security policy that protects all your network resources. VPN-1 adds to this by enabling secure site-to-site connectivity. This enables your users to work from remote or mobile workstations without exposing valuable data to harm.

Passing secure network traffic across a Check Point-based network requires proper integration and configuration of your VPN-1/FireWall-1. While a complete discussion of this is outside the scope of this document, a synopsis of the steps required to configure Check Point's VPN-1/FireWall-1 is provided in Appendix B.

Once your Check Point VPN-1/ FireWall-1 and your local CA are properly configured, the next step in preparing to pass secure traffic is to configure your workstation(s).

Configuring your local and remote workstations

This section describes the tasks required to prepare your workstations to use Datakey smart cards. The basic steps include:

- Install Datakey CIP software and Datakey card readers
- Enable the Datakey CIP *Delete On Removal* option
- Install the CA root certificate
- Request a user certificate and key pair
- Download and install the user certificate
- Create a new site in SecuRemote (remote workstations only)

Install Datakey CIP and a Datakey card reader

This document assumes that Datakey CIP and a Datakey card reader are already installed on each workstation. If Datakey CIP and/or your card reader are not installed, please see the *Datakey CIP User's Guide* for complete installation instructions.

Enable the *Delete On Removal* option

The *Datakey Auto Cert Registration Utility* automatically registers digital credentials contained on a Datakey smart card with Microsoft Windows and many other desktop applications. If you want the digital credentials to be deleted from the Windows certificate store whenever the smart card is removed from the card reader, perform the following steps:

1. Start the CIP Utilities program by selecting *Start -> Programs -> Datakey CIP -> CIP Utilities*.
2. From within CIP Utilities, select *Options -> Auto Cert Register* and toggle on the *Delete On Removal* option.
A check mark appears when this option is enabled.
3. Exit CIP Utilities by selecting *File -> Exit*.
4. Reboot the workstation.

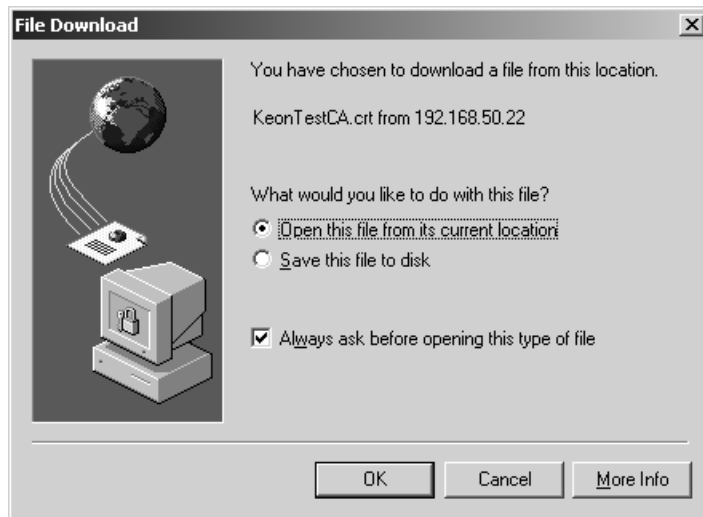
Install the CA root certificate

Each workstation must obtain a copy of your CA's root certificate and store it in the workstation's certificate store. This is necessary so that the workstation can validate the certificates of all the other entities on the network.

One method of installing the CA root certificate is as follows:

1. Start your Web browser (either Internet Explorer or Netscape Communicator).
2. Access the Web site of the certificate authority used by your company (RSA, Verisign, Microsoft, etc.).
3. Follow the directions on the Web site to initiate the CA certificate installation process.
4. When prompted, choose to open the certificate file from its current location.

For example, you might see a window similar to the following:



5. When prompted, install the certificate to your workstation's certificate store.

For example, you might see a window similar to the following:



Requesting and installing a certificate and key pair

Only an authorized certificate authority can issue a certificate. To submit a request for a new user certificate and public/private key pair via the Web, perform the following steps:

Note: This section provides generalized steps for requesting a certificate from a CA. For a more detailed example, please refer to Appendix A.

1. Insert your smart card into the card reader.
2. Start your Web browser (either Internet Explorer or Netscape Communicator).
3. Access the Web site of the certificate authority used by your company (RSA, Verisign, Microsoft, etc.).
4. Follow the directions on the Web site for obtaining a digital certificate.



IMPORTANT! When asked to select the Cryptographic Service Provider name, you must select **Datakey RSA CSP**.

If your request is approved a public and private key pair will be generated and written to your smart card. Please be patient as the key generation process may take several minutes to complete. In addition, you will receive an email message containing instructions for downloading the associated certificate.

Note: You may chose to generate the public/private key pair on your own. In this case the CA uses the public key you provide and generates a certificate that authenticates you as the owner of that public key.

5. Follow the instructions in the email message to download the new certificate and install it on your smart card.

Configuring and using SecuRemote on remote workstations

Check Point VPN-1 SecuRemote enables remote and mobile users to establish secure connections with networks and individual servers by extending your organization's VPN. It protects your critical data by using your personal digital credentials to encrypt the data before it leaves the workstation. In turn, a Datakey smart card is used by each workstation user to protect the valuable digital credentials.

In order to use SecuRemote you must create a new SecuRemote site on each workstation. To create a new site on a workstation, perform the following steps:

1. Start Check Point's VPN-1 SecuRemote by selecting *Start -> Programs -> Check Point VPN-1 SecuRemote -> SecuRemote*.

2. Right-click on the VPN-1 SecuRemote icon located in the system tray. 

3. Select *Open*.

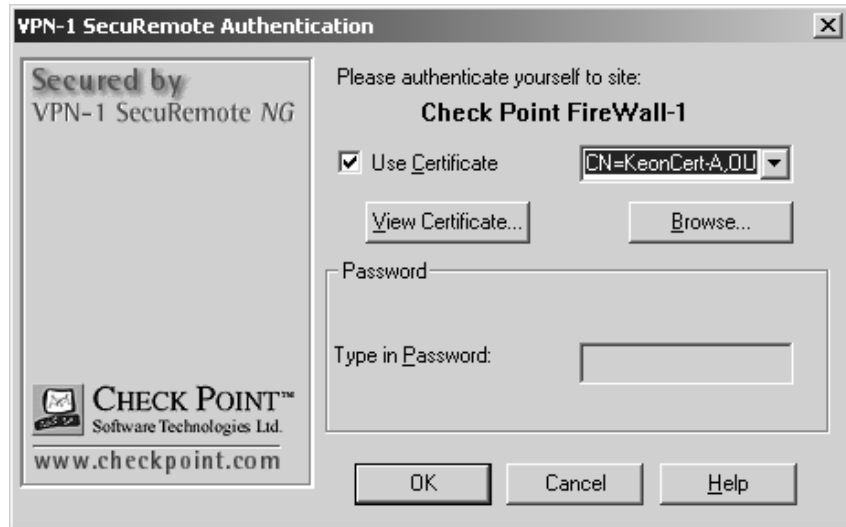
The *VPN-1 SecuRemote* window appears.

4. Select *Sites -> Create New*.

The *Create New Site* window appears.

5. Type a name for the site in the *Nickname* field.
6. Type the external network address of the Check Point firewall in the *Name/IP* field.
7. Click *OK*.

The *VPN-1 SecuRemote Authentication* window appears.



8. Enable the *Use Certificate* checkbox.
9. Select a certificate from the drop-down list.
10. Click *OK*.

The *Cryptographic Service Provider* window appears (it is sometimes “hidden” behind the *VPN-1 SecuRemote* window).

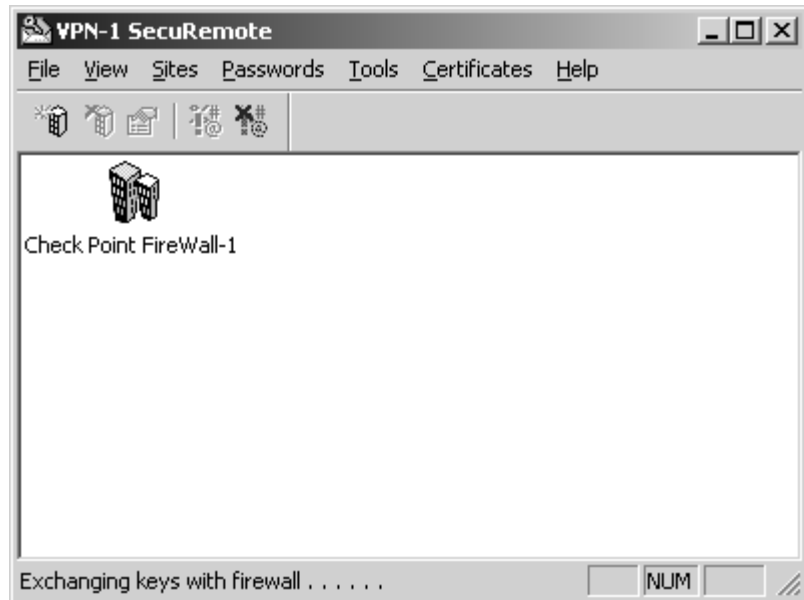


11. Type your smart card’s passphrase, then click *OK*.

The *Verify Certificate* window appears.

12. Verify the information, then either click *OK* to approve the new site or click *Cancel* to abort the process.

When the process is complete a window similar to the following appears:



Using Datakey smart cards in a Check Point environment

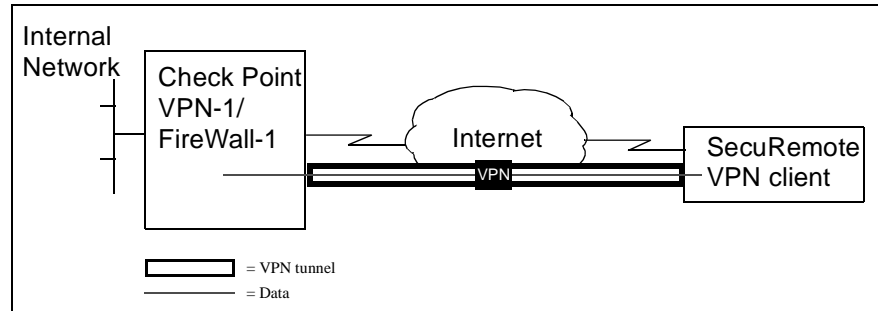
There are many different uses for Datakey smart cards in a Check Point environment. Some of the most common are:

- Securing your VPN
- Securing your email messages
- Securing your Web transactions
- Using Datakey CIP Desktop functions

Securing your VPN

One of the most popular uses of digital credentials in a Check Point environment involves virtual private networks (VPNs). A VPN enables your remote and mobile workstations to use the Internet and other public networks to communicate with

your organization's private network in a secure manner. A "VPN tunnel" can be created between two endpoints that protects the traffic from your remote and mobile workstations even as it travels across public networks. Check Point users will typically use Check Point VPN-1 SecuRemote to help establish the VPN connection (see "Configuring and using SecuRemote on remote workstations" on page 9 for more information).



Digital credentials are one of the many components used when communicating via a VPN tunnel. Your digital credentials are used for authenticating your identity to securely access and conduct business across the VPN. It is therefore important to protect your digital credentials, as the credentials are critical in determining who is an authorized user of the VPN. The preferred way to protect the digital credentials is with a Datakey smart card.

Securing your email messages

Securing email transactions is one of the most common uses of digital credentials. Digitally signing a message assures the email recipient as to the source of a message and protects against someone attempting to change the original content of the message. Encrypting a message prevents unauthorized recipients from reading the message. Today's advanced technology makes it relatively easy to secure your email. All you need to get started are digital credentials that uniquely identify you as a specific user and an email application that is capable of recognizing digital IDs.

Implementing a secure email system within your Check Point environment is fairly straightforward. You simply configure the email program of your choice to use digital credentials when sending and receiving messages. This enables the program to encrypt and digitally sign messages so that the message contents remain confidential and private.

Adding a Datakey smart card into the mix completes the security picture. Not only do the smart cards provide increased security for your digital credentials, they also make the digital credentials portable. In addition, the smart cards are easily integrated into any computing environment, including your Check Point environment. And once they are installed and configured they become virtually transparent to the user.

Securing your Web transactions

Providing secure Web-based services to employees is a must for many organizations. For example, your organization may need to distribute sensitive internal communications using the company Intranet, or it may need to support secure transactions via the Web. In a Check Point system this can be accomplished using a security-capable browser such as Netscape Communicator or Microsoft Internet Explorer. Using this feature enables organizations to support Web-based services by:

- Authenticating the person logging in to Web applications
- Keeping information on a corporate Intranet, or data that is transmitted through a Web service, private—even when the information isn't in use
- Using entitlements to dictate different levels of authorized access to different employees
- Verifying transactions that were made over the Web so that processes requiring signatures can be performed online

Using a Datakey smart card to store each employee's digital credentials does not affect this easy-to-use Web procedure, but it does provide each employee with an important security tool for protecting his/her digital credentials when accessing sensitive material on a Web site.

Datakey CIP Desktop functions

In addition to the traditional services supported by Datakey smart cards, Check Point users can also take advantage of several other functions offered by *Datakey CIP Desktop*. Datakey CIP Desktop is a suite of complementary applications and utilities that work seamlessly with Datakey's field-tested CIP middleware to extend the usability of Datakey smart cards with functions like password management, data storage and smart card configuration. The individual applications and utilities that comprise Datakey CIP Desktop include:

- ❑ **SmartMonitor:** Provides an easy method for launching and controlling your Datakey CIP Desktop components. The CIP Desktop installation process places a SmartMonitor icon into your computer's system tray. When active, you can left-click this icon to use the SmartLogon Auto Fill feature, or you can right-click the icon to quickly access CIP Utilities, the SmartLogon application, the SmartNotes application, or the PassPhrase utility.
- ❑ **SmartLogon:** Enables you to store user name and/or password entries on your Datakey smart card. The program recognizes and remembers the application or Web site associated with each entry. This enables you to log on to an application or Web site with a single click—SmartLogon automatically fills in the correct user name and/or password for you. Using SmartLogon you only need to remember one password—your smart card password—to access any of these Web sites or applications. Your user names and passwords are secure, and you can easily access your favorite Web sites and applications through a single mouse click.
- ❑ **SmartNotes:** SmartNotes enables you to securely store personal notes and data on your Datakey smart card. With SmartNotes your smart card becomes a portable electronic notebook, allowing you to store account information, favorite URLs, personal reminder notes, and other often-used data. And this information is safe, protected by the passphrase needed to activate the smart card.
- ❑ **PassPhrase Utility:** The PassPhrase Utility allows you to update and change the passphrase that protects and activates your smart card. You can also use this utility to issue unblocking codes—passphrases that unlock a smart card should it become blocked by too many incorrect log-in attempts. Unblocking codes are available on Datakey Model 330U smart cards. Finally, the PassPhrase Utility can be used to initiate the Identity PIN on a Datakey Model 330i Identrus smart card and to change both the Identity PIN and the Utility PIN on an Identrus smart card.
- ❑ **Auto Cert Registration Utility:** The Auto Cert Registration Utility automatically registers digital credentials contained on a Datakey smart card with Microsoft Windows and all desktop applications. This provides a quick and easy deployment of your personal digital credentials, enabling instant and transparent use of all Windows applications that require digital credentials.
- ❑ **CIP Utilities:** The Datakey CIP Utilities is an intuitive, easy-to-use program that is used to view and manage Datakey smart cards and the objects contained on the smart cards. The program reports smart card and reader status and can be used for base-level diagnostics. Administrators can configure the functionality and features available for enterprise deployment through an administrative wizard included with CIP Utilities.

Viewing digital credentials on your smart card

To view the certificates and public/private keys stored on your smart card you must use the CIP Utilities program. You can do this by performing the following steps:

1. Start the CIP Utilities program by selecting *Start -> Programs -> Datakey CIP -> CIP Utilities*.
2. In the left pane of the CIP Utilities window, select the certificate or key you wish to view.

Information about the selected item is displayed in the right pane of the CIP Utilities window.

For additional information about the CIP Utilities program, see the *Datakey CIP User's Guide*.

Troubleshooting

There are a few common problems that may occur when using Datakey's smart cards. This section presents solutions to these common problems. If you continue to have problems, please contact the Datakey Technical Support department at 1-888-DATAKEY (1-888-328-2539) or 952-808-2390. You can also email your questions to support@datakey.com.

TABLE 1. Troubleshooting common Datakey CIP problems

Problem	Possible Cause	Solution
Drop-down menu does not allow me to select my smart card during key/certificate generation.	Datakey CIP not installed properly.	Install or re-install Datakey CIP.
	Card reader or smart card is not functioning properly.	See the section titled <i>Troubleshooting Using CIP Utilities</i> in the <i>Datakey CIP User's Guide</i> . Automatic installation installs to only one profile. Ensure that Datakey is installed in your current profile.
When I tried to generate a new key pair or download my new certificate, I received one of the following errors: <ul style="list-style-type: none"> • Unable to generate public/private key pair • The security library has received bad data. You will be unable to connect to this site securely. 	Insufficient room on smart card for new keys/certificate.	If you have no important information already on your smart card, reinitialize the smart card, reboot, and repeat the certification process. If you have existing certificates on your smart card you wish to keep (for instance, to be able to decrypt archived email messages), you should obtain a new smart card, personalize it, and repeat the certification process.
I can't log into my smart card.	Smart card is locked after too many failed password attempts.	Re-initialize the smart card and obtain a new certificate.

Configuring a CA for use in a Check Point environment

This appendix describes the basic steps required to create and configure a CA for use in a Check Point environment. For the sake of example, an RSA Keon® CA is used to illustrate the various steps. The steps you perform on your own CA are likely to be different.

Note: An RSA Keon CA is used here because that was the CA used during testing to achieve Check Point OPSEC certification for Datakey products.

Create a new CA

Using your Web browser, perform the following steps:

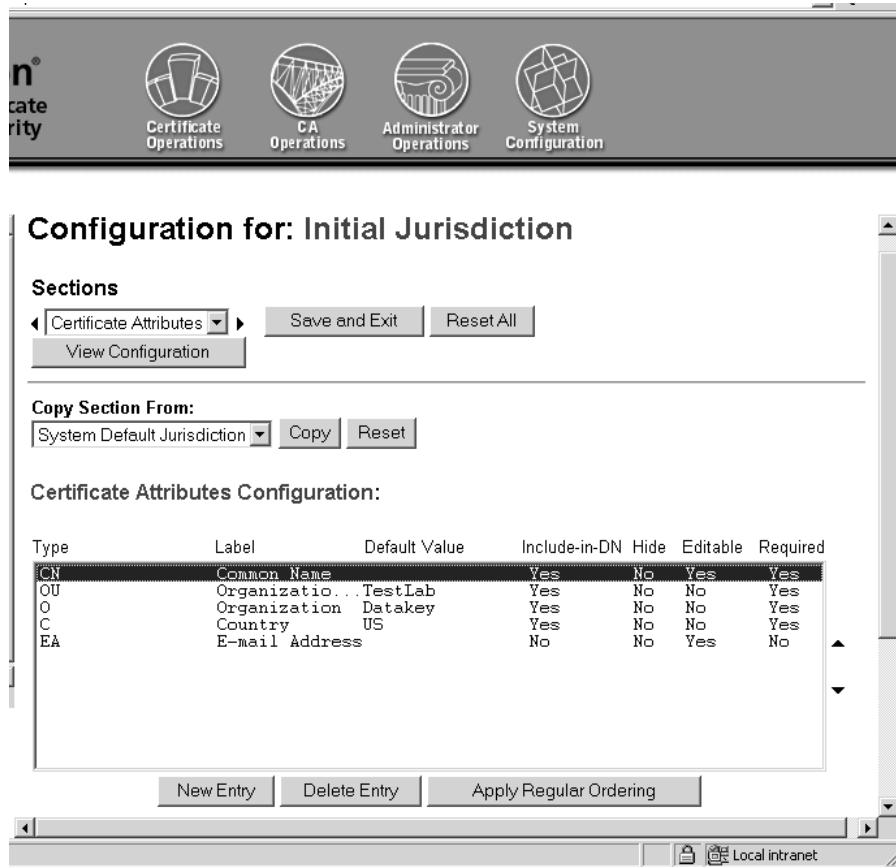
1. Navigate to the home page of your RSA Keon CA.
2. On the CA Operations menu, click *Create*.
The *Create a New CA* page appears.
3. In the *Issuer* field select *Self*.
4. In the *Jurisdiction* field select *Create new Jurisdiction*.
5. Click *Next*.

Configure the initial jurisdiction

Configure the certificate attributes as follows:

1. In the *Sections* field select *Certificate Attributes*.
2. Create attribute entries similar to those shown in the following figure.
You'll need to scroll down to modify the values in an entry.

Note: The values shown here are sample values. You must create unique entries that apply to your organization.

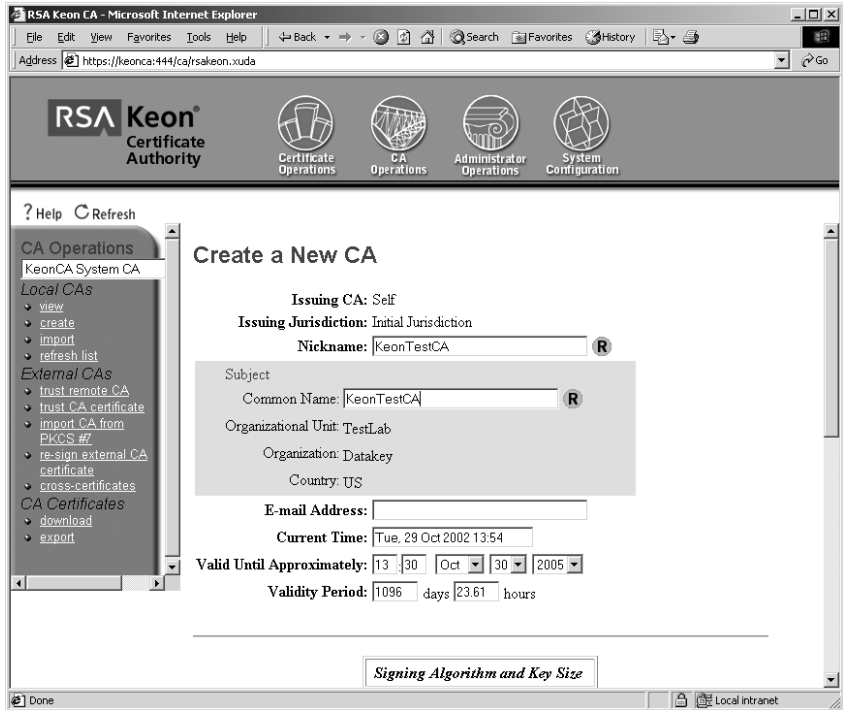


3. When done, click *Save and Exit*.
The *Create a New CA* window appears.

Specify settings for the new CA

1. Specify a name in the *Nickname* and *Common Name* fields.

In many cases you can use the same name in both fields, as illustrated in the following figure.



2. Accept the default values in all remaining fields.
3. Scroll to the bottom of the page and click *Next*.
The *Pass Phrases for New CA* window appears.
4. Type unique passwords when prompted, then click *Create CA*.

Create a new extension profile

1. Click the *System Configuration* icon in the green bar at the top of the page to access the *System Configuration* page.
2. Click on *Extension Profiles* (under *General* on the left side of page).
The *Profile Management* window appears.
3. In the *Existing Profiles* drop-down box, select *Custom End-Entity*.
4. Click *Create*.

The *Profile Editor* window appears.



5. Set *Profile Name* to *Check Point FireWall-1*.
6. Set the *Profile Type* field to *End entity*.
7. In the *Extension Name* table, set *Key Usage* and *Subject Alternative Names* to *Mandatory*.

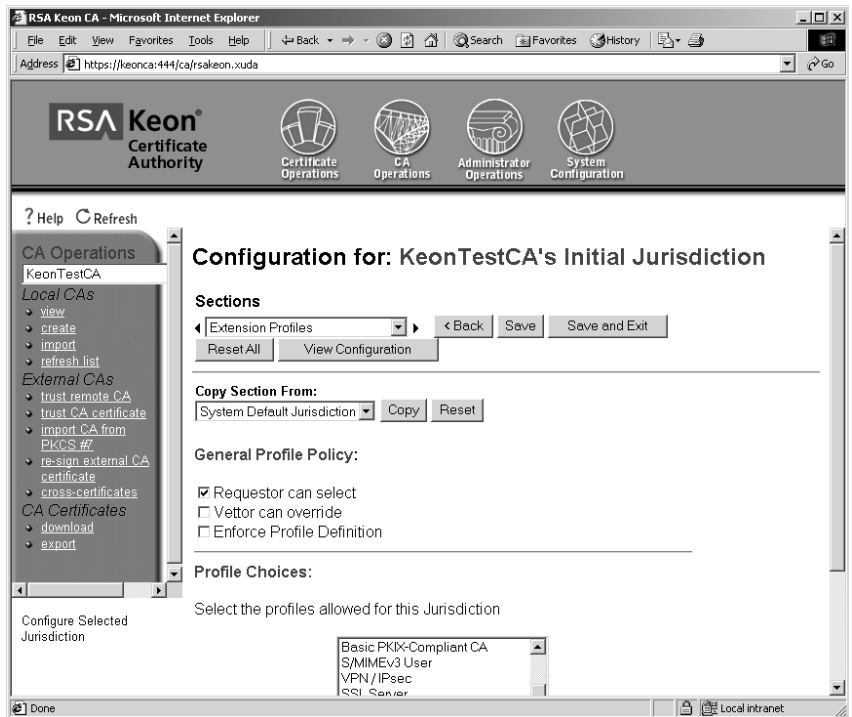
The remaining extension names can retain their default values.

8. Scroll to the bottom of the page and click *Save*.
9. Click *Continue*.

Configure jurisdiction to use new extension profile

1. Click the *CA Operations* icon located at the top of the window.
2. In the *Issuer* drop-down list, select the name of your CA.
In this example the name of the CA is *KeonTestCA*.
3. On the left side of the window, under *Local CAs*, click *View*, then scroll to the bottom the page.
4. Click the *Configure* button that is located next to the *Jurisdiction Configuration* drop-down list.

The following window appears:



5. In the *Sections* drop-down list, select *Extension Profiles*.

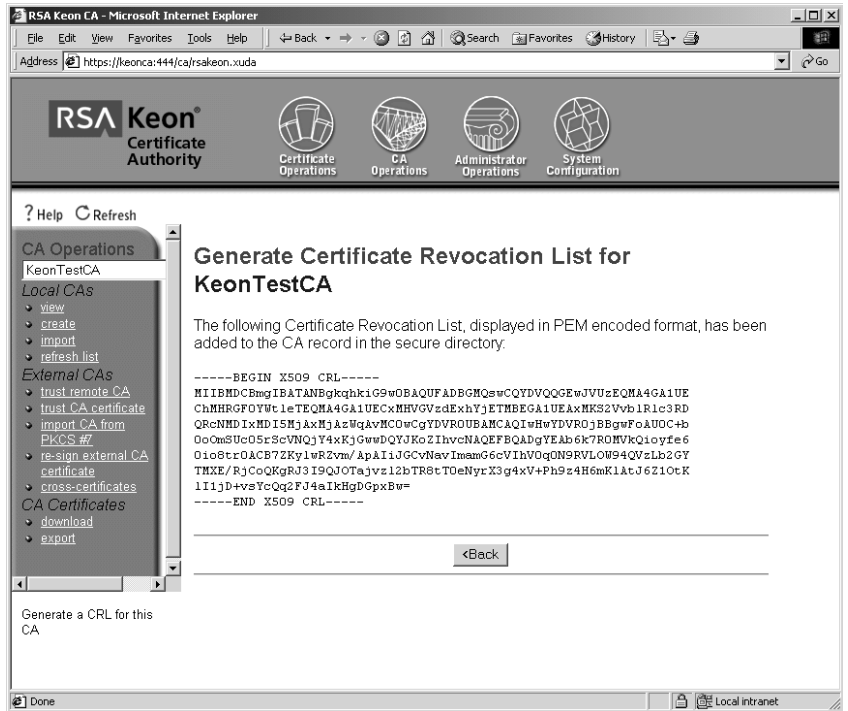
6. In the *General Profile Policy* field, enable the *Requestor can select* option.
7. In the *Profile Choices* drop-down list, select *Check Point FireWall-1*.
8. Scroll back to the top of the page, then click *Save*.
9. In the *Sections* drop-down list, select *Local Certificate Publishing*.
10. Check the *Enable Local Certificate Publishing* option.
11. Click *Save and Exit*.

The *Certificate Authority* window reappears.

Configure CRL options

1. Scroll to the bottom of the *Certificate Authority* window, then click the *CRL Publishing* button in the *CA Configuration* section.
2. Check the *Enable local CRL publishing* option, then select *Publish to LDAP server*.
3. Click *Modify Configuration*.
4. When prompted to confirm the change, click *OK*.
5. On the *Local CRL Publishing* window, click *OK*.
The *Certificate Authority* window reappears.
6. Scroll to the bottom of the page, then click the *Generate CRL* button in the *CA Configuration* section.

A window similar to the following appears:



7. Click *<Back*.

Download the CA's root certificate to diskette

1. From the *CA Operations* page, view your CA.
2. Scroll to the bottom of the page, then click the *Download* button in the *CA Configuration* section.

This saves the CA root certificate to diskette.

Configuring your Check Point VPN-1/FireWall-1

This appendix provides sample configuration steps used to enable a Check Point VPN-1/FireWall-1 to interact with a CA and with a remote workstation. The configuration steps illustrated here are for purposes of example only and are not meant to provide complete configuration information for your Check Point firewall.

Note: *The configuration steps shown here are performed on a Check Point FireWall-1 NG. (A Check Point FireWall-1 NG was used when performing testing to achieve Check Point OPSEC certification for Datakey products.) If you are using a different version of FireWall-1 the configuration steps are likely to be different.*

Create a workstation object

1. From the Check Point Visual Policy Editor™, select *Manage > Network Objects*.
2. On the *Network Objects* window, click *New > Workstation*.
The *Workstation Properties* window appears.
3. Provide values for the following fields.
 - *Name:* Specify the host name of the machine running the RSA Keon CA
 - *IP Address:* Specify the IP address of the machine running the RSA Keon CA
 - *Type:* Select *Host*All other fields can take their default values.
4. Click *OK*.
5. Click *Close*.

Create an LDAP Account Unit object

1. From the Check Point Visual Policy Editor, select *Manage > Servers*.
The *Servers* window appears.
2. Click *New > LDAP Account Unit*.
The *LDAP Account Unit Properties* window appears.
3. Select the *General tab*, then provide values for the following fields:
 - *Name*: Specify *Keon_LDAP*
 - *Account Unit Usage*: Enable both *CRL Retrieval* and *User Management*
 - *Host*: Select *RSA Keon CA* from the drop-down list
 - *Port*: Specify *389*, unless a different port was specified for the Directory (LDAP) Server during the installation of the RSA Keon CA
 - *LDAP Rights*: Enable *R*, disable *W*
 - *Priority*: *1*
 - *LDAP server profile*: Select *Netscape_DS* from the drop-down list
 - *Branches*: Click *Add*, then enter define your distinguished name entry.
4. On the *Users tab*, enable *Use Default User Template*, then select *LDAP_Template* from the drop-down list.
5. Click *OK*.
6. Click *Close*.

Create a CA instance

1. From the Check Point Visual Policy Editor, select *Manage > Servers*.
The *Servers* window appears.
2. Click *New > Certificate Authority*.
The *Certificate Authority Properties* window appears.
3. Select the *General tab*.
4. Provide values for the following fields:
 - *Name*: Give it the name of your CA (e.g. *KeonTestCA*)
 - *Certificate Authority*: Select *OPSEC PKI* from the drop-down list
5. Select the *OPSEC PKI tab*.

6. Enable the *LDAP Server* and the *HTTP Server(s)* options within the *Retrieve CRL From* field.
7. Click *Get*.
8. Navigate to the file containing your CA's certificate, then click *Open*.
9. Click *OK*.

Generate a Certificate Signing Request

1. Open the *TestCKFW1* workstation object by double-clicking on it in either the network diagram or in the list of network objects in the left pane of the window. The *Workstation Properties* window appears.
2. In the field on the left, click *VPN*.
3. Click *Add*.
4. The *Certificate Properties* window appears.



5. Enter a value in the *Certificate Nickname* field.
6. Select *KeonTestCA* from the *Certificate Authority* drop-down list.
7. Click *Generate*.

The *Generate Certificate Request* window appears.

8. In the *DN* field, enter the following value:
CN=FW1,OU=TestLab,O=Datakey,C=US
9. Click *OK*.
10. On the *Certificate Properties* window, click *View*.

The *Certificate Request View* window appears.



11. Click and drag to select the contents of the certificate request.
Select only the text between the *---Begin Certificate Request---* and the *---End Certificate Request---* markers; do not select the markers themselves.
12. Right-click the selected text and copy the contents to the clip board.
13. Click *OK*.
14. Leave the *Certificate Properties* window open. It will be used in a later step.
15. Using your Web browser, go to your local *RSA Keon CA Enrollment* page.
16. Select *KeonTestCA's Initial Jurisdiction* from the drop-down list, then click *Continue*.
17. On the next page, click on the *Make a PKCS #10 Certificate request* link to view the *PKCS #10 Request Form* page.
18. Scroll to the bottom of the *Request Form* page and in the *Certificate Profile* drop-down list select *Check Point FireWall-1*.

19. Paste the *Certificate Request* text from the clip board (from step 12) into the box at the bottom of the page.
20. Scroll to the bottom of the page and click *Submit Request*.

Approve the request on your local RSA Keon CA

On your local RSA Keon CA, approve the certificate signing request, then copy the certificate to a diskette.

Load the FireWall-1 certificate from diskette

After your CA approves the certificate signing request and creates the certificate, you must load the certificate onto the firewall.

1. Go to the *FireWall-1* console.
2. On the *Certificate Properties* window, click *Get*.
3. Navigate to the location of the certificate file (in this case it is on diskette), then click *Open*.
4. Click *OK*.

Return to the *Workstation Properties* window.

Configure the IKE properties

To set the firewall's Internet Key Exchange (IKE) properties, perform the following steps:

1. On the *Workstation Properties* window, click *Set default IKE properties*.

The *IKE Properties* window appears.



2. Enable the *MD5*, *SHAI*, and *Public Key Signatures* options.
3. Click *Specify*.

The *Allowed Certificates* window appears.

4. Select *The gateway can use any of its certificates*, then click *OK*.

Define a TCP service

1. From the Check Point Visual Policy Editor, select *Manage -> Services*.
The *Services* window appears.

2. Click *New -> TCP*.

The *TCP Service Properties* window appears.

3. Specify a value in the *Name* field.

For example, you might give it the name *KeonEnrollentPage*.

4. In the *Port* field, specify 555 unless another port was defined for the Enrollment Server during the installation of your RSA Keon CA.
The default values can be used in all the other fields on this window.
5. Click *OK*.
6. Click *Close*.

Create an external user group

1. From the Check Point Visual Policy Editor, select *Manage -> Users & Administrators*.
The *Users* window appears.
2. Click *New->External Group*.
The *External User Group (LDAP) Properties* window appears.
3. Specify a value in the *Name* field.
For example, you might give it the name *LDAP_External_Keon*.
4. In the *Account Unit* field, specify *Keon_LDAP* from the drop-down list.
5. In the *Group's Scope* field, select *All Account-Unit's Users*.
The default values can be used in all the other fields on this window.
6. Click *OK*.
7. Click *Close*.

Configure and install an initial security policy

Using the Check Point Visual Policy Editor, select *Rules -> Add Rule* and create three rules.

- Rule 1 should allow any source to access to your CA using the TCP service you created on page 30.
- Rule 2 should allow any member of the external user group created in the previous section to access any destination using any service, on the condition they perform *client encryption*.
- Rule 3 should drop all other packets.

The following figure illustrates these three rules.



The screenshot shows the 'Policy Editor - KeonOnly' window. The main area displays a table with three rules. The table has columns for NO., SOURCE, DESTINATION, SERVICE, ACTION, TRACK, INSTALL ON, and TIME.

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	* Any	KeonCA	TCP KeonEnrollmentIP	accept	Log	Gateways	* Any
2	LDAP_External_Keon@Any	* Any	* Any	Client Encrypt	Log	Gateways	* Any
3	* Any	* Any	* Any	drop	Log	Gateways	* Any

8. Select *Policy* -> *Install*.

9. Click *Select All*.

10. Click *OK*.

The *Install Policy* window appears.

11. Wait until the policy is successfully installed, then click *Close*.

Datakey Corporate Headquarters

407 West Travelers Trail

Minneapolis, MN 55337-2558

Phone: (952) 890-6850

Toll-free: 1-888-328-2539

Fax: (952) 890-2726