VASCO
THE AUTHENTICATION COMPANY

DIGIPASS CertiID

User Manual

3.1.0

Disclaimer of Warranties and Limitations of Liabilities

The Product is provided on an 'as is' basis, without any other warranties, or conditions, express or implied, including but not limited to warranties of merchantable quality, merchantability of fitness for a particular purpose, or those arising by law, statute, usage of trade or course of dealing. The entire risk as to the results and performance of the product is assumed by you. Neither we nor our dealers or suppliers shall have any liability to you or any other person or entity for any indirect, incidental, special or consequential damages whatsoever, including but not limited to loss of revenue or profit, lost or damaged data of other commercial or economic loss, even if we have been advised of the possibility of such damages or they are foreseeable; or for claims by a third party. Our maximum aggregate liability to you, and that of our dealers and suppliers shall not exceed the amount paid by you for the Product. The limitations in this section shall apply whether or not the alleged breach or default is a breach of a fundamental condition or term, or a fundamental breach. Some states/countries do not allow the exclusion or limitation or liability for consequential or incidental damages so the above limitation may not apply to you.

Copyright

Trademarks

VASCO, VACMAN, IDENTIKEY, aXsGUARD, DIGIPASS and the Vasco 'V' logo are either registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries.

Version: 2009-06-22

Table of Contents

Illustration Index

Index of Tables

1 Introduction

Welcome to the DIGIPASS CertiID (DP CertiID) User Manual. This document provides you the information you will need to use and configure DP CertiID applications.

This manual provides information about how to:

- manage certificates using DP CertiID Management Application
- manage authentication objects using DP CertiID Management Application
- manage tokens using DP CertiID Management Application
- use DP CertiID to generate one-time passwords (OTPs)
- use DP CertiID Tray Agent
- configure DP CertiID applications using DP CertiID Configuration Center
- troubleshoot and diagnose issues using DP CertiID Troubleshooting and Diagnostics

This manual does **not** provide:

- detailed instructions about preparing and installing DP CertiID (refer to DIGIPASS CertiID Installation Guide)
- detailed instructions about using DP CertiID with common third-party applications (refer to DIGIPASS CertiID Getting Started Manual)

1.1 About this manual

1.1.1 How to use this manual

You can use this manual in different ways, depending on your skill and knowledge level. You can read it from the beginning to the end (highly recommended for novice users), you can browse through the chapter abstracts and read specifically the chapters relevant to your needs, or you can search by key words in the index, if you need to find certain references quickly.

If you need to…	Refer to
…use DP CertiID Management Application to manage digital certificates on your tokens	Chapter "2 Using DP CertiID Management Application" -AND- Chapter "4 Managing Certificates"
…get a better understanding of different data and authentication objects on your token	Section "5.1 Understanding Authentication Objects"
…use DP CertiID Management Application to manage authentication codes, such as PINs and PUKs, on your tokens	Chapter "5 Managing Authentication Objects"
…use DP CertiID Management Application to manage your tokens	Chapter "3 Managing Tokens"
…use DP CertiID Tray Agent to automatically register/unregister certificates and to verify the status of DIGIPASS CertiID middleware	Chapter "6 Using the DP CertiID Tray Agent"
…use Group Policy or DP CertiID Configuration Center to configure DIGIPASS CertiID	Chapter "7 Configuring DIGIPASS CertiID"
…use DP CertiID Troubleshooting and Diagnostics to diagnose and troubleshoot middleware issues	Chapter "8 Troubleshooting and Diagnostics"
…use DP CertiID to generate one-time passwords (OTPs)	Chapter "9 Appendix: Using DP CertiID with One-Time Passwords (OTP)"
…get a better understanding of PKI and digital certificates	Chapter "10 Appendix: PKI and Certificate Basics"

1.1.2 Document conventions

The following typographic style conventions are used throughout this document.

Typography	Meaning
Boldface	Names of user interface widgets, e.g. the **OK** button
Blue	Values for options; placeholders for information or parameters that you provide, e.g. select Server name in the list box.
UPPERCASE	Keyboard keys, e.g. CTRL for the Control key
`Monospace`	Windows Registry Keys; commands you are supposed to type in or are displayed in a command prompt shell, including directories and filenames; API functions and source code examples

Typography	Meaning
blue, underlined	Internet links

The following visual hint colour schemes are used throughout this document.

TIP
Tips contain supplementary information that is not essential to the completion of the task at hand, including explanations of possible results or alternative methods.

NOTE
Notes contain important supplementary information.

CAUTION
Cautions contain warnings about possible data loss, breaches of security, or other more serious problems.

1.1.3 Providing feedback

Every effort has been made to ensure the accuracy and usefulness of this manual. However, as the reader of this documentation, *you* are our most important critic and commentator. We appreciate your judgment and would like you to write us your opinions, suggestions, critics, questions, and ideas. Please send your commentary to: documentation@vasco.com.

To recognize the particular document you are referring to, please include the following information in your subject header: DPC-UM-3.1.0en-22062009

Please note that product support is not offered through the above mail address.

2 Using DP CertiID Management Application

DP CertiID Management Application is an administration tool allowing you to manage your tokens and digital certificates. This chapter gives an overview of the tool and how to use it.

It covers the following topics:

- Getting to Know DP CertiID Management Application
- Exploring your Token

2.1 Getting to Know DP CertiID Management Application

➢ To start DP CertiID Management Application

- Select **Start > Programs > VASCO > DIGIPASS CertiID > Management Application**.

  -OR-

  Select **Management Application** in the **DP CertiID Tray Agent** menu.

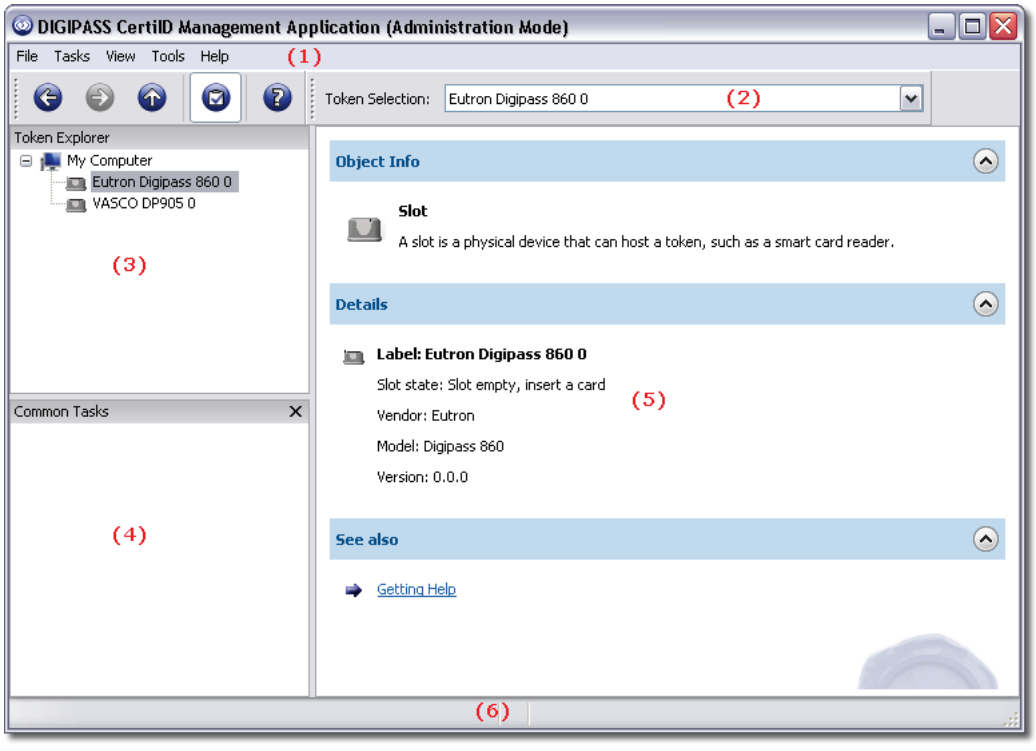

Figure 1: DP CertiID Management Application Main Window

The DP CertiID Management Application main window consists of the following:

1. Menu bar and toolbar
2. Token selection
3. Token explorer sidebar
4. Common tasks sidebar
5. Object view
6. Status bar

TIP
You can show, hide, and move most of the sidebars as you like. To reset the main window view to its default layout, select **View > Reset view** in the menu bar.

2.1.1 Toolbar

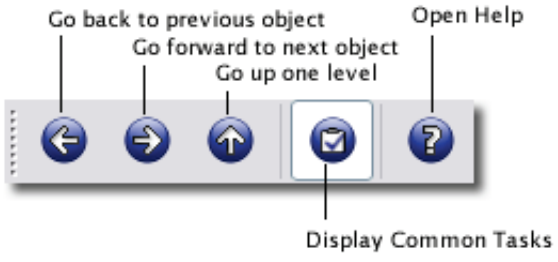

Figure 2: DP CertiID Management Application Toolbar

The toolbar provides quick navigation commands and allows quick showing or hiding of the sidebars.

2.1.2 Token selection

The token selection list contains all connected readers and tokens. Readers and tokens are enumerated and listed by name or device type for better distinction, respectively.

2.1.3 Token explorer sidebar

The token explorer sidebar displays the connected smart card readers and tokens as well as the various kinds of data objects they may contain in a hierarchical list.

2.1.4 Common tasks sidebar

The common tasks sidebar shows the most relevant properties of the selected object and provides quick access to the most common tasks applicable to it. For example, if the selected object is a certificate, a set of certificate related tasks is shown, such as **View certificate** and **Export certificate**.

2.1.5 Object view

The object view displays the objects, which are logically associated with the object currently selected in the token explorer sidebar.

2.1.6 Status bar

The status bar at the bottom of the window displays information about the current state, background tasks, and other contextual information.

2.2 Exploring your Token

The token explorer sidebar allows you to quickly browse and explore your tokens. It displays all connected smart card readers and tokens grouped hierarchically.

An initialized token may usually contain the following folders:

- Authentication Objects
- CA Certificates
- Data Objects
- Other Certificates
- OTP Key Objects
- Secret Key Objects

Additionally, it may contain one or more key and certificate containers.

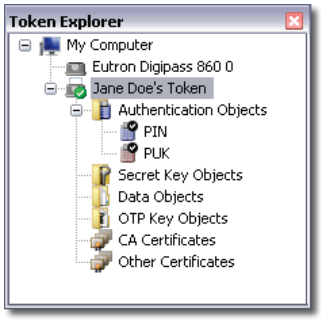

Figure 3: Exploring Token

2.2.1 Authentication objects

This folder contains all authentication objects on the token, i.e. all PINs, PUKs, and the administrator key, if present. In most cases, you will see at least a default PIN (a PIN object with the label PIN) and a default PUK (a PUK object with the label PUK).

2.2.2 CA certificates

This folder contains all CA certificates that are not associated with a key pair.

2.2.3 Other certificates

This folder contains all other third-party certificates (other people).

2.2.4 Data objects

This folder contains any generic data objects that are not authentication objects, certificates, or key objects.

2.2.5 OTP key objects

This folder contains OTP key objects. An **OTP key object** (in this context) is an abstract representation of an OTP generating mechanism. This can be an OTP hardware token (e.g. DP860) or a secret key object on the token used to calculate OTPs.

2.2.6 Secret key objects

This folder contains all secret key objects on the token, including master administrator keys. A **secret key** is a key used for cryptographic operations where the same key is used for both encryption and decryption, also known as **symmetric cryptography**.

2.2.7 Key and certificate container

A **key container** contains a key pair used for cryptographic operations where different keys are used for encryption and decryption, also known as **asymmetric cryptography**. A key pair consists of a public key and a private key. The **private key** is kept secret and used to decrypt data that has been encrypted with the corresponding public key or to sign data. The **public key** is widely distributed and used to verify data that has been signed with the corresponding private key or to encrypt data.

A **certificate container** is a key container with an associated certificate.

You can see which authentication objects are used to protect a particular data or key object in the token explorer sidebar.

3 Managing Tokens

This chapter gives an overview of how to manage tokens using **DP CertiID Management Application**.

It covers the following topics:

- Initializing Tokens
- Personalizing Tokens
- Resetting Tokens
- Resetting Token Personalization

3.1 Initializing Tokens

To use an empty token with DIGIPASS CertiID, you need to initialize the token first. During **initialization**, a so-called token template is applied to the token, which contains important token configuration data, such as default PIN/PUK protection.

You can skip some settings during initialization, such as specifying the default PIN and the default PUK. In this case the token is called to be **pre-initialized**. Before it can be used, initialization needs to be completed by personalizing the token, meaning to apply the individual settings, which were omitted during initialization.

3.1.1 Before you begin

You can only initialize empty tokens. To re-initialize a token you need to reset the token first (see Section "Resetting Tokens").

You need to consider, which token template you want to use. A token template contains the default token configuration settings, such as which default authentication mode is used. Currently the following token templates are available:

- Standard PIN/PUK template
  This token template provides authentication using a default PIN, protected by a default PUK. Their values and retry counters may be set during the initialization process.
  This is the default token template and may be used for all supported CAs.
- Standard PIN/AdminKey template
  This token template provides authentication using a default PIN, protected by external authentication using an administrator key. Their values and retry counters may be set during the initialization process.
  This token template is highly recommended, if you want to use **VASCO Card Module** under Microsoft Windows Vista.
- Entrust-optimized PIN/PUK template
  This token template provides the same authentication mechanisms as the Standard PIN/PUK template. It is optimized for use with Entrust Certification Authorities (CA), but you can use it with any other CAs as well. Although it is recommended to use this token template with Entrust CAs, you may also use the other token templates.
- Entrust-optimized PIN/AdminKey template
  This token template provides the same authentication mechanisms as the Standard PIN/AdminKey template. It is optimized for use with Entrust Certification Authorities (CA), but you can use it with any other CAs as well. Although it is recommended to use this token template with Entrust CAs, you may also use the other token templates.

> NOTE
> Your system or token administrator may remove some token templates, so not all of these token templates may be available to you.

3.1.2 Initializing a token

➢ To initialize a token

1. Insert your token.
2. Select the token in the token explorer tree.

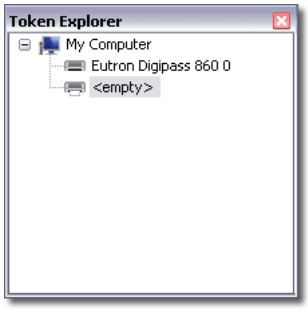

Figure 4: Inspecting Token to Initialize

3. Select **Initialize** from the shortcut menu.

   -OR-

   Select **Tasks > Initialize** from the menu bar.

   The **Initialize Token Wizard** appears.

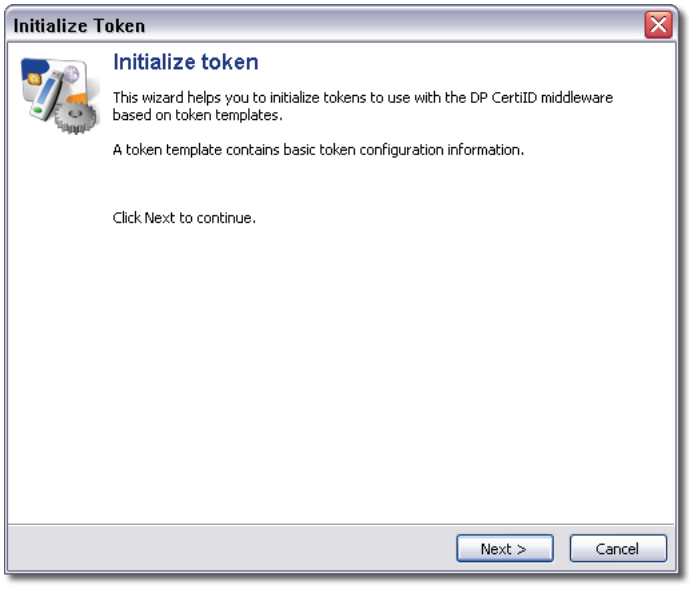

Figure 5: Initializing Token (1)

4. Select the token template in the list.

   A token template contains the default token configuration settings, such as which default authentication mode is used.

   You can select a default value profile to set the standard values for initialization.

   If you do not enable **Edit default values**, the values defined in the default value profile are loaded and used for initialization automatically. The subsequent wizard pages are not displayed and you are redirected directly to the **Ready to Initialize** page.

   If you enable **Edit default values**, the values defined in the default value profile are loaded and filled in the respective fields in the subsequent wizard pages.

   If the standard values defined in the default value profile do not comply with the effective PIN and PUK policy, the values defined in the default value profile are loaded and used for initialization. However, you are redirected to the particular wizard pages to correct the invalid values.

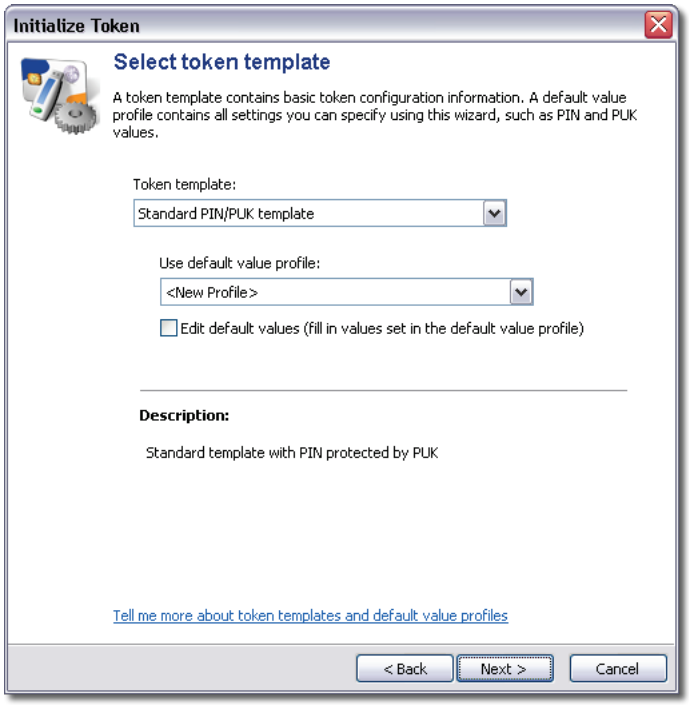

Figure 6: Initializing Token (2) – Selecting Token Template

5. Specify a cardholder name.

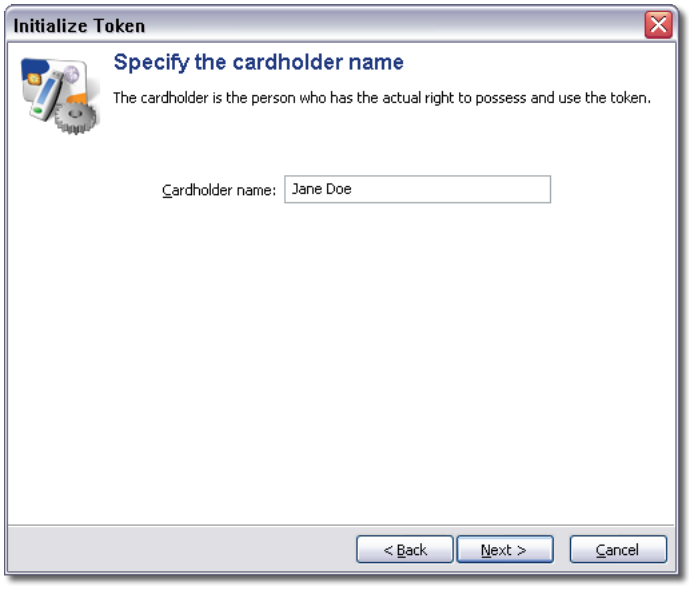

Figure 7: Initializing Token (3) – Specifying Cardholder Name

6. Specify a label for the token.

   The token label is the name used to refer to this token helping to distinguish between different tokens.

Figure 8: Initializing Token (4) – Specifying the Token Label

7. Specify the token reset protection.

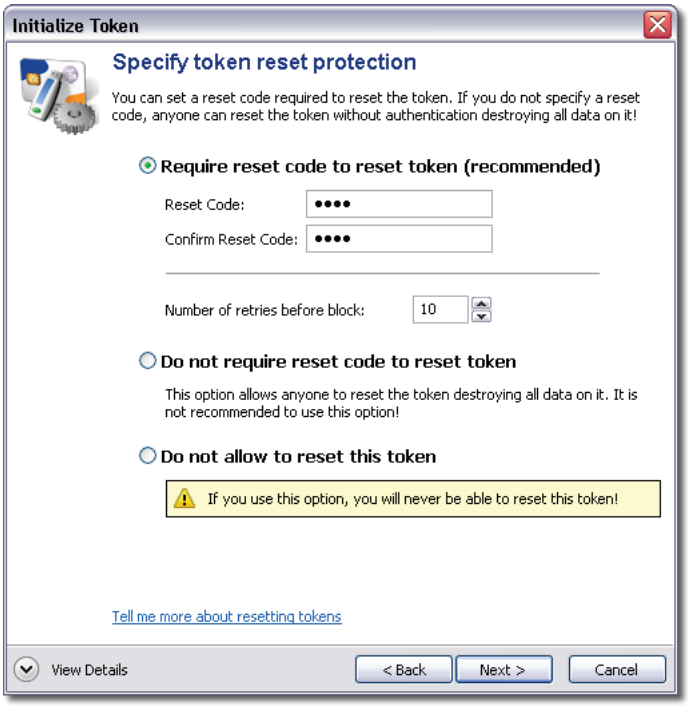

Figure 9: Initializing Token (5) – Specifying Reset Code

- Select **Require reset code to reset token**, if you want to protect the token with a reset code.

  The token can be reset only with the correct reset code.

  Type a value for the reset code twice to prevent typing errors.

  The **Number of retries before block** box defines, how often an incorrect value for the reset code can be consecutively typed, before it is blocked.
- Select **Do not require reset code to reset token**, if you want to allow resetting the token without a reset code.

  If you do not require a reset token, anyone (including unauthorized persons) can reset the token without any prior authentication.
- Select **Do not allow to reset this token**, to prevent to reset this token at all.

CAUTION
If you use this option, you will never be able to reset the token again!

8. Specify a token security mode.

   The token security mode defines your default rights on the objects on the token.

Figure 10: Initializing Token (6) – Selecting Token Security Mode

- The VASCO Default Mode allows you to create and use all objects on the token. You can also delete all objects from the token, except for authentication objects.
- The Secure Signature Mode is more restrictive. You can delete data objects, but are not allowed to delete authentication objects, key objects, or certificates.

9. Specify keypad hardware support.

   If you enable keypad support, PINs on the token can be entered using keypad hardware (if available). If no keypad hardware is found, PINs are entered using PIN dialogs on the screen.
   If you don't enable keypad support, PINs on the token are always entered using PIN dialogs on the screen.

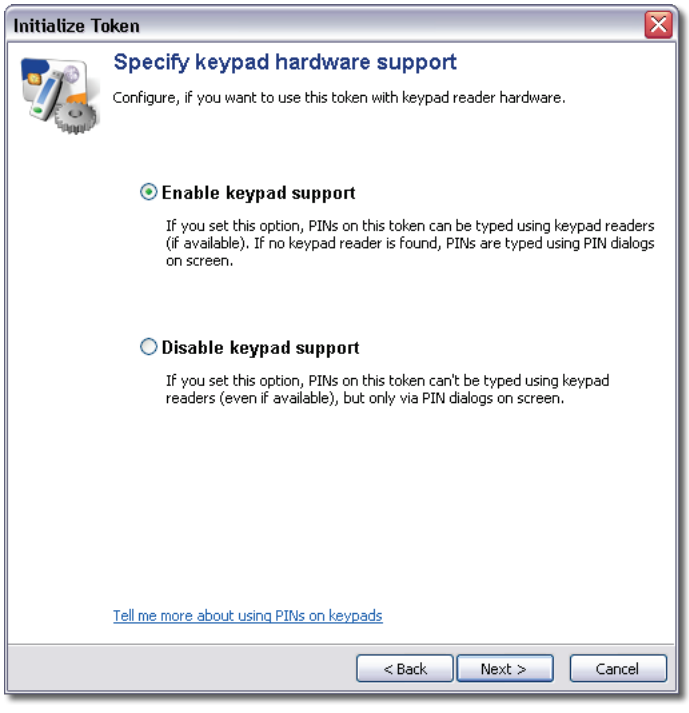

Figure 11: Initializing Token (7) – Specifying Keypad Hardware Support

10. If required, specify a default PIN.

    This option is only available, if the token template configuration includes a default PIN.

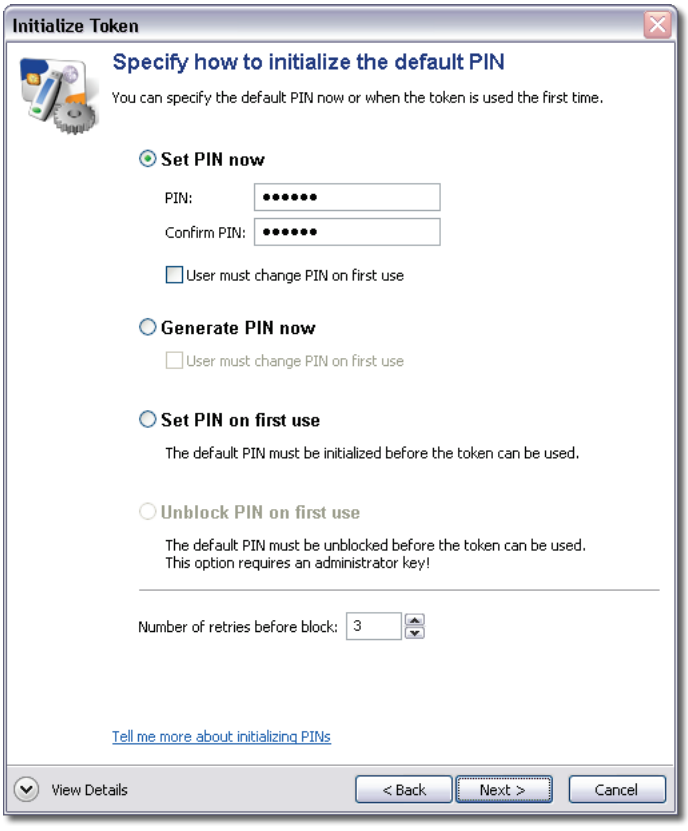

Figure 12: Initializing Token (8) – Specifying Default PIN

- Select **Set PIN now** and type a value for the PIN twice to prevent typing errors.

  If you select the **User must change PIN on first use** check box, the user is asked to change the PIN before the token can be used.

  Next remains disabled until the new PIN complies with the effective PIN policy!

TIP
Click **View Details** to show the effective PIN policy to see why the specified PIN does not comply with it.

- Select **Generate PIN** to have a PIN automatically generated for you.

  The generated PIN value is displayed after the wizard has performed the requested actions. It will also be shown in the PIN letter, if you request to print one (see Step 13).

  If you select the **User must change PIN on first use** check box, the user is asked to change the PIN before the token can be used.

- Select **Set PIN on first use**, if you don't want to set the default PIN now.

The default PIN is not set now, i.e. the token is pre-initialized. The next time the token is inserted, the user is asked to complete the initialization via the **Personalize Token Wizard**. This option is useful, if you want to prepare a token with a personalized default PUK or default administrator key, but want the user to set the default PIN.

- Select **Unblock PIN on first use** to create a blocked default PIN that needs to be unblocked first.

  This option is only available, if the token template configuration includes an administrator key.

  The default PIN is created, but blocked. The next time the token is inserted, the user is asked to unblock the PIN via challenge/response before the token can be used.

  The **Number of retries before block** box defines, how often an incorrect value for the PIN can be consecutively typed, before it is blocked and needs to be unblocked.

11. If required, specify a default PUK.

This option is only available, if the token template configuration includes a default PUK.

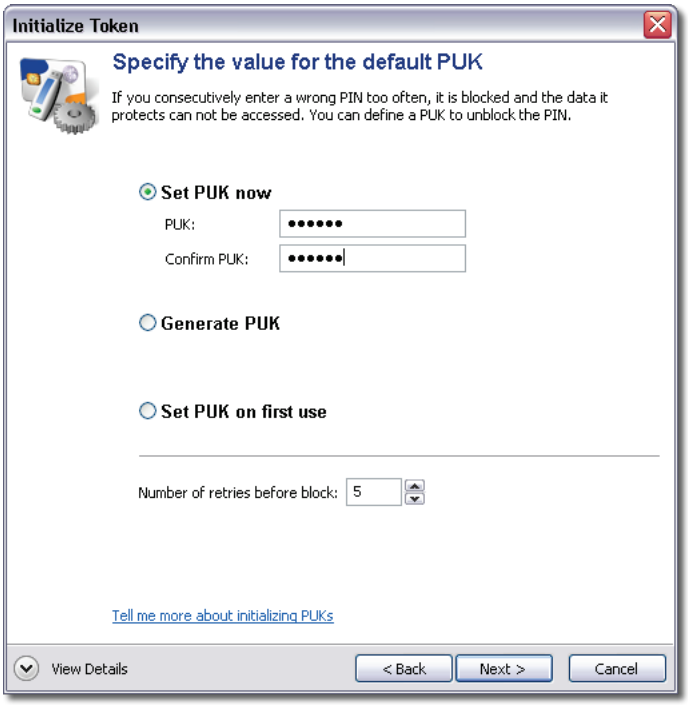

Figure 13: Initializing Token (9) – Specifying Default PUK

- Select **Set PUK now** and type a value for the PUK twice to prevent typing errors.

  Next remains disabled until the new PUK complies with the effective PUK policy!

TIP
Click **View Details** to show the effective PUK policy to see why the specified PUK does not comply with it.

- Select **Generate PUK** to have a PUK automatically generated for you.

  The generated PUK value is displayed after the wizard has performed the requested actions. It will also be shown in the PIN and/or PUK letter, if you request to print one (see Step 13).

- Select **Set PUK on first use**, if you don't want to set the default PUK now.

  This option is only available, if the **Set PIN on first use** option was selected (see Step 9).

  The default PUK is not set now, i.e. the token is pre-initialized. The next time the token is inserted, the user is asked to complete the initialization via the **Personalize Token Wizard**.

  The **Number of retries before block** box defines, how often an incorrect value for the PUK can be consecutively typed, before it is blocked.

12. If required, specify an administrator key.

This option is only available, if the token template configuration includes an administrator key.

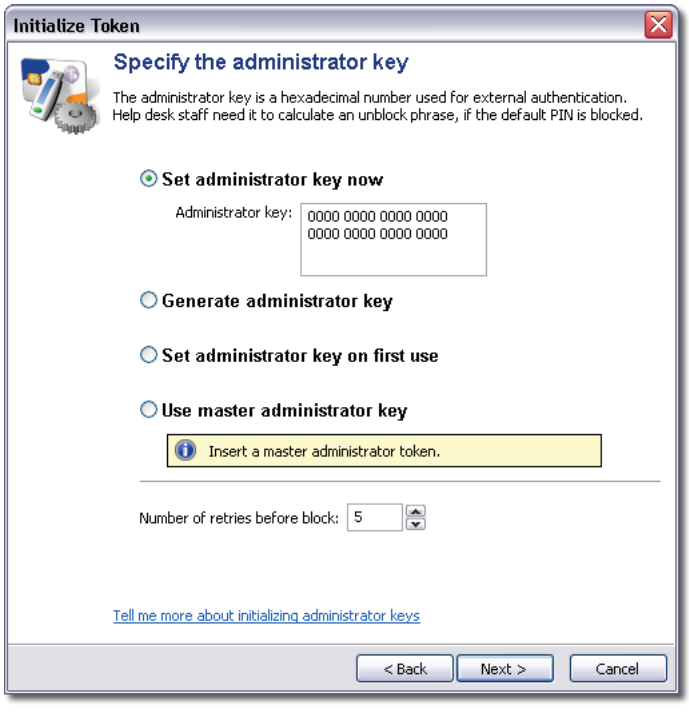

Figure 14: Initializing Token (10) – Specifying Administrator Key

- Select **Set administrator key now** and type a value for the administrator key.
- Select **Generate administrator key** to have an administrator key automatically generated for you.

  The generated administrator key value is displayed after the wizard has performed the requested actions. It will also be shown in the PIN and/or administrator key letter, if you request to print one (see Step 13).

- Select **Set administrator key on first use**, if you don't want to set the default administrator key now.

  This option is only available, if the **Set PIN on first use** option was selected (see Step 9).

  The default administrator key is not set now, i.e. the token is pre-initialized. The next time the token is inserted, the user is asked to complete the initialization via the **Personalize Token Wizard**.

- Select **Use master administrator key**, if you want to use a master administrator key to derive the administrator key for this token.

  (a) Insert the administrator token.

  (b) Select the master administrator key in the **Master key** list.

  (c) Type the PIN for the master administrator key.

The **Number of retries before block** box defines, how often an incorrect value for the administrator key can be consecutively typed, before it is blocked.

13. Specify whether to print a PIN/PUK/administrator key letter and select a printing device to print.

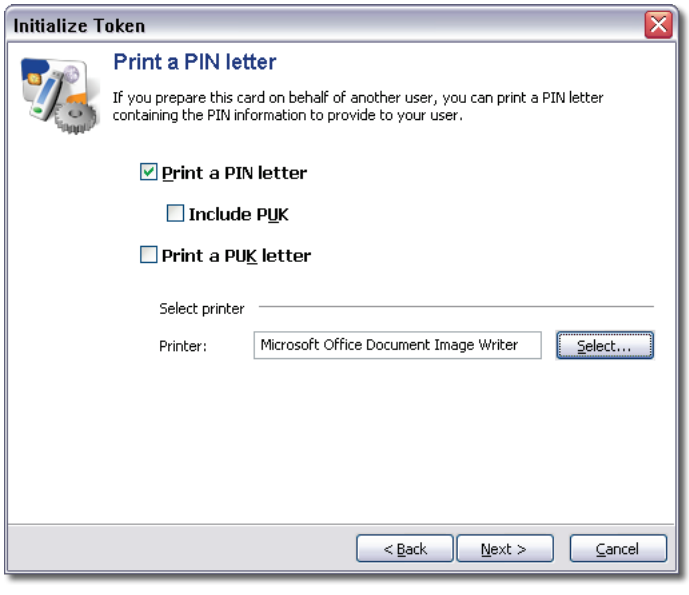

Figure 15: Initializing Token (11) – Printing PIN/PUK Letter

14. Click **Finish** to initialize the token.

    You may save your settings to a default values profile, which you can select the next time you initialize a token. Type a profile name in the **Profile name** box and click **Save**.

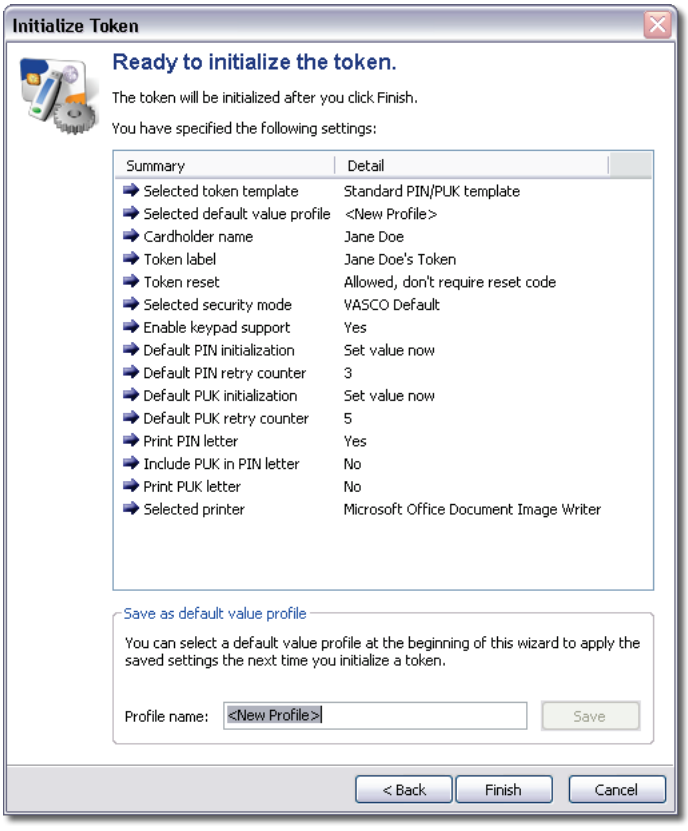

Figure 16: Initializing Token (12) – Ready to Initialize

15. If required, select **I acknowledge this information** and click **OK** to confirm the effective PIN, PUK and/or administrator key that were automatically generated when initializing the token.

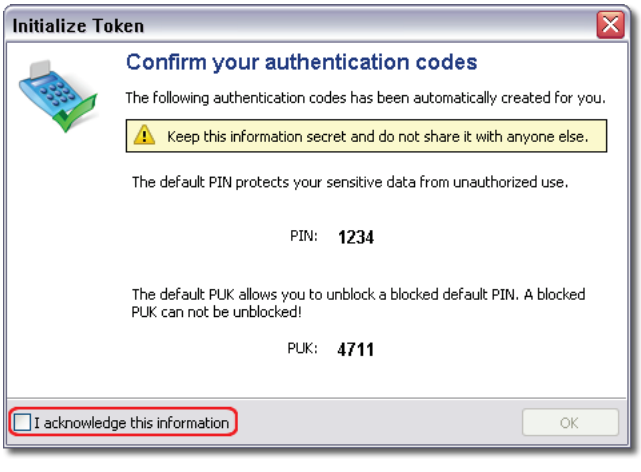

Figure 17: Initializing Token (13) – Confirming Authentication Codes

3.1.3 Additional considerations

- The token template specifies the default authentication mechanism. You can change the authentication mechanism of an initialized token, by adding individual PINs, by removing PIN protection, and by migrating PUKs to administrator keys.
- The system or token administrator may restrict access to certain program features. If a particular option is not available, you may not have the privileges to use it.
- After applying a token template, you cannot switch to another token template. If you want to apply a different token template, you need to reset the token first.
- You can re-issue a token to another user by resetting the personalization data. This way you do not have to reset and re-initialize the token completely.
- You can save your settings to a default values profile without actually initializing a token. Specify your settings, save them to a default values profile in the **Ready to Initialize** page and then click **Cancel**.
- The Set on first use options for PIN, PUK, and administrator key apply to the values only. The retry counter is set as specified in the respective pages.
- You can adapt the text and style of PIN/PUK letters by changing the respective template files.

3.1.4 Additional references

- Personalizing Tokens
- Resetting Tokens
- Resetting Token Personalization
- Generating Master Administrator Keys
- Access Configuration
- Changing the Security of Objects
- Understanding Authentication Objects
- Configuring DIGIPASS CertiID
- Appendix: Customizing PIN/PUK Letters

3.2 Personalizing Tokens

You can skip some settings during initialization, such as specifying the default PIN and the default PUK. In this case the token is called to be **pre-initialized**. Before it can be used, initialization needs to be completed by personalizing the token. **Personalizing** means applying the individual settings, which were omitted during initialization.

Personalizing a token means applying personal or individual settings to the token, which have been omitted during initialization.

Personalization includes:

- Setting the token label
- specifying cardholder data
- Setting the default PIN
- Setting the default PUK or default administrator key

3.2.1 Before you begin

To personalize a token you need:

- **DP CertiID Management Application** or **DP CertiID Tray Agent**
- a pre-initialized token

3.2.2 Personalizing a token

➢ To personalize a token

1. Insert your token.
2. Select the token in the token explorer tree.
3. Select **Personalize** from the shortcut menu.

   -OR-

   Select **Tasks > Personalize** from the menu bar.

   The **Personalize Token Wizard** appears.

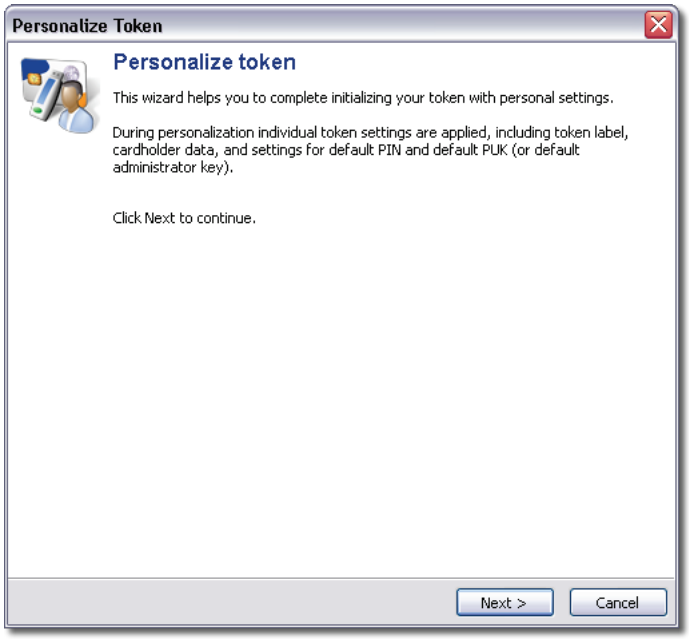

Figure 18: Personalizing Token (1)

4. Specify a cardholder name.

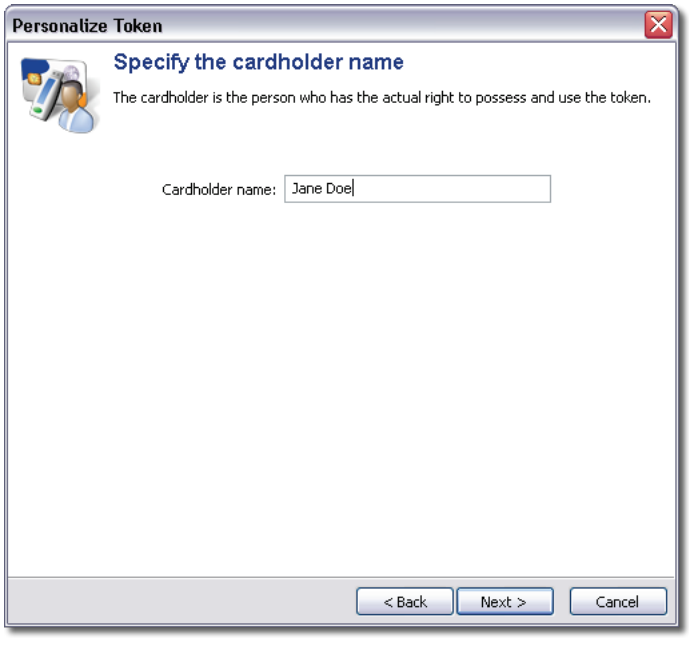

Figure 19: Personalizing Token (2) – Specifying Cardholder Name

5. Specify a label for the token.

The token label is the name used to refer to this token helping to distinguish between different tokens.

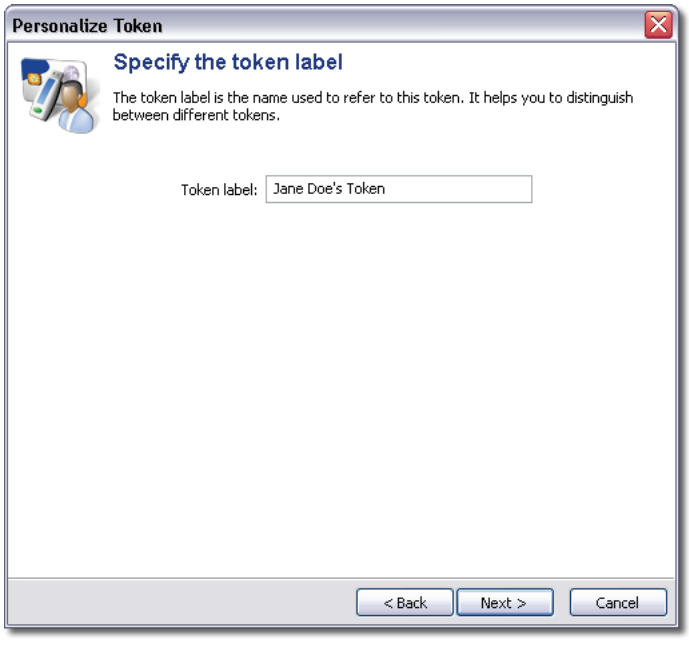

Figure 20: Personalizing Token (3) – Specifying Token Label

6. If required, specify a default PIN.

   This option is only available, if the token template configuration includes a default PIN and the **Set PIN on first use** option was selected during initialization.

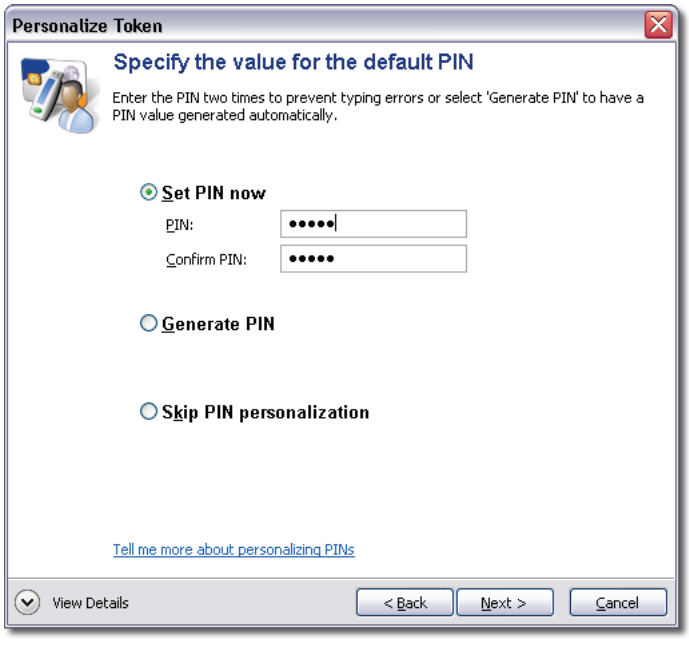

Figure 21: Personalizing Token (4) – Specifying Default PIN

- Select **Set PIN now** and type a value for the PIN twice to prevent typing errors.

  Next remains disabled until the new PIN complies with the effective PIN policy!

TIP
Click **View Details** to show the effective PIN policy to see why the specified PIN does not comply with it.

- Select **Generate PIN** to have a PIN automatically generated for you.

  The generated PIN value is displayed after the wizard has performed the requested actions. It will also be shown in the PIN letter, if you request to print one (see Step 9)

- Select **Skip PIN personalization**, if you don't want to personalize the default PIN now.

  This option is only available, if neither the default PUK nor the default administrator key has been personalized so far, respectively.

  The default PIN is not set now, but asked again for the next time the **Personalize Token Wizard** appears for this token. This option is useful, if you want to prepare a token with a personalized default PUK or default administrator key, but want the user to set the default PIN.

7. If required, specify a default PUK.

   This option is only available, if the token template configuration includes a default PUK and the **Set PUK on first use** option was selected during initialization.

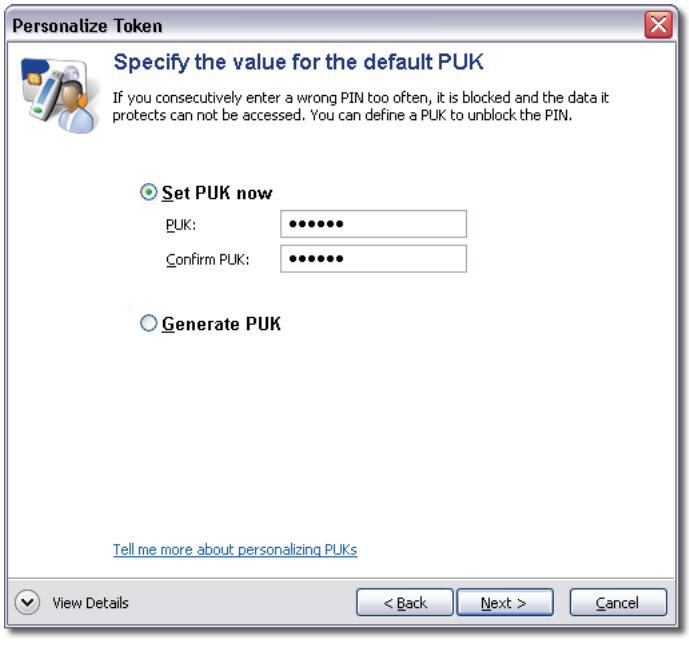

Figure 22: Personalizing Token (5) – Specifying Default PUK

- Select **Set PUK now** and type a value for the PUK twice to prevent typing errors.

  Next remains disabled until the new PUK complies with the effective PUK policy!

TIP
Click **View Details** to show the effective PUK policy to see why the specified PUK does not comply with it.

- Select **Generate PUK** to have a PUK automatically generated for you.

  The generated PUK value is displayed after the wizard has performed the requested actions. It will also be shown in the PIN and/or PUK letter, if you request to print one (see Step 9)

8. If required, specify an administrator key.

   This option is only available, if the token template configuration includes an administrator key and the **Set administrator key on first use** option was selected during initialization.

Figure 23: Personalizing Token (6) – Specifying Administrator Key

- Select **Set administrator key now** and type a value for the administrator key.
- Select **Generate administrator key** to have an administrator key automatically generated for you.

  The generated administrator key value is displayed after the wizard has performed the requested actions. It will also be shown in the PIN and/or administrator key letter, if you request to print one (see Step 9).
- Select **Use master administrator key**, if you want to use a master administrator key to derive the administrator key for this token.

  (a) Insert the administrator token.

  (b) Select the master administrator key in the **Master key** list.

  (c) Type the PIN for the master administrator key.

9. Specify whether to print a PIN/PUK/administrator key letter and select a printing device to print.
10. Click **Finish** to personalize the token.
11. If required, select **I acknowledge this information** and click **OK** to confirm the effective PIN, PUK and/or administrator key that were automatically generated when initializing the token.

3.2.3 Additional considerations

- The system or token administrator may restrict access to certain program features. If a particular option is not available, you may not have the privileges to use it.

- You can set up **DP CertiID Tray Agent** to automatically invoke the **Personalize Token Wizard** upon inserting tokens.
- If you specify to use a master administrator key, the generated administrator key is neither displayed for confirmation nor printed.
- You can re-issue a token to another user by resetting the personalization data. This way you do not have to reset and re-initialize the token completely.
- You can adapt the text and style of PIN/PUK letters by changing the respective template files.

3.2.4 Additional references

- Initializing Tokens
- Resetting Token Personalization
- Generating Master Administrator Keys
- Access Configuration
- Understanding Authentication Objects
- Configuring DIGIPASS CertiID
- Using the DP CertiID Tray Agent
- Appendix: Customizing PIN/PUK Letters

3.3 Resetting Tokens

You can reset a token to an empty state to apply another token template to it, i.e. to re-initialize it.

CAUTION
Resetting a token deletes all data on it, including your digital certificates and key pairs! Ensure that you really won't need the data on the token for later use before you reset the token!

CAUTION
If your token is protected by a reset code and you consecutively enter an incorrect reset code too many times, the reset code is blocked!

You **cannot** unblock a blocked reset code, thus losing the possibility to reset the token in the future!

3.3.1 Before you begin

Usually a token reset is only necessary, if you have blocked your PUK or the administrator key.

You do not have to reset the token, if you want to use an administrator key instead of a PUK to unblock PINs, as you can replace PUKs with administrator keys (see Section "Replacing a PUK with an Administrator Key").

To reset a token you need:

- **DP CertiID Management Application**
- the reset code for the token, if it is protected by one

3.3.2 Resetting a token

➢ To reset a token

1. Insert your token.

2. Select the token to reset in the token explorer tree.

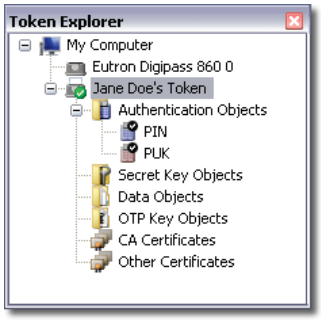

Figure 24: Inspecting Token to Reset

3. Select **Reset** from the shortcut menu.

   -OR-

   Select **Tasks > Reset** from the menu bar.

4. Click **Yes** to confirm resetting the token.

   If the token is protected with a reset code, the **Reset Token Dialog** appears.

Figure 25: Entering Reset Code

5. If required, type the reset code and click **OK**.

3.3.3 Additional considerations

- The system or token administrator may restrict access to certain program features. If the reset token option is not available, you may not have the privileges to use it.
- During initialization tokens can be configured to be not reset at all. If you try to reset a token, which can't be reset, you will get an appropriate error message.
- After a successful reset, the token is empty. To use it with the middleware, you need to initialize it again.

- If the reset code is blocked, you will not be able to reset the token ever again. However, you can continue using it normally.

3.3.4 Additional references

- Initializing Tokens
- Replacing a PUK with an Administrator Key
- Access Configuration
- Understanding Authentication Objects

3.4 Resetting Token Personalization

You can reset the personalization data on a token to reset it to a pre-personalized state. By resetting the token personalization you can re-issue the token to another user without having the token completely reset and re-initialized.

3.4.1 Before you begin

To reset the personalization of a token you need:

- **DP CertiID Management Application**
- the default PUK or administrator key

3.4.2 Resetting token personalization

➢ To reset the personalization of a token

1. Insert your token.
2. Select the token in the token explorer tree.
3. Select **Reset personalization** from the shortcut menu.

   -OR-

   Select **Tasks > Reset personalization** from the menu bar.

   The **Reset Token Personalization Wizard** appears.

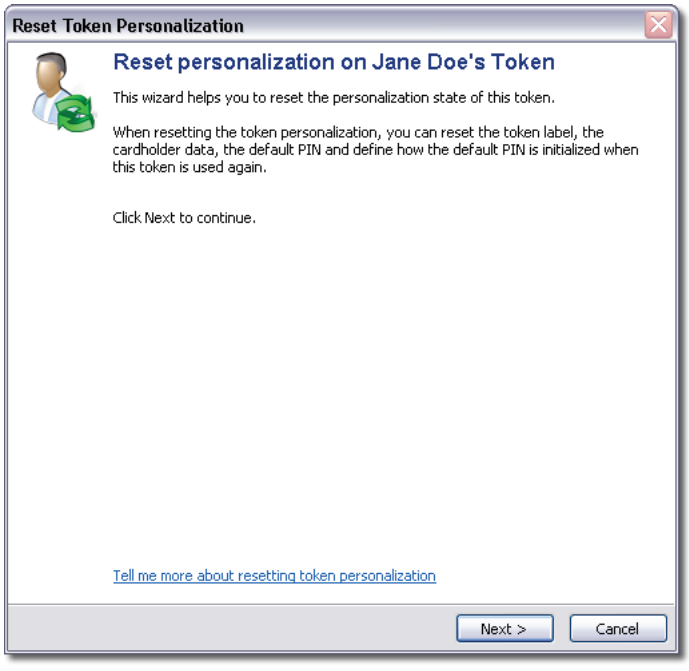

Figure 26: Reset Token Personalization (1)

4. Specify a new cardholder name or click **Next** to keep the current one.

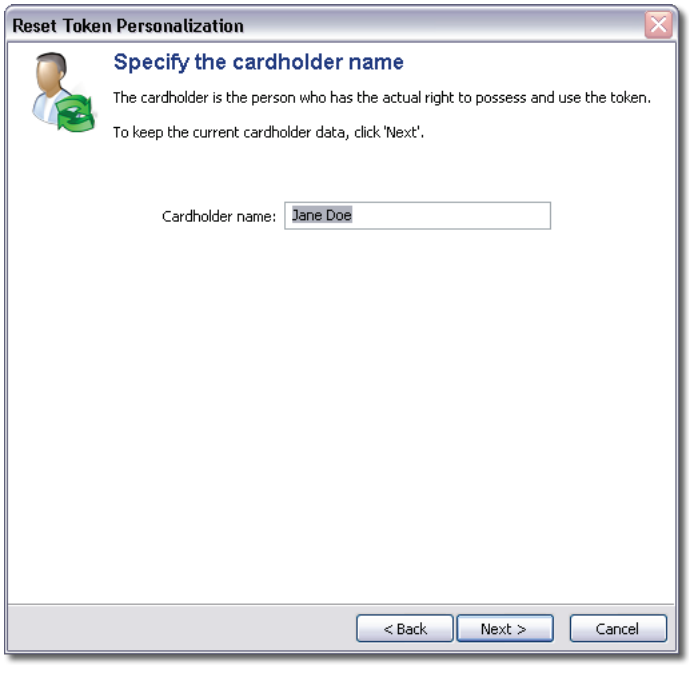

Figure 27: Reset Token Personalization (2) – Specifying Cardholder Name

5. Specify a new token label or click **Next** to keep the current one.

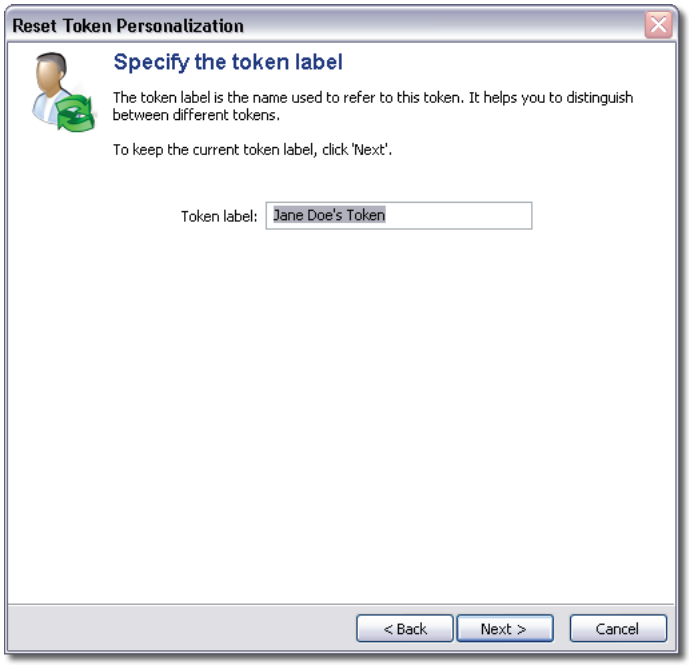

Figure 28: Reset Token Personalization (3) – Specifying Token Label

6. Specify how to initialize the default PIN.

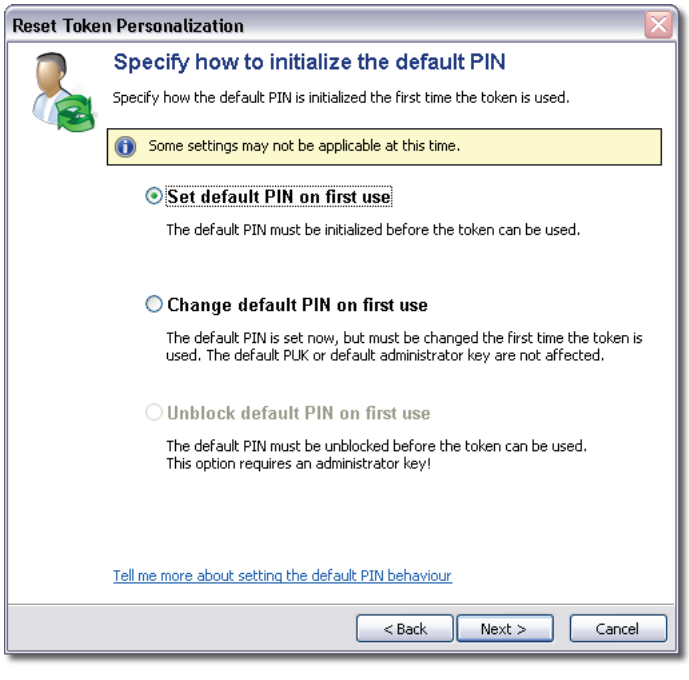

Figure 29: Reset Token Personalization (4) – Specifying Default PIN Initialization

- Select **Set default PIN on first use**, if you don't want to set a new value for the default PIN now.
- Select **Change default PIN on first use**, if you want to set a new value for the default PIN now, but have the user change it the first time the token is used.
- Select **Unblock default PIN on first use**, if you want the user to unblock it the first time the token is used.

  This option is only available, if an administrator key exists on the token.

  The default PIN is blocked. The next time the token is inserted, the user is asked to unblock the PIN via challenge/response before the token can be used

7. If required, specify the new default PIN.

   This option is only available, if the **Change default PIN on first use** option was selected (see Step 6).

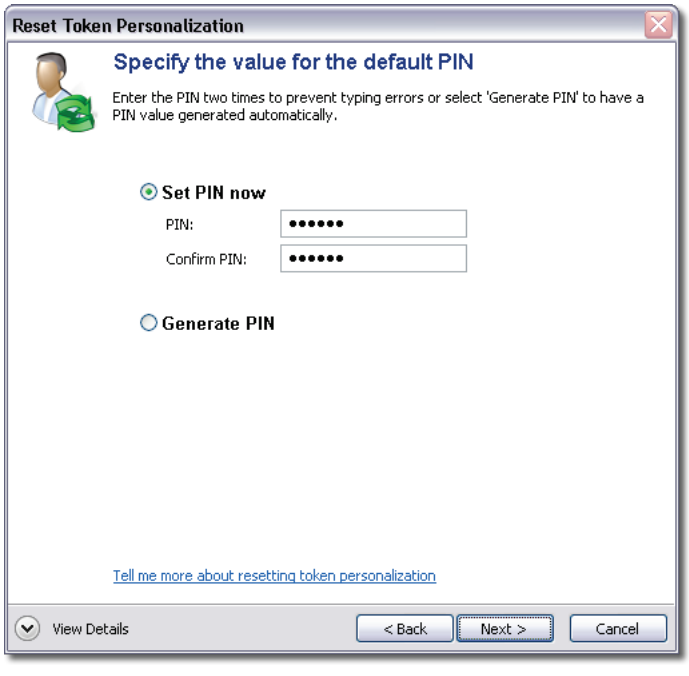

Figure 30: Reset Token Personalization (5) – Specifying Default PIN

- Select **Set PIN now** and type a value for the default PIN twice to prevent typing errors.

  Next remains disabled until the new PIN complies with the effective PIN policy!

TIP
Click **View Details** to show the effective PIN policy to see why the specified PIN does not comply with it.

- Select **Generate PIN** to have a PIN automatically generated for you.

The generated PIN value is displayed after the wizard has performed the requested actions. It will also be shown in the PIN letter, if you request to print one (see Step 8).

8. If required, specify whether to print a PIN letter and select the printing device to print.

   This option is only available, if the **Change default PIN on first use** option was selected (see Step 6).

9. Click **Finish** to reset the token personalization.

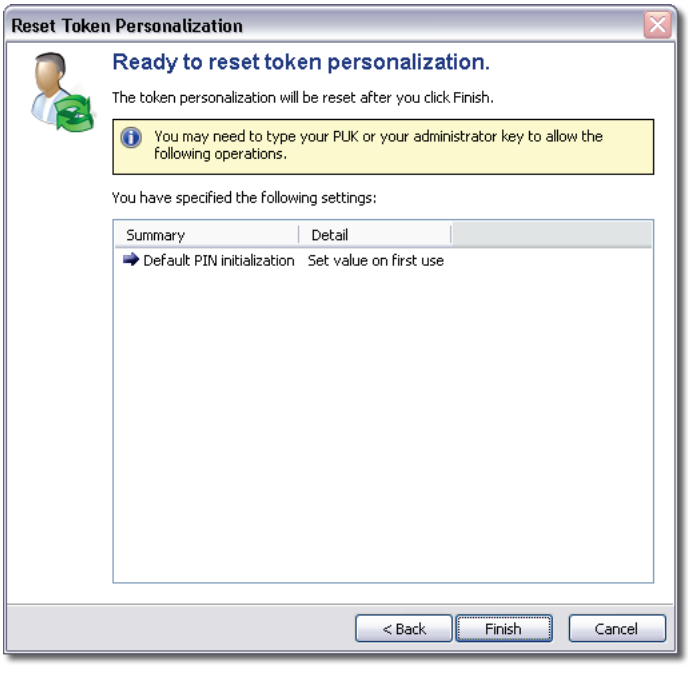

Figure 31: Reset Token Personalization (6) – Ready to Reset Token Personalization

10. If required, type the default PUK or administrator key and click **OK**.

11. If required, select **I acknowledge this information** and click **OK** to confirm the effective PIN, PUK and/or administrator key that were automatically generated when initializing the token.

3.4.3 Additional considerations

- The system or token administrator may restrict access to certain program features. If the reset token personalization option is not available, you may not have the privileges to use it.
- Resetting the personalization data, affects cardholder information, token label, and the default PIN, and sets the token to a pre-personalized state. All other objects are not affected and remain on the token, including certificates and key pairs.
- You can adapt the text and style of PIN/PUK letters by changing the respective template files,

3.4.4 Additional references

- Initializing Tokens
- Personalizing Tokens
- Resetting Tokens
- Appendix: Customizing PIN/PUK Letters

4 Managing Certificates and Containers

This chapter gives an overview of how to manage digital certificates and key containers on a token using **DP CertiID Management Application**.

It covers the following topics:

- Importing Certificates
- Exporting Certificates
- Deleting Objects
- Registering and Unregistering Certificates
- Testing Key Pairs

4.1 Importing Certificates

You can import a certificate from disk to a data container on your token. Depending on whether the certificate is intended for you or if it is a third-party certificate (other people or certification authorities), the certificate is added either to the **CA Certificates** or the **Other Certificates** folder on the token or to an existing key container, which may already contain a certificate.

4.1.1 Before you begin

To import a certificate you need:

- Access to the file containing the respective certificate
- **DP CertiID Management Application**

4.1.2 Importing a certificate

➢ To import a certificate to a token

1. Insert your token.
2. Select the token in the reader explorer tree.
3. Select **Import** from the shortcut menu.

   -OR-

   Select **Tasks > Import** in the menu bar.

   The **Import Certificate Wizard** appears.

Figure 32: Importing Certificate (1)

4. Click **Next** to begin.
5. Select the file name.

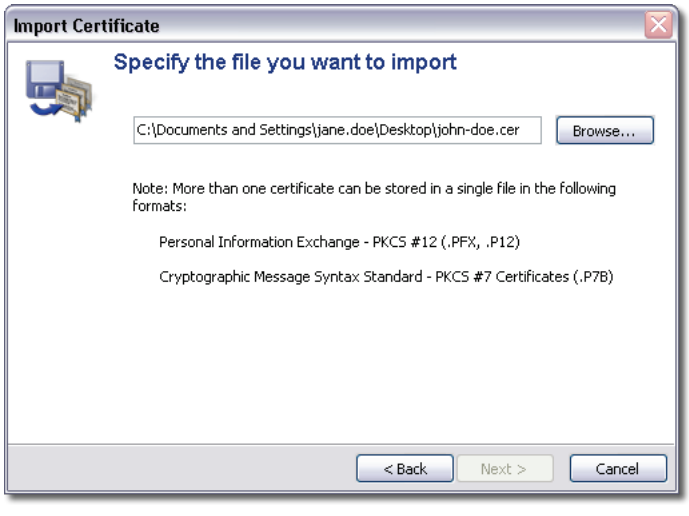

Figure 33: Importing Certificate (2) - Specifying File

6. If you are importing a PKCS #12 file:

   Type the passphrase used to encrypt the private key.

Figure 34: Importing Certificate (3) - Entering Password

7. Select the certificate category.

Figure 35: Importing Certificate (4) - Selecting Certificate Category

8. Click **Finish**.

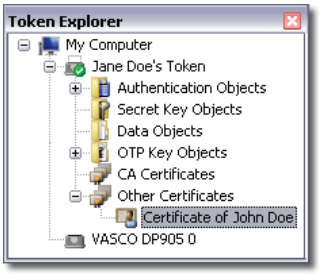

Figure 36: Inspecting Imported Certificate

4.1.3 Additional considerations

- Importing a certificate is not the same as enrolling a certificate. If you import a certificate, you put an existing (already enrolled) certificate from disk on the token. If you enroll a certificate, you request a new certificate to be created and issued from a certification authority.
- The imported certificate file is not deleted and will remain on the disk after the import.
- If you import a certificate for which a corresponding key pair exists on the token, it is added to the particular key container. This does not remove any existing certificate already assigned to the key pair.
- If you import a certificate that is already on the token, it is not imported a second time. The certificate already stored on the token is not replaced by the imported certificate file.

NOTE
VASCO CertiID Smart Card Crypto Provider and VASCO Card Module always use the first certificate assigned with a key pair, since the Microsoft cryptographic architecture assumes that key pairs have only one assigned certificate.

4.1.4 Additional references

- Certificate File Formats
- Certificate Category
- Exporting Certificates

4.2 Exporting Certificates

You can export a certificate from a token to disk to store a copy in a secure location or to import it on another computer or token.

> NOTE
> If you export a personal certificate with an associated key pair, only the certificate is exported to disk, since you cannot extract the private key from a token!

4.2.1 Before you begin

To export a certificate you need:

- **DP CertiID Management Application**

4.2.2 Exporting a certificate

➢ To export a certificate to disk

1. Insert your token.
2. Select the certificate you want in the token explorer tree.

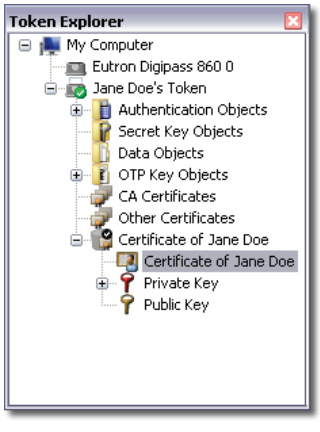

Figure 37: Inspecting Certificate to Export

3. Select **Export** from the shortcut menu.

   -OR-

   Select **Tasks > Export** in the menu bar.

The **Export Certificate Wizard** appears.

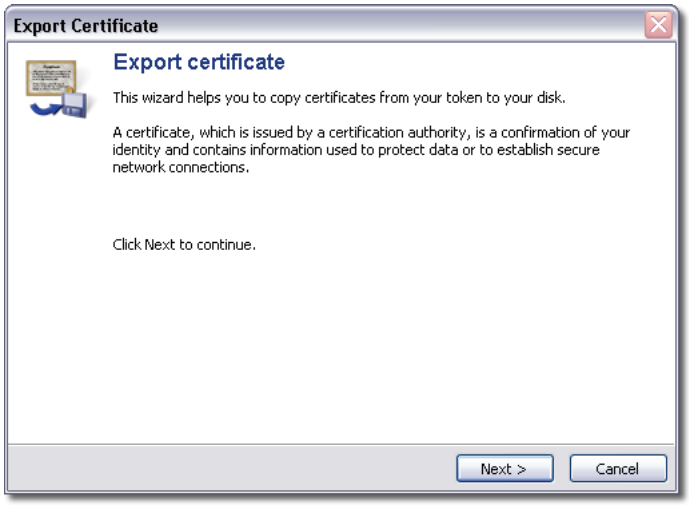

Figure 38: Exporting Certificate (1)

4. Click **Next** to begin.
5. Specify the file format for the certificate file.

Figure 39: Exporting Certificate (2) - Specifying File Format

6. Specify the path and the name for the file that will contain the exported certificate.

Figure 40: Exporting Certificate (3) - Specifying File

7. Click **Finish**.

4.2.3 Additional considerations

- The certificate will remain on the token after the export. If you want to remove it from the token, you must delete it.

4.2.4 Additional references

- Certificate File Formats
- Importing Certificates
- Deleting Objects

4.3 Deleting Objects

You can delete objects from your token, such as certificates, containers, data objects, or secret key objects.

4.3.1 Before you begin

CAUTION
Ensure that you really won't need the object for later use before you delete it!

If you delete a key container, the key pair it contains is deleted and cannot be recovered. You can't decrypt data encrypted using that key pair anymore!

To delete an object you need:

- **DP CertiID Management Application**

4.3.2 Deleting an object

➢ To delete an object from a token

1. Insert your token.
2. Select the object you want to delete in the token explorer tree.
3. Select **Delete** from the shortcut menu.

   -OR-

   Select **Tasks > Delete** from the menu bar.
4. Click **Yes** to confirm deleting the object.

4.3.3 Additional considerations

- The system or token administrator may restrict access to certain program features. If a particular option is not available, you may not have the privileges to use it.
- The types of objects you can delete depend on the security mode set when initializing the token. If a particular object can't be deleted, you may not be allowed to do so.
- If a certificate to be deleted has a corresponding key pair, the key pair is not deleted and will remain on the token. If you want to remove it as well, you must explicitly delete the remaining key container.
- You may export a certificate before you delete it from the token for backup purposes.

- A PIN that may be assigned to protect the private key in a container remains on the token after deleting the container.

4.3.4 Additional references

- Exporting Certificates
- Initializing Tokens

4.4 Registering and Unregistering Certificates

Registering a certificate means adding it to the appropriate certificate store on the machine. A certificate store is the system area where certificates are stored locally by the operating system and made accessible for applications using cryptographic services, e.g. e-mail applications.

Unregistering a certificate means removing it from the certificate store.

4.4.1 Before you begin

To register or unregister a certificate you need:

- **DP CertiID Management Application**

4.4.2 Registering and unregistering a certificate

➢ To register a certificate

1. Insert your token.
2. Select the certificate to register in the token explorer tree.
3. Select **Register** from the shortcut menu.

   -OR-

   Select **Tasks > Register** from the menu bar.

NOTE
If you install a CA certificate, you confirm that you explicitly trust this CA and any certificate issued by it. Due to the impact (and security risks) of this, Microsoft Windows may display a security warning, when **DP CertiID Tray Agent** tries to register a certificate for a CA. Microsoft Windows registers the CA certificate only, if you confirm that you trust the respective CA.

➢ To unregister a certificate

1. Insert your token.
2. Select the certificate to unregister in the token explorer tree.
3. Select **Unregister** from the shortcut menu.

   -OR-

Select **Tasks > Unregister** from the menu bar.

4.4.3 Additional considerations

- Registering only adds the certificate and the associated public key to the certificate store. The associated private key is never read from the token.
- The certificate will remain on the token after unregistering. If you want to remove it from the token, you must delete it.
- The certificate remains registered, when you remove the token, unless **DP CertiID Tray Agent** is running and configured to automatically unregister certificates. If you want to remove it from the certificate store, you need to explicitly unregister it.
- You can use **DP CertiID Tray Agent** to automatically register and unregister your certificates upon inserting and removing the token.

4.4.4 Additional references

- Using the DP CertiID Tray Agent
- Deleting Objects

4.5 Testing Key Pairs

You can test key pairs to validate whether encryption/decryption and signing/verifying operations work correctly. The key pair to test may have an associated certificate.

4.5.1 Before you begin

To test a key pair you need:

- **DP CertiID Management Application**
- the PIN that protects the private key of the respective key pair

4.5.2 Testing a key pair

➢ To test a key pair

1. Insert your token.
2. Select the private key of the key pair to test in the token explorer tree.

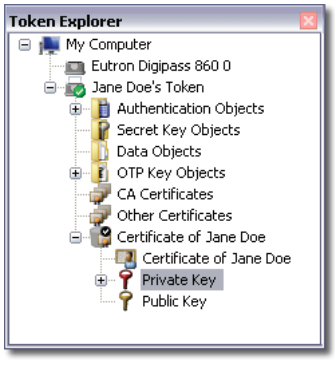

Figure 41: Selecting Private Key

3. Select **Test key pair** from the shortcut menu.

   -OR-

   Select **Tasks > Test key pair** from the menu bar.

   The **Test Key Pair Wizard** appears.

4. To test for encryption and decryption operation do the following:

Figure 42: Testing Key Pair for Encryption

(a) Type some arbitrary text in **Plaintext** and click **Test**.

The key pair is used to encrypt the plaintext. The encrypted text is then reversely decrypted again. If **Decrypted Text** matches **Plaintext**, the key pair works correctly for encryption/decryption. A green checkmark indicates the test completed successfully, otherwise you will receive an error message.

(b) When you have finished testing for encryption, click **Next**.

5. To test for signing and verifying operation do the following:

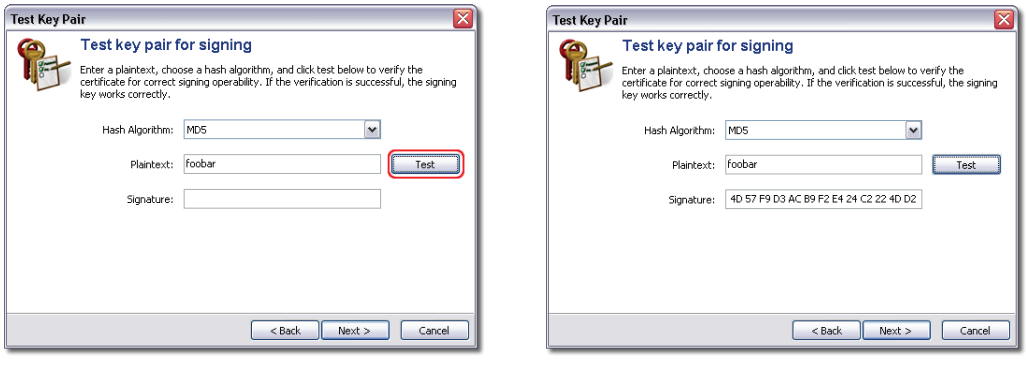

Figure 43: Testing Key Pair for Signing

(a) Type some arbitrary text in **Plaintext**.

(b) Select a hash algorithm in the **Hash Algorithm** list and click **Test**.

The key pair is used to create a signature for the plaintext based on the selected hash algorithm. The signature is then verified for validity. A green checkmark indicates the test completed successfully, otherwise you will receive an error message.

(c) When you have finished testing, click **Next**.

6. Verify the test results and click **Close**.

4.5.3 Additional considerations

- If you try to test a single key instead of a key pair (e.g. because only one key was created during an unsuccessful enrollment), you will get an appropriate error message.

4.5.4 Additional references

- Appendix: PKI and Certificate Basics

5 Managing Authentication Objects

This chapter gives an overview of authentication objects and how to manage them on a token using **DP CertiID Management Application**.

It covers the following topics:

- Understanding Authentication Objects
- Changing PINs
- Changing PUKs
- Changing Administrator Keys
- Unblocking PINs
- Changing the Security of Objects
- Removing the PIN Protection
- Replacing a PUK with an Administrator Key
- Generating Master Administrator Keys
- Using the Response Calculator

5.1 Understanding Authentication Objects

This section provides an overview of different types of authentication mechanisms, which will help you to gain a better understanding of the software. It further introduces some term definitions that are frequently used in DIGIPASS CertiID, both in the software and in the user documentation. If you are new to PKI software, it is recommended that you read this section carefully.

5.1.1 Data objects

Data on a token is organized similarly to data on a computer disk. Some objects (or files in the analogy) contain user data. Such an object is called **data object** and can be, for example, a certificate.

5.1.2 Key objects

Key objects are special data objects used for cryptographic operations. For instance, public key encryption uses pairs of cryptographic keys, consisting of a **public key** and a **private key**.

5.1.3 Authentication objects

Access to certain objects may be protected or supposed to be protected, for example, the private key of a key pair should not be publicly accessible. The access to such data objects worth protecting is protected by so-called **authentication objects** (or **authentication codes**).

CertiID distinguishes between four different types of authentication objects:

- Personal identification numbers (PIN)
- Personal unblocking keys (PUK)
- External authentication objects (administrator keys)
- Reset codes

As a measure of security, an authentication object is blocked after a certain number of incorrect authentication attempts. For instance, if you enter an incorrect PIN three times in a row, it is blocked and no longer valid, meaning the data it protects cannot be accessed at all. The number of allowed retries is called the **retry counter**. All authentication objects have a separate retry counter.

5.1.3.1 Personal Identification Number (PIN)

The most basic authentication object is the **personal identification number (PIN)**. A PIN is a secret (numeric, alphanumeric, or Unicode) password ideally known only to the legitimate user and the token. Before you can

access a certificate (more precisely the private key associated with the certificate), e.g. to use it for a signing operation, you are required to provide the respective PIN. Only after you typed the correct PIN, the data object can be used for the desired operation.

A token may contain more than one PIN, protecting different data objects. It may also contain a **default PIN**, i.e. a PIN object that is used by default to protect newly created data object. The default PIN is a regular PIN object with the label PIN. For example, if you enrol a certificate with a private key on the token, access to it is automatically protected by the default PIN (but can be changed afterwards).

If you enter an incorrect PIN several times in a row, it is blocked and the data it protects can no longer be accessed. A blocked PIN must be unblocked in order to access the protected data again.

5.1.3.2 Personal Unblocking Key (PUK)

To unblock a blocked PIN you need to provide an **unblock code**. The unblock code is either a **personal unblocking key (PUK)** or an **unblock response**. A PUK, similar to a PIN, is a secret (numeric, alphanumeric, or Unicode) password. When data protected by a blocked PIN is accessed, the PUK is requested to unblock (and reset) the PIN first.

A PUK can be used to unblock one or more PINs on a token. A token can contain more than one PUK. It may also contain a **default PUK**, i.e. a PUK object that is used by default to unblock the default PIN (and other PIN objects). The default PUK is a regular PUK object with the label PUK.

If you enter an incorrect PUK several times in a row, it is blocked and can no longer be used to unblock the associated PINs. A blocked PUK cannot be unblocked!

5.1.3.3 Administrator Key

An unblock response is calculated via **external authentication**. The basic principle is that the token creates a so-called **challenge**. Using that challenge with the **administrator key**, a **response** is calculated. This is often done by the system or token administrator. The response is then typed and verified by the token. If it is correct, the PIN is unblocked. Depending on the token capabilities, the administrator key is usually either 16 or 24 bytes long.

An administrator key can be used to unblock one or more PINs on a token. A token can contain one administrator key.

TIP
The advantage of administrator keys is that the token user does not necessarily need to know the administrator key to unblock a PIN, but only the response created with it. This allows scenarios, where the PIN is only known by the user, while the administrator key is known only by the system or token administrator, which is not possible with a PUK.
Since the token generates a different challenge each time, the respective response is valid only one time and could not be misused by some unauthorized person gaining knowledge of it!

If you enter an incorrect administrator key several times in a row, it is blocked and can no longer be used to unblock the associated PINs. A blocked administrator key cannot be unblocked!

5.1.3.4 Reset Code

If desired, a **reset code** may be set when initializing a token. The reset code protects a token from unauthorized deletion. The reset code is optional. If you want to reset a protected token, you are required to type the reset code.

If you enter an incorrect reset code several times in a row, it is blocked and can no longer be used to reset the token. A blocked reset code cannot be unblocked! A token with a blocked reset code can no longer be reset!

Feature	PIN	PUK	Administrator key	Reset code
Purpose	Protect data objects	Unblock PINs	Unblock PINs (via challenge/ response)	Reset token
Retry counter	Yes	Yes	Yes	Yes
Can be unblocked	Yes	No	No	No
Maximum number per token	*n*	*n*	1	1
Length	Policy dependent	Policy dependent	16 – 24 bytes	up to 16 chars

Table 1: Authentication Codes (Overview)

5.1.4 Master Administrator Key

A **master administrator key** is a secret key used to derive an actual administrator key. It is used to implement the concept of **administrator tokens**. Instead of typing the administrator key directly when needed, the token with the respective master administrator key is required. After successful authentication with the PIN, the master administrator key is used to derive the administrator key.

This introduces an additional level of security as the actual administrator key is unknown. Furthermore, to use an administrator key an additional physical device is required, i.e. the administrator token. A master administrator key itself may be protected with a PIN.

One master administrator key is used to derive exactly one administrator key. Since a master administrator key is basically a secret key object, a token can contain several master administrator keys.

5.1.5 Examples

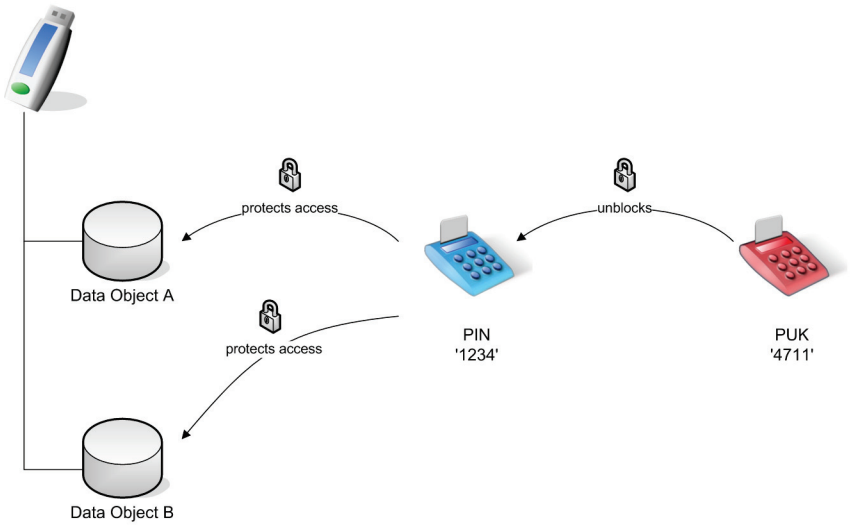

Figure 44: Two Data Objects protected by a PIN that is unblocked by a PUK (Example)

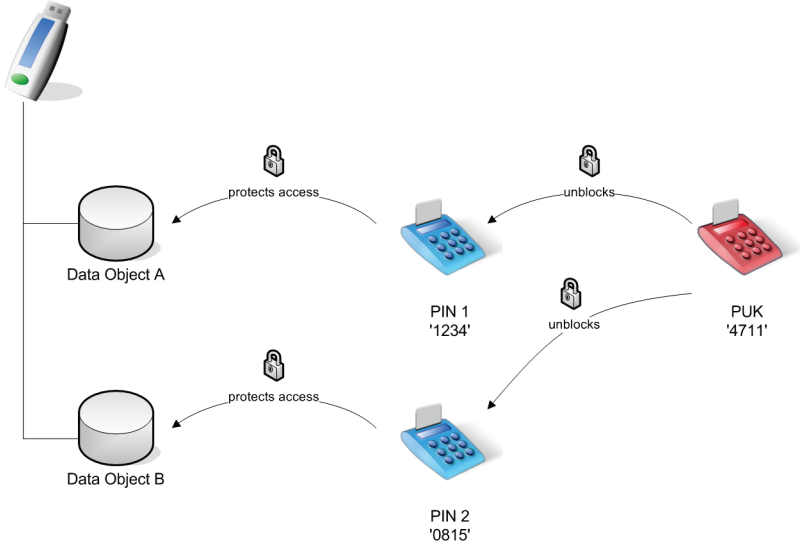

Figure 45: Two Data Objects protected by two different PINs that are unblocked by one PUK (Example)

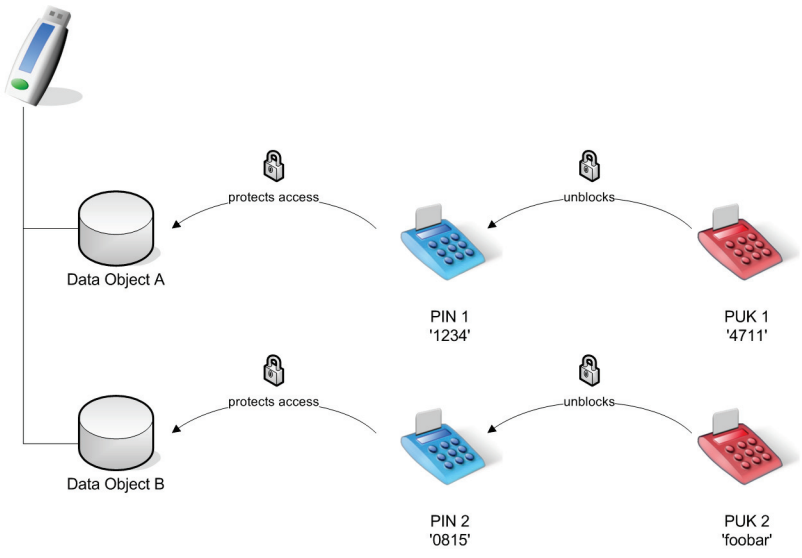

Figure 46: Two Data Objects protected by two different PINs that are each unblocked by two different PUKs (Example)

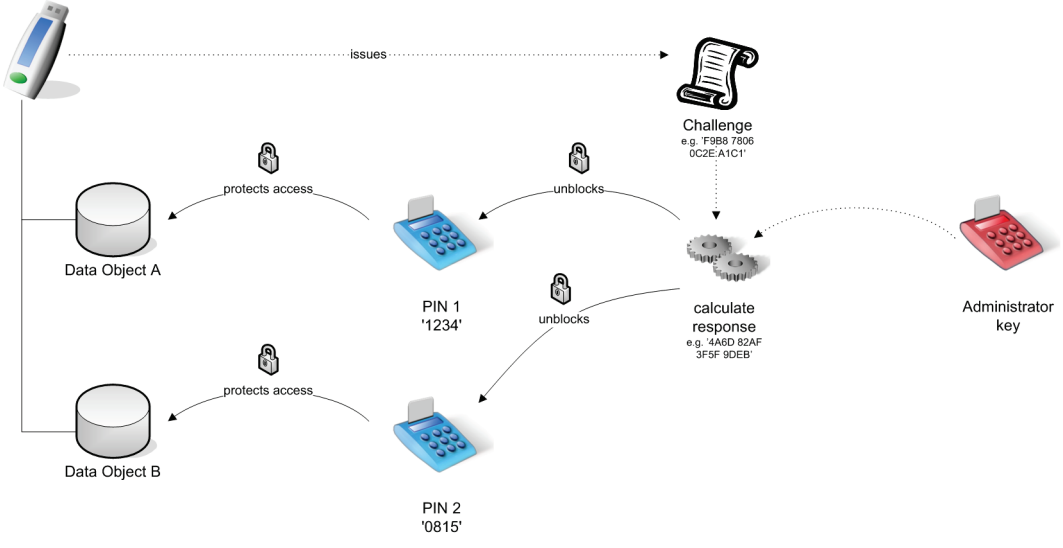

Figure 47: Two Data Objects protected by two different PINs that are unblocked via external authentication (Example)

5.1.6 Additional references

- Changing the Security of Objects
- Initializing Tokens

5.2 Changing PINs

A **personal identification number (PIN)** protects certain data objects, such as certificates, from unauthorized access. By changing your PINs regularly, you can keep the data on your token more secure.

> NOTE
> You should change your PIN immediately, if you suspect that it has been compromised, guessed, or revealed by someone else!

5.2.1 Before you begin

To change a PIN you need:

- **DP CertiID Management Application**
- the current PIN
- to choose a strong PIN that can't be easily guessed, but still easily remembered by you

> **CAUTION**
> Do not record your PIN either in writing or electronically and do not disclose it to anyone (including supervisors or co-workers)!

5.2.2 Changing a PIN

➢ To change a PIN

1. Insert your token.
2. Select the PIN to be changed in the token explorer tree.
3. Select **Change** from the shortcut menu.

   -OR-

   Select **Tasks > Change** from the menu bar.
   The **Change PIN Dialog** appears.

Figure 48: Changing PIN

4. Type the current PIN and a new PIN two times to prevent typing errors.
5. Click **Change**.

   Change remains disabled until the new PIN complies with the effective PIN policy!

TIP
Click **View Details** to show the effective PIN policy to see why the specified PIN does not comply with it.

5.2.3 Additional considerations

- The system or token administrator may enact a PIN policy to encourage and enforce strong PINs.
- The **Authentication Objects** folder in the token explorer tree contains all PINs on a particular token. The PIN effectively assigned to protect a certain private key is shown below the private key of the respective certificate.

5.2.4 Additional references

- Unblocking PINs
- Changing PUKs
- PIN Policy Rules
- Changing the Security of Objects
- Understanding Authentication Objects

5.3 Changing PUKs

Similar to your PINs, you can change your PUKs.

NOTE
You should change your PUK immediately, if you suspect that it has been compromised, guessed, or revealed by someone else!

5.3.1 Before you begin

To change a PUK you need:

- **DP CertiID Management Application**
- the current PUK
- to choose a strong PUK that can't be easily guessed, but can still easily be remembered by you

CAUTION
If you need to record your PUK either in writing or electronically, store it in a secure place!

Do not disclose it to anyone (including supervisors or co-workers)!

CAUTION
If you consecutively enter an incorrect PUK too many times, it is blocked!

You **cannot** unblock a blocked PUK, thus losing the possibility to unblock the assigned PINs!

5.3.2 Changing a PUK

➢ To change a PUK

1. Insert your token.
2. Select the PUK to be changed in the token explorer tree.
3. Select **Change** from the shortcut menu.

   -OR-

   Select **Tasks > Change** from the menu bar.

   The **Change PUK Dialog** appears.

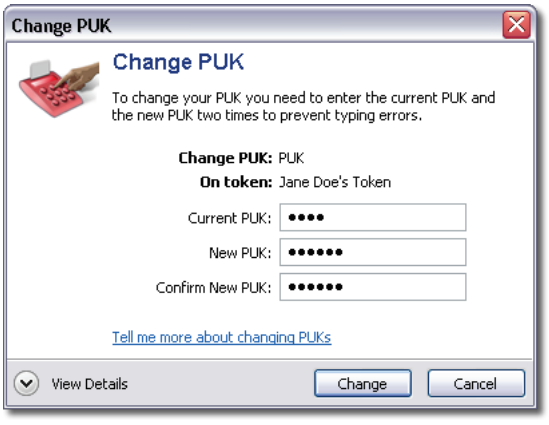

Figure 49: Changing PUK

4. Type the current PUK and a new PUK two times to prevent typing errors.
5. Click **Change**.

   Change remains disabled until the new PUK complies with the effective PUK policy!

TIP
Click **View Details** to show the effective PUK policy to see why the specified PUK does not comply with it.

5.3.3 Additional considerations

- The system or token administrator may enact a PUK policy to encourage and enforce strong PUKs.
- The **Authentication Objects** folder in the token explorer tree contains all PUKs on a particular token. The PUK effectively assigned to unblock a certain PIN is shown along with the respective PIN below the private key of the respective certificate.
- Changing a PUK does not affect the PIN that is unblocked with the PUK.

5.3.4 Additional references

- Unblocking PINs
- Changing PINs
- Changing Administrator Keys
- PUK Policy Rules
- Changing the Security of Objects
- Understanding Authentication Objects

5.4 Changing Administrator Keys

Similar to your PINs and PUKs, you can change your administrator key. However, due to their nature, changing an administrator key requires a response calculated based on a challenge issued by the token.

NOTE
You should change your administrator key immediately, if you suspect that it has been compromised, guessed, or revealed by someone else!

5.4.1 Before you begin

To change an administrator key you need:

- **DP CertiID Management Application**
- the current administrator key

  -OR-

  the master administrator key

  If you do not know your administrator key or don't possess the master administrator key, you should contact your token administrator.

CAUTION
If you need to record your administrator key either in writing or electronically, store it in a secure place!

Do not disclose it to anyone (including supervisors or co-workers)!

CAUTION
If you consecutively enter an incorrect administrator key too many times, it is blocked!

You **cannot** unblock a blocked administrator key, thus losing the possibility to unblock the assigned PINs via external authentication!

5.4.2 Changing an administrator key

➢ To change an administrator key

1. Insert your token.
2. Select the administrator key to be changed in the token explorer tree.

3. Select **Change** from the shortcut menu.

   -OR-

   Select **Tasks > Change** from the menu bar.

   The **Change Administrator Key Dialog** appears.

Figure 50: Changing Administrator Key (1)

4. Do one of the following:

   - If you know the current administrator key

     (a) Click **Generate response**  .

     The **Enter Administrator Key Dialog** appears.

Figure 51: Entering Administrator Key

(b) Type the administrator key and click **OK** to return to the **Change Administrator Key Dialog**.

The response is calculated using the provided administrator key and automatically entered into the **Response** box.

- If you possess the master administrator key

  (a) Insert the administrator token.

  (b) Select **Use master administrator key**.

  (c) Select the master administrator key in the **Master key** list.

  (d) Type the PIN for the master administrator key and click **OK** to return to the **Change Administrator Key Dialog**.

  The response is calculated using the provided administrator key and automatically entered into the **Response** box.

- If you do not know the administrator key, contact your token administrator and read the challenge information shown in the **Challenge** box in the **Change Administrator Key Dialog** to receive the response.

5. Type a new administrator key in the **New administrator key** box.

Figure 52: Changing Administrator Key (2)

6. Click **Change**.

Change is disabled, if either the **Response** box or the **New administrator key** box is empty.

5.4.3 Additional considerations

- The **Authentication Objects** folder in the token explorer tree contains all authentication objects on the token, including the administrator key. If the administrator key is assigned to protect a PIN, it is shown along with the PIN below the private key of the respective certificate.

- Changing an administrator key does not affect the PIN that is unblocked using the administrator key.

If you are the token administrator:

- You can use the response calculator (available via **Tools > Response Calculator** in the **DP CertiID Management Application** menu bar) to calculate a response for a challenge requested by a user.
- You can generate master administrator keys to derive secret administrator keys.

5.4.4 Additional references

- Unblocking PINs
- Changing PUKs
- Changing the Security of Objects
- Generating Master Administrator Keys
- Understanding Authentication Objects
- Using the Response Calculator

5.5 Unblocking PINs

If you consecutively enter a wrong PIN too many times, the PIN is blocked to prevent an unauthorized person from checking all possible PIN combinations by trial and error.

To access the data objects protected by the PIN again, you need to unblock the PIN first by entering an unblock code. The unblock code may be a **personal unblocking key (PUK)** or an **unblock response** calculated via external authentication.

Whether you need a PUK or an unblock response to unblock a PIN is determined by the type of authentication object, which is assigned to unblock the PIN.

5.5.1 Before you begin

To unblock a PIN you need:

- **DP CertiID Management Application**
- the respective unblock code.
  If you do not know your unblock code, contact your token administrator.

CAUTION
Do not record your PIN either in writing or electronically and do not disclose it to anyone (including supervisors or co-workers)!

CAUTION
If you consecutively enter an incorrect PUK or an incorrect administrator key to unblock a PIN too many times, the PUK or the administrator key is blocked as well!

You **cannot** unblock a blocked PUK or a blocked administrator key, thus losing the possibility to unblock the assigned PIN!

5.5.2 Unblocking a PIN with a PUK

➢ To unblock a PIN with a PUK

1. Insert your token.
2. Select the PIN to be unblocked in the token explorer tree.
3. Select **Unblock** from the shortcut menu.

   -OR-

Select **Tasks > Unblock PIN** from the menu bar.

The **Unblock PIN Dialog** appears requiring you to enter a PUK.

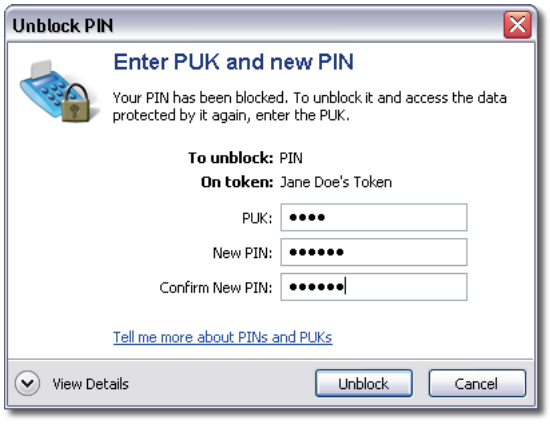

Figure 53: Unblocking PIN with a PUK

4. Type the required PUK and a new PIN two times to prevent typing errors.
5. Click **Unblock**.

   Unblock remains disabled until the new PIN complies with the effective PIN policy!

TIP
Click **View Details** to show the effective PIN policy to see why the specified PIN does not comply with it.

5.5.3 Unblocking a PIN with external authentication

➢ To unblock a PIN using an unblock response

1. Insert your token.
2. Select the PIN to be unblocked in the token explorer tree.
3. Select **Unblock** from the shortcut menu.

   -OR-

   Select **Tasks > Unblock PIN** from the menu bar.

   The **Unblock PIN Dialog** appears requiring you to enter a response (unblock code).

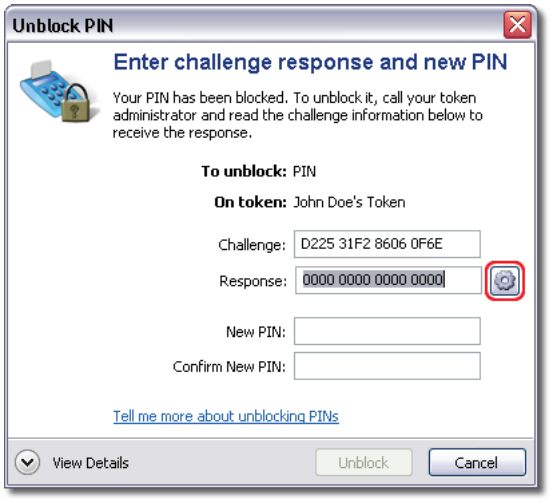

Figure 54: Unblocking PIN with an Administrator Key (1)

4. Do one of the following:

   - If you know the respective administrator key

     (a) Click **Generate response** .

     The **Enter Administrator Key Dialog** appears.

Figure 55: Entering Administrator Key

     (b) Type the administrator key and click **OK** to return to the **Unblock PIN Dialog**.

     The response is calculated using the provided administrator key and automatically entered into the **Response** box.

   - If you possess the master administrator key

(a) Click **Generate response**.

The **Enter Administrator Key Dialog** appears.

(b) Insert the administrator token.

(c) Select **Use master administrator key**.

(d) Select the master administrator key in the **Master key** list.

(e) Type the PIN for the master administrator key and click **OK** to return to the **Change Administrator Key Dialog**.

The response is calculated using the provided administrator key and automatically entered into the **Response** box.

- If you do not know the administrator key, contact your token administrator and read the challenge information shown in the **Challenge** box in the **Unblock PIN Dialog** to receive the response.

5. Type a new PIN twice to prevent typing errors.

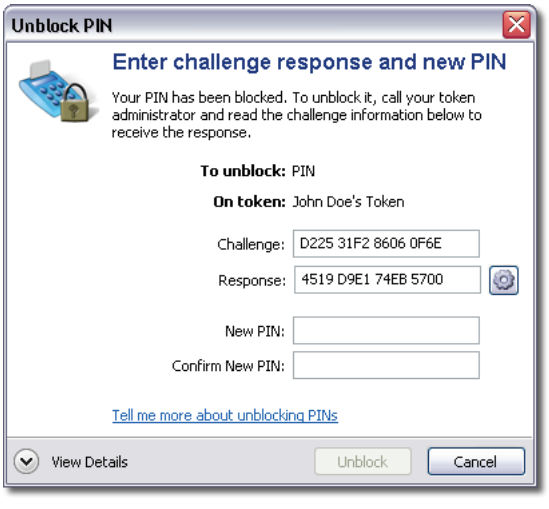

Figure 56: Unblocking PIN with an Administrator Key (2)

6. Click **Unblock**.

Unblock remains disabled until the new PIN complies with the effective PIN policy!

TIP
Click **View Details** to show the effective PIN policy to see why the specified PIN does not comply with it.

5.5.4 Additional considerations

- The **Unblock PIN Dialog** appears automatically, if you try to access a data object protected by a blocked PIN.
- The retry counter of the PIN is automatically reset to its initial value, after a successful unblock.
- The system or token administrator may enact a PIN policy to encourage and enforce strong PINs.
- The **Authentication Objects** folder in the token explorer tree contains all PINs on a particular token. The PIN effectively assigned to protect a certain certificate is shown below the private key of the respective certificate.

If you are the token administrator:

- You can use the response calculator (available via **Tools > Response Calculator** in the menu bar) to create a response for a challenge requested by a user.
- You can generate master administrator keys to derive secret administrator keys.
- You can specify support contact information that is displayed in the Unblock PIN Dialog (via **DP CertiID Configuration Center**), so users may discover who to contact if their PIN is blocked.

5.5.5 Additional references

- Changing PUKs
- Changing Administrator Keys
- Replacing a PUK with an Administrator Key
- Understanding Authentication Objects
- Using the Response Calculator
- Configuring DIGIPASS CertiID

5.6 Changing the Security of Objects

You can have more than one PIN object on a token, each protecting different data objects. If you enroll a certificate to a token, its private key is automatically protected by the default PIN, if the token contains a default PIN. If desired, you may assign a different PIN to the private key.

Using different PINs for different data objects potentially increases security. However, consider that you

- need to keep track of and remember several PINs
- choose strong PINs that can't be easily guessed, but still can easily be remembered by you

5.6.1 Before you begin

To assign a different PIN you need:

- **DP CertiID Management Application**
- the current PIN
- to choose a strong PIN that can't be easily guessed, but still can easily be remembered by you

CAUTION
Do not record your PIN either in writing or electronically and do not disclose it to anyone (including supervisors or co-workers)!

5.6.2 Assigning a PIN

You assign a different PIN via the **Change Object Security Wizard**.

➢ To invoke the Change Object Security Wizard

1. Select the data object to which you want to assign a PIN in the token explorer tree.
2. Select **Change object security** from the shortcut menu.

   -OR-

   Select **Tasks > Change object security** from the menu bar.

With the **Change Object Security Wizard** you can either

- assign an existing PIN to the data object or
- create a new PIN and assign it to the data object.

➢ To assign an existing PIN

1. Invoke the **Change Object Security Wizard** (see above).
2. Select **Use an existing PIN** and click **Next**.

Figure 57: Changing Object Security – Using Existing PIN (1)

3. Select an existing PIN in the **PIN** box and click **Next**.

Figure 58: Changing Object Security - Using Existing PIN (2)

4. Click **Finish**.

   From now on, the selected PIN is requested to access the data object.

➢ To create and assign a new PIN

1. Invoke the **Change Object Security Wizard** (see above).
2. Select **Create new PIN** and click **Next**.

Figure 59: Changing Object Security – Generating New PIN

3. Specify the value and retry counter for the new PIN.

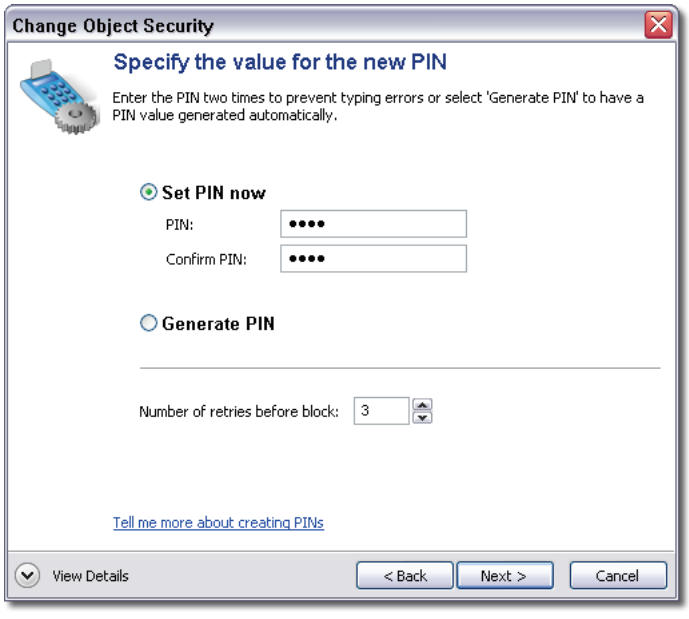

Figure 60: Changing Object Security – Specifying New PIN

- Select **Set PIN now** and type a value for the PIN twice to prevent typing errors.

  Next remains disabled until the new PIN complies with the effective PIN policy!

TIP
Click **View Details** to show the effective PIN policy to see why the specified PIN does not comply with it.

- Select **Generate PIN** to have a PIN automatically generated for you.

  The generated PIN value is displayed after the wizard has performed the requested actions. It will also be shown in the PIN letter, if you request to print one (see Step 8).

  The **Number of retries before block** box defines, how often an incorrect value for the PIN can be consecutively typed, before it is blocked and needs to be unblocked.

4. Specify a label for the new PIN.

   The PIN label is the name used to refer to this PIN helping to distinguish between different PINs.

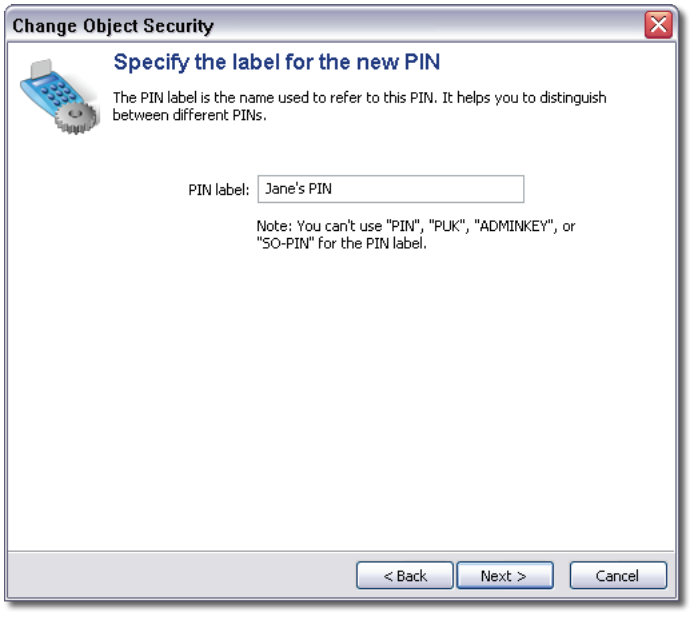

Figure 61: Changing Object Security – Specifying PIN Label

NOTE
The PIN label can't be set to PIN, PUK, ADMINKEY, or SO-PIN, as these labels are reserved for the default PIN, the default PUK, and the administrator key, respectively.

PKCS #11 refers to the PUK as SO-PIN.

5. Select how to unblock the PIN.

Figure 62: Changing Object Security – Specifying Unblock Mechanism

- Select **Use default PUK** to use the default PUK to unblock the PIN, if it is blocked.

  This option is only available, if a default PUK exists on the token.

  Continue with Step 8.
- Select **Generate new PUK**, if you want to create a new PUK object to unblock the new PIN.
- Select **Use administrator key** to use external authentication using the administrator key to unblock the new PIN.

  This option is only available, if an administrator key exists on the token.

  Continue with Step 8.

6. Specify the value and retry counter for the new PUK.

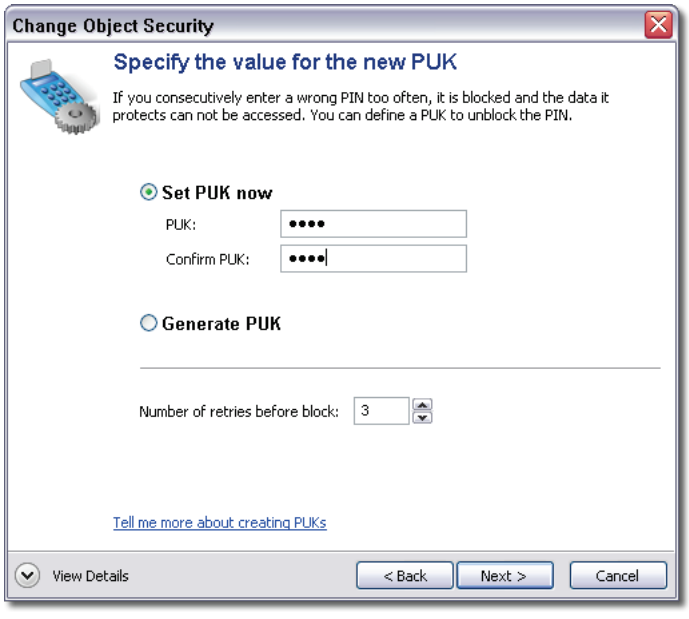

Figure 63: Changing Object Security – Specifying New PUK

- Select **Set PUK now** and type a value for the PUK twice to prevent typing errors.

  Next remains disabled until the new PUK complies with the effective PUK policy!

TIP
Click **View Details** to show the effective PUK policy to see why the specified PUK does not comply with it.

- Select **Generate PUK** to have a PUK automatically generated for you.

  The generated PUK value is displayed after the wizard has performed the requested actions. It will also be shown in the PIN and/or PUK letter, if you request to print one (see Step 8).

  The **Number of retries before block** box defines, how often an incorrect value for the PUK can be consecutively typed, before it is blocked.

7. Specify a label for the new PUK.

   The PUK label is the name to refer to this PUK helping to distinguish between different PUKs.

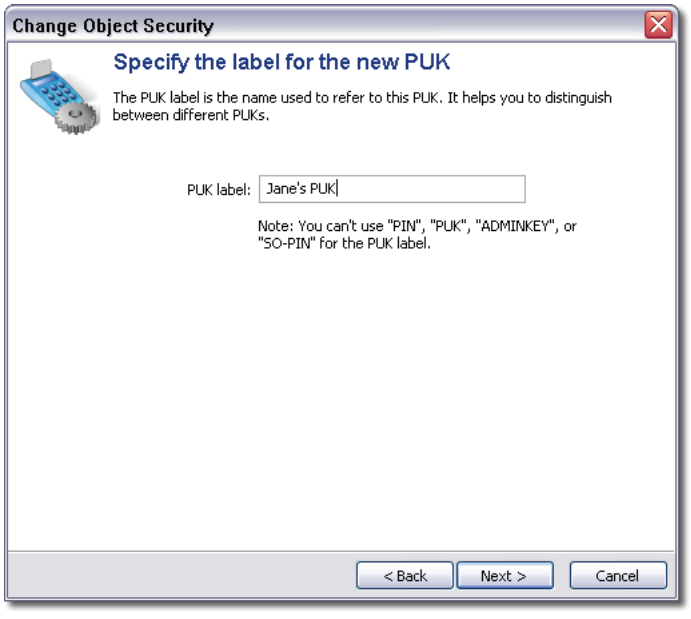

Figure 64: Changing Object Security – Specifying PUK Label

NOTE
The PUK label can't be set to PIN, PUK, ADMINKEY, or SO-PIN, as these labels are reserved for the default PIN, the default PUK, and the administrator key, respectively!

PKCS #11 refers to the PUK as SO-PIN.

8. Specify whether you want a PIN and/or a PUK letter to be printed on the selected printer.

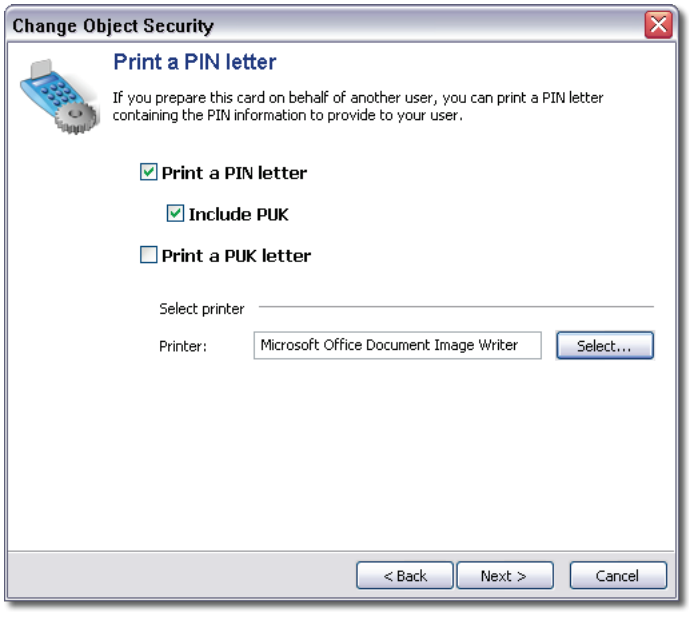

Figure 65: Changing Object Security – Printing PIN/PUK Letter

9. Click **Finish**.

5.6.3 Additional considerations

- The system or token administrator may restrict access to certain program features. If a particular option is not available, you may not have the privileges to use it.
- Assigning a different PIN to a data object is not the same as changing a PIN. If you assign a different PIN, you replace the current PIN object by another PIN object. If you change a PIN, you change the value of that PIN object.
- The previous PIN remains on the token after assigning another PIN to a data object, even if the previous PIN does not protect any other data objects.
- It is not recommended to use different PINs (other than the default PIN) with PKCS #11, since some PKCS #11 applications do not support context-specific authentication, including Mozilla Thunderbird 2.x.
- Assigning a different PIN to a data object does not affect the protection of other data objects.
- The system or token administrator may enact a PIN/PUK policy to encourage and enforce strong PINs and PUKs.

5.6.4 Additional references

- Removing the PIN Protection
- Understanding Authentication Objects
- Access Configuration

5.7 Removing the PIN Protection

You can remove the PIN protection of a particular data object. If you remove the PIN protection from a data object, it becomes accessible to anyone without any authentication.

CAUTION
It is recommended not to use this option! It removes the PIN protection from a data object allowing anyone (including unauthorized persons) to use the data without any prior authentication!

5.7.1 Before you begin

Due to its potential security risk, this option is unavailable by default and must be enabled in the program access conditions.

To remove the PIN protection from a data object you need:

- **DP CertiID Management Application**
- the current PIN

5.7.2 Removing a PIN

➢ To remove the PIN protection from a data object

1. Insert your token.
2. Select the data object currently protected in the token explorer tree.
3. Select **Change object security** from the shortcut menu.

   -OR-

   Select **Tasks > Change object security** from the menu bar.

   The **Change Object Security Wizard** appears.
4. Select **Remove current PIN** and click **Next**.
5. Click **Finish** to confirm removing the PIN protection.

5.7.3 Additional considerations

- The system or token administrator may restrict access to certain program features. If the remove PIN protection option is unavailable, you may not have the privileges to use it.
- Removing the PIN protection is not the same as removing the PIN object. The PIN object remains on the token.
- Removing the PIN protection of one data object does not affect the PIN protection of other data objects.
- You can only remove the link between a PIN object and a data object. You cannot remove a PIN object itself from the token!

5.7.4 Additional references

- Changing the Security of Objects
- Access Configuration
- Understanding Authentication Objects

5.8 Replacing a PUK with an Administrator Key

You can change the way a PIN is unblocked, by replacing the assigned PUK with an administrator key. If the PIN is blocked afterwards, it must be unblocked via external authentication using the administrator key instead of the PUK.

5.8.1 Before you begin

Using external authentication instead of a PUK, potentially increases security and allows the help desk to unblock PINs for user tokens remotely without disclosing the unblock secret, i.e. the administrator key.

However, consider that you

- need to keep the administrator key in a secure place
- choose a strong administrator key that can't be guessed
- can't switch back from an administrator key protection to PUK protection

To replace a PUK with an administrator key you need:

- **DP CertiID Management Application**
- the current PUK

CAUTION
If you need to record your administrator key either in writing or electronically, store it in a secure place!

Do not disclose it to anyone (including supervisors or co-workers)!

5.8.2 Replacing a PUK with an administrator key

➢ To replace a PUK with an administrator key

1. Insert your token.
2. Select the PUK you want to replace with an administrator key in the token explorer tree.
3. Select **Replace with administrator key** from the shortcut menu.

   -OR-

   Select **Tasks > Replace with administrator key** from the menu bar.

The **Replace PUK with Administrator Key Dialog** appears.

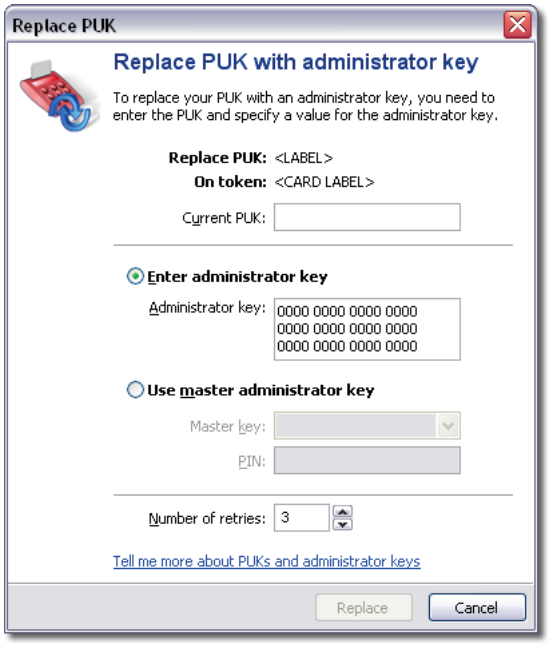

Figure 66: Replacing PUK with Administrator Key

4. Type the PUK in the **Current PUK** box
5. Do one of the following:
   - If you want to specify the administrator key
     (a) Select **Enter administrator key**.
     (b) Type the administrator key.
     (c) Specify the retry counter.

     The **Number of retries before block** box defines, how often an incorrect value for the administrator key can be consecutively typed, before it is blocked.
   - If you want to use a master administrator key
     (a) Insert the administrator token.
     (b) Select **Use master administrator key**.
     (c) Select the master administrator key in the **Master key** list.
     (d) Type the PIN for the master administrator key.
     (e) Specify the retry counter.

The **Number of retries before block** box defines, how often an incorrect value for the administrator key can be consecutively typed, before it is blocked.

- If an administrator key already exists on the token, it is assigned to unblock the particular PIN. In this case, you can't specify a value for the administrator key.

6. Click **Replace**.

If no administrator key exists on the token, it is created and assigned to unblock the particular PIN.

5.8.3 Additional considerations

- The system or token administrator may restrict access to certain program features. If the replace PUK option is not available, you may not have the privileges to use it.
- The previous PUK object remains on the token after replacing it with an administrator key.
- If you replace the PUK protection of a PIN, the protection is only changed for that particular PIN. It does not affect any other PIN objects unblocked by the same PUK.
- You can replace a PUK with an administrator key, but not vice versa.
- You cannot remove a PUK object itself from the token. Neither can you remove the administrator key itself from the token.
- You can generate master administrator keys to derive secret administrator keys.

5.8.4 Additional references

- Changing the Security of Objects
- Generating Master Administrator Keys
- Access Configuration
- Understanding Authentication Objects

5.9 Generating Master Administrator Keys

A **master administrator key** is a secret key used to derive an actual administrator key. Instead of typing the administrator key directly when needed, the token with the respective master administrator key is required. After successful authentication with the PIN, the master administrator key is used to derive the administrator key.

5.9.1 Before you begin

To generate a master administrator key you need:

- **DP CertiID Management Application**

TIP
Although you can put master administrator keys on any token you like, it is highly recommended to use a designated token solely for the purpose of storing master administrator keys.

5.9.2 Generating a master administrator key

➢ To generate a master administrator key

1. Insert your administrator token.
2. Select the **Secret Key Objects** folder in the token explorer tree.
3. Select **Generate master administrator key** from the shortcut menu.

   -OR-

   Select **Tasks > Generate master administrator key** from the menu bar.

   The **Generate Master Administrator Key Dialog** appears.

Figure 67: Generating Master Administrator Key

4. Type a key label.

   The key label is the name to refer to the key to distinguish between different master administrator keys.

5. Type a passphrase.

   The passphrase is used to calculate the master administrator key. The more random and complex the passphrase the more random and secure the master administrator key.

6. Click **Generate**.

5.9.3 Additional considerations

- The system or token administrator may restrict access to certain program features. If the generate master administrator key option is not available, you may not have the privileges to use it.
- The passphrase is used only once to generate the master administrator key. You do not need it to use or access the master administrator key once it has been generated.
- One particular passphrase generates exactly one particular master administrator key value. If the token with a master administrator key is damaged, you can re-create the master administrator key using the original passphrase. You can also create multiple cards with the same muster administrator key using one passphrase, e.g. for different helpdesk members.
- Basically, a master administrator key is a secret key. The **Secret Key Objects** folder in the token explorer tree contains all secret keys (and all master administrator keys).
- Administrator token is a theoretical term. Any token containing master administrator keys is an administrator token, but can be used normally like any other token. However, it is highly recommended to use a designated token solely for the purpose of storing master administrator keys.

5.9.4 Additional references

- Access Configuration
- Understanding Authentication Objects

5.10 Using the Response Calculator

The response calculator is a tool allowing you to calculate a response for a given challenge using an administrator key. It is primarily intended for token administrators or help desk staff that need to remotely help users to unblock PINs protected by administrator keys.

The response calculator is available via **Tools > Response Calculator** in the **DP CertiID Management Application** menu bar.

5.10.1 Before you begin

To use the response calculator you need:

- **DP CertiID Management Application**
- the administrator key of the token that issued the respective challenge

  -OR-

  the master administrator key

5.10.2 Using the response calculator

➢ To calculate a response with the response calculator

1. Select **Tools > Response Calculator** in the menu bar.

   The **Response Calculator Dialog** appears.

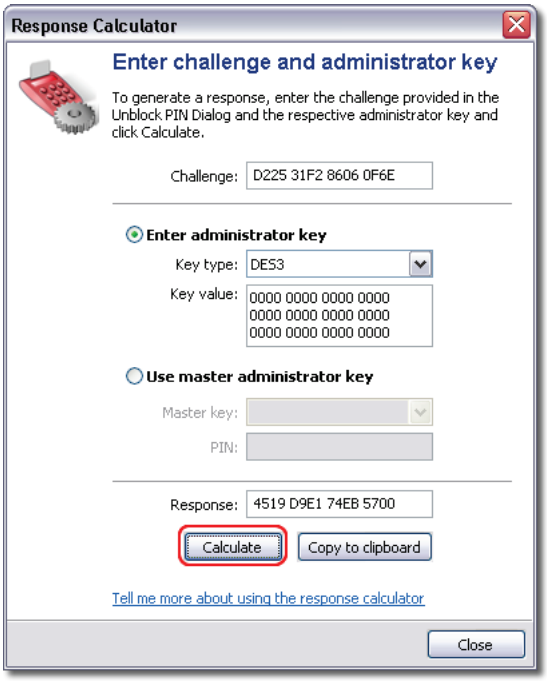

Figure 68: Using Response Calculator

2. Type the challenge given in the **Unblock PIN Dialog** in the **Challenge** box.
3. Do one of the following:
   - If you know the current administrator key
     (a) Select **Enter administrator key**.
     (b) Select the administrator key type in the **Key Type** list.
     (c) Type the administrator key for the respective token in the **Administrator key** box.
   - If you possess the master administrator key
     (a) Insert the administrator token.
     (b) Select **Use master administrator key**.
     (c) Select the master administrator key in the **Master key** list.
     (d) Type the PIN for the master administrator key.
4. Click **Calculate**.

   The response is calculated and returned in the **Response** box. If you are the token administrator, you may read the response to the user on the phone or click **Copy to clipboard** to copy and paste the response code into another application and provide it to the user, e.g. via E-mail.

5.10.3 Additional considerations

- You don't need a token connected to use the response calculator, except for the administrator token (if required).
- Since tokens generate a different challenge each time, the respective response is valid only one time and could not be misused by some unauthorized person gaining knowledge of it!

5.10.4 Additional references

- Unblocking PINs
- Changing Administrator Keys
- Understanding Authentication Objects

6 Using the DP CertiID Tray Agent

This chapter gives an overview of **DP CertiID Tray Agent** and how to use it.

It covers the following topics:

- Introduction
- Getting to Know the DP CertiID Tray Agent Icon

6.1 Introduction

The **DP CertiID Tray Agent** is an application that adds itself to the notification area. Its functionality can be extended via plug-ins.

Depending on the installed plug-ins, **DP CertiID Tray Agent** performs the following tasks:

- Registering/unregistering certificates
- Generating/viewing one-time passwords (OTP) using OTP-capable hardware tokens
- Displaying the smart card reader and token status via a notification area icon

6.1.1 Registering and unregistering certificates

Registering a certificate means adding it to the appropriate certificate store on the machine. A certificate store is the system area where certificates are stored locally by the operating system and made accessible for applications using cryptographic services, e.g. e-mail applications.

NOTE
If you install a CA certificate, you confirm that you explicitly trust this CA and any certificate issued by it. Due to the impact (and security risks) of this, Microsoft Windows may display a security warning, when **DP CertiID Tray Agent** tries to register a certificate for a CA. Microsoft Windows registers the CA certificate only, if you confirm that you trust the respective CA.

Unregistering a certificate means removing it from the certificate store.

DP CertiID Tray Agent can be configured to automatically unregister all previously registered certificates of a token first, when the respective token is inserted. Then it automatically registers the certificates, which are configured to be automatically registered. When the token is removed, all certificates previously registered are automatically unregistered.

NOTE
The DP CertiID Tray Agent unregisters all smart card certificates, including those registered manually using the **DP CertiID Management Application**.

6.2 Getting to Know the DP CertiID Tray Agent Icon

The **DP CertiID Tray Agent** automatically adds an icon to the notification area, displaying the overall status of the CertiID middleware.

Figure 69: DP CertiID Tray Agent Notification Area

Tray Agent Icon	Meaning
	Status: OK. Smart card reader present, but no tokens connected
	Status: OK. At least one valid token connected
	Status: OK. At least one token is pre-initialized
	Status: OK. Certificate data is being read and registered
	Status: Attention. No smart card reader or token connected
	Status: Warning, e.g. the connected token is empty
	Status: Unknown token, i.e. at least one token is not supported
	Status: Error. At least one token is invalid or not responding

Table 2: Tray Agent Icon States (Overview)

TIP
If the **DP CertiID Tray Agent** icon is not present, it may be hidden. To show it again, launch **Start > Programs > VASCO > DIGIPASS CertiID > Tray Agent**!

If you right-click the **DP CertiID Tray Agent** icon, the shortcut menu opens.

Figure 70: DP CertiID Tray Agent Shortcut Menu

The shortcut menu contains:

- A list of all connected tokens and smart card readers
- Quick launch options to start important DP CertiID applications and tools
- Some options to show and hide the icon and the status hover pane and to exit DP CertiID Tray Agent

TIP
If you want to launch DP CertiID Management Application to explore a specific token directly, select the respective token in the shortcut menu!

6.2.1 Using the status hover pane

The status hover pane displays all connected tokens and smart card readers including their current status and provides quick access to common commands for the particular smart card readers and tokens. It further indicates, if system and/or user diagnostics is active.

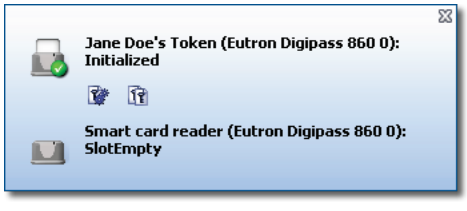

Figure 71: Status Hover Pane

➢ To show the status hover pane

- Select **View Hover Pane** in the shortcut menu.

  The status hover pane appears and remains visible, until you either click **Close** ☒.

The hover pane can appear automatically, if the token status changes. For instance, when a token is inserted or removed.

➢ To prevent the status hover pane to appear automatically

- Clear **View Status Changes** in the shortcut menu.

  The status hover pane will no longer automatically appear, when inserting or removing a token (or card reader).

6.2.2 Showing and hiding the DP CertiID Tray Agent icon

➢ To hide the DP CertiID Tray Agent icon permanently

- Select **Hide Tray Icon** in the shortcut menu.

  The **DP CertiID Tray Agent** icon disappears and remains hidden, even after a system reboot. However, certificates will still be automatically registered and unregistered.

  You can show the **DP CertiID Tray Agent** icon again by launching **Start > Programs > VASCO > DIGIPASS CertiID > Tray Agent**.

➢ To hide the DP CertiID Tray Agent icon temporarily

- Select **Exit** in the shortcut menu.

  The **DP CertiID Tray Agent** icon disappears and the DP CertiID Tray Agent is shut down. If configured, certificates are still automatically registered or unregistered. However, the DP CertiID Tray Agent is restarted after a system reboot.

6.2.3 Generating one-time passwords (OTP)

You can use DP CertiID Tray Agent to quickly generate and view one-time passwords (OTP) using OTP-capable hardware tokens or tokens with OTP key objects.

➢ To generate and view a one-time password (OTP)

1. Plug in your OTP token, e.g. DP860

2. Select **Generate One-Time Password (OTP)** from the shortcut menu.

   -OR-

   If you have more than one OTP tokens connected, select **<TOKEN> > Generate One-Time Password (OTP)** where <TOKEN> is the respective token.

   The **Generate OTP Dialog** appears.

Figure 72: Generating One-Time Password (OTP)

3. If required, type the PIN and click **OK**
4. Click **Generate** to generate a new OTP.

   The **OTP** box displays the current valid OTP. After a certain time span (default 30 seconds) the field changes to *Expired*.

5. Click **Copy** to copy the current OTP to the clipboard.

TIP
You can select **<TOKEN> > Generate One-Time Password (OTP) to Clipboard** to generate and copy a one-time password directly to the clipboard without opening the **Generate OTP Dialog**.

6.2.4 Additional references

- Using DP CertiID Management Application
- Access Configuration
- Appendix: Using DP CertiID with One-Time Passwords (OTP)

7 Configuring DIGIPASS CertiID

This chapter gives an overview of how to configure CertiID and describes what options can be set using **DP CertiID Configuration Center**.

It covers the following topics:

- Using Group Policy to configure DIGIPASS CertiID
- Using DP CertiID Configuration Center to configure DIGIPASS CertiID
- PIN Handling
- PIN Policy
- Certificate Handling
- Access Configuration

7.1 Using Group Policy to configure DIGIPASS CertiID

DIGIPASS CertiID includes Administrative Templates that provide policy information to configure DIGIPASS CertiID software affecting all or only a group of computers and users in a domain.

This section gives a brief overview of how to use Administrative Templates and use them to manage registry-based policy. For more information, refer to Windows Server Group Policy documentation on Microsoft TechNet (technet.microsoft.com).

7.1.1 Before you begin

To complete the following procedure, you need to be logged on with a user account with administrator privileges or an account that has Edit setting permission to edit a Group Policy Object (GPO).

> NOTE
> Settings configured via Group Policy take precedence over settings configured via DP CertiID Configuration Center.

7.1.2 Configuring DIGIPASS CertiID using Group Policy

➢ To configure DIGIPASS CertiID using Group Policy (Windows Server 2008)

1. Start **Group Policy Management** via command prompt by typing gpmc.msc.
2. Select the domain or organizational unit for which you want to set a group policy in the group policy management tree.

3. Select **Create a GPO in this domain, and Link it here** from the context menu.

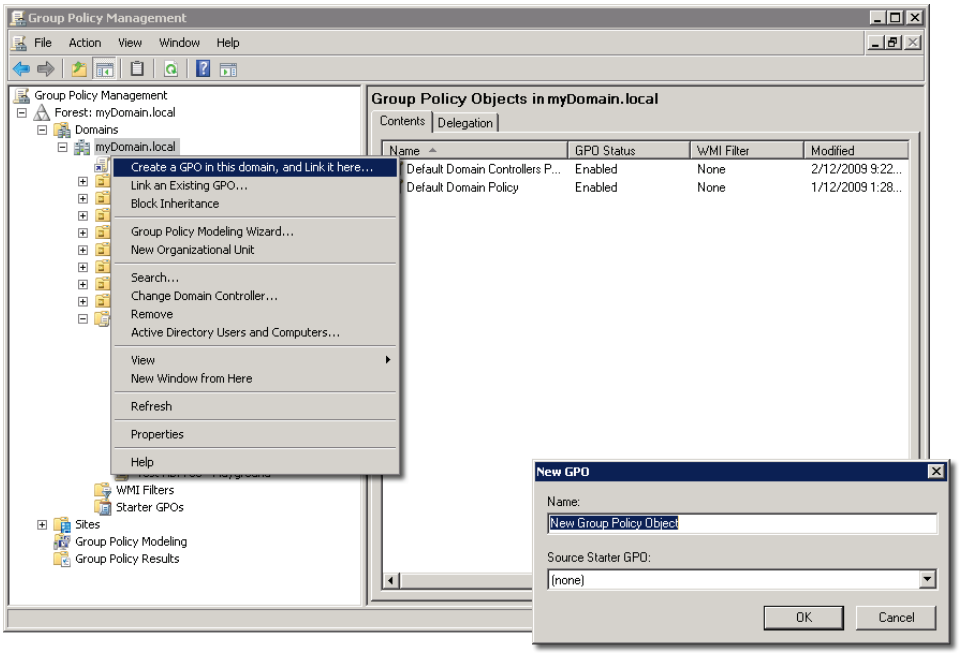

Figure 73: Configuring DIGIPASS CertiID via Group Policy (1) – Group Policy Management

4. Type a name for the new Group Policy object.
5. Select the Group Policy Object in the tree.
6. Select **Edit** from the context menu.

   The **Group Policy Object Editor** appears.

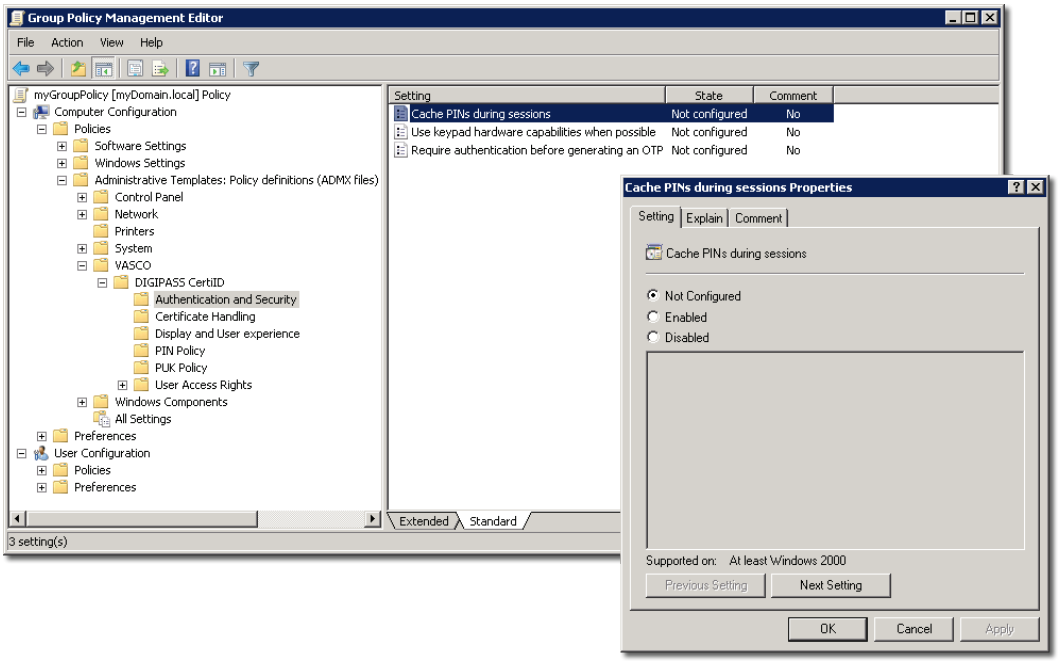

Figure 74: Configuring DIGIPASS CertiID via Group Policy (2) – Group Policy Object Editor (Server 2008)

7. Select **Computer Configuration > Policies > Administrative Templates > VASCO > DIGIPASS CertiID** in the Group Policy Object tree and use the right pane to configure the software settings.

   If the **VASCO > DIGIPASS CertiID** branch does not exist in the Group Policy Object tree, verify whether the Group Policy Administrative Templates files (VascoDPCertiID.admx and VascoDPCertiID.adml) are in the correct directory.

8. Close **Group Policy Object Editor**, when you have finished configuring the Group Policy Object.

➢ To configure DIGIPASS CertiID using Group Policy (Windows Server 2003)

1. Start **Active Directory Users and Computers** via **Start > Control Panel > Administrative Tools > Active Directory Users and Computers**.

2. Select the domain or organizational unit for which you want to set a group policy in the console tree.

3. Select **Properties** from the context menu.

4. Switch to the **Group Policy** tab.

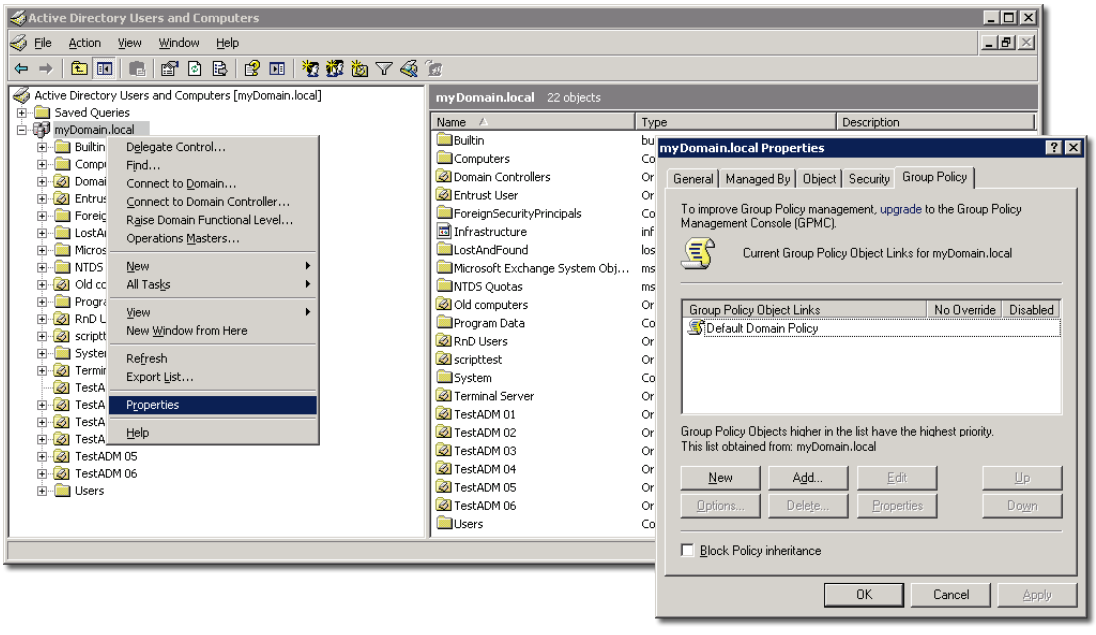

Figure 75: Configuring DIGIPASS CertiID via Group Policy (1) – Active Directory Users and Computers

5. Do one of the following:
   - If you want to create a new Group Policy object, click **New** and type a name for the new Group Policy object.
   - If you want to edit an existing Group Policy object, select the respective Group Policy object in the list.
6. Click **Edit**.

   The **Group Policy Object Editor** appears.

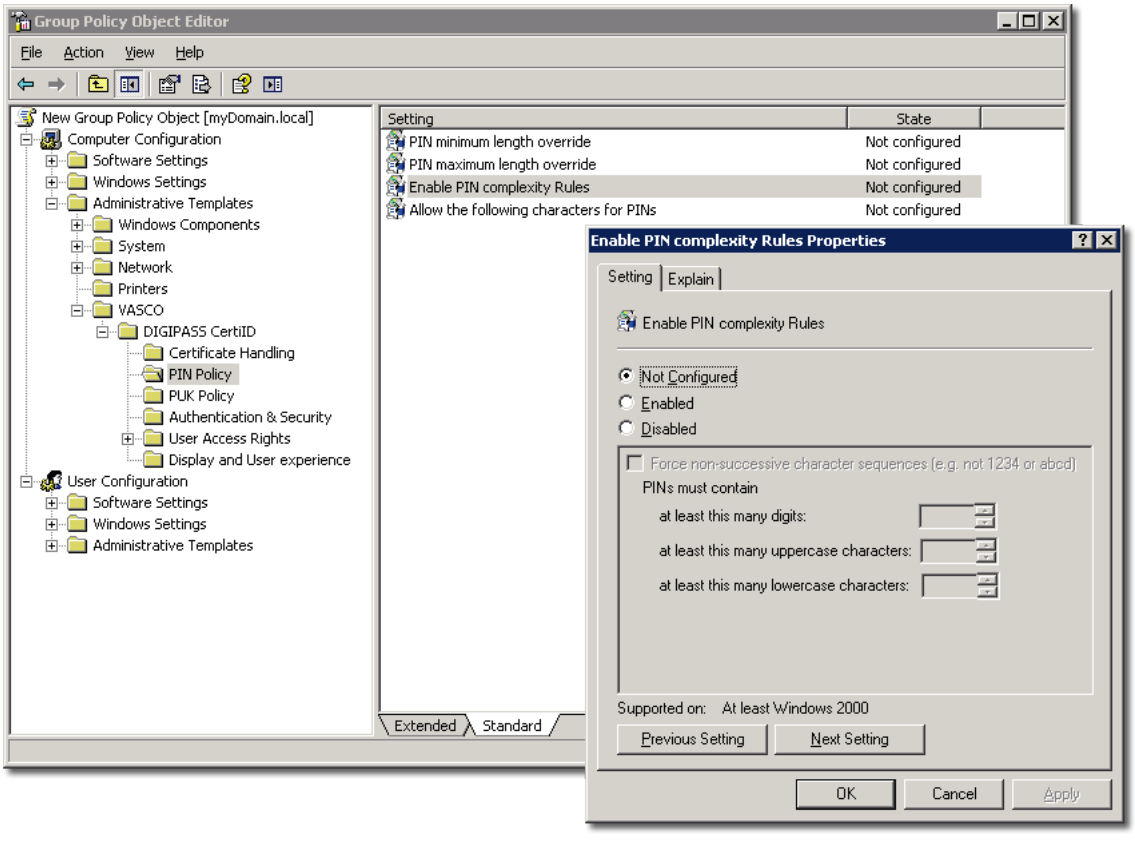

Figure 76: Configuring DIGIPASS CertiID via Group Policy (2) – Group Policy Object Editor (Server 2003)

7. Select **Computer Configuration > Administrative Templates > VASCO > DIGIPASS CertiID** in the Group Policy Object tree and use the right pane to configure the software settings.

   If the **VASCO > DIGIPASS CertiID** branch does not exist in the Group Policy Object tree, you can add it manually:

   (a) Select **Administrative Templates** in the Group Policy Object tree.

   (b) Select **Add/Remove Templates** from the shortcut menu.
   The **Add/Remove Templates Dialog** appears.

   (c) Select VascoDPCertiID in the list.
   If this item is not listed, click **Add** and browse for the respective Group Policy Administrative Template file (VascoDPCertiID.adm).

   (d) Click **Close** to return to the **Group Policy Object Editor**.

8. Close **Group Policy Object Editor**, when you have finished configuring the Group Policy Object.

9. Click **Close** to apply the new Group Policy.

7.1.3 Additional considerations

- If you want to use domain Group Policy, but don't want to install DIGIPASS CertiID on the domain controller, you can just copy the Administrative Templates to the respective directories. The plain Administrative Templates are on the DIGIPASS CertiID product CD in the Install\Group Policy folder.

  For Windows Server 2008 copy VascoDPCertiID.admx and en-US\VascoDPCertiID.adml to <WindowsFolder>\PolicyDefinitions, respectively, where <WindowsFolder> is the full path to your Windows folder, e.g. C:\Windows\.

  For Windows Server 2003 copy VascoDPCertiID.adm to <SystemFolder>\GroupPolicy\Adm, where <SystemFolder> is the full path to your system folder, e.g. C:\Windows\System32\.

- If you use DIGIPASS CertiID in an environment without a domain controller, you can use **Local Group Policy Editor** to configure DIGIPASS CertiID via Group Policy. To start Local Group Policy Editor, open a command prompt and type gpedit.msc.

7.2 Using DP CertiID Configuration Center to configure DIGIPASS CertiID

The **DP CertiID Configuration Center** is a configuration application allowing you to configure system wide options for all middleware components.

7.2.1 Before you begin

To start and use DP CertiID Configuration Center you need to be logged on with a user account with local administrator privileges.

7.2.2 Starting DP CertiID Configuration Center

➢ To start DP CertiID Configuration Center

- Select **Start > Programs > VASCO > DIGIPASS CertiID > Configuration Center**.

  -OR-

  Select **Tools > Configuration Center** in the **DP CertiID Management Application** menu bar.

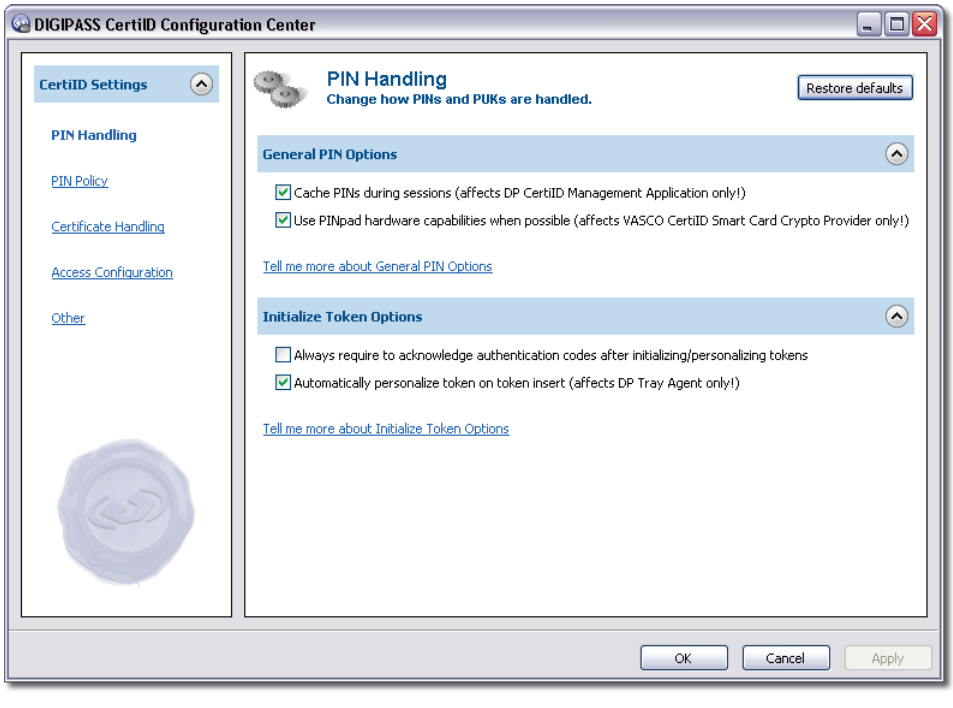

Figure 77: Configuration Center

7.3 PIN Handling

7.3.1 General PIN Options

Cache PINs during sessions
Select this option to enable PIN caching for **DP CertiID Management Application**. When you access a protected data object the first time, you are prompted for the PIN. If you enter the correct PIN, it is cached. If you subsequently access the same object again (or any other data object protected by the same PIN object), you will not be prompted for the PIN again. The PIN is kept until you remove the token or exit **DP CertiID Management Application**.

Use keypad hardware capabilities when possible
Select this option to allow **VASCO CertiID Smart Card Crypto Provider** to use keypad hardware whenever possible, unless specified otherwise by the calling client application. This option requires the particular tokens to be initialized with enabled keypad support and affects **VASCO CertiID Smart Card Crypto Provider** only.

NOTE
When authenticating to Microsoft Windows, this flag has no effect, because the underlying process, winlogon.exe, does always require the PIN to be typed using its own dialog.

7.3.2 Cryptographic Service Provider (CSP) PIN Caching Options

Cache PINs during cryptographic sessions
Select this option to enable PIN caching for **VASCO CertiID Smart Card Crypto Provider**. If enabled, the PIN is cached after a valid PIN authentication, when a third-party application opens a non-silent cryptographic context (session) to perform one or more cryptographic operations. Non-silent means that PIN authentication is handled by **VASCO CertiID Smart Card Crypto Provider** directly; silent means that the respective third-party application handles PIN authentication itself. The PIN cache is cleared when the application releases the cryptographic context, but not longer than a certain timeout (if enabled using **PIN cache timeout**). If **Cache PINs during cryptographic sessions** is disabled, PIN authentication is required for each operation. This option affects **VASCO CertiID Smart Card Crypto Provider** only.

NOTE
Whether a cryptographic operation is silent or non-silent or whether a new cryptographic context is created for each operation or not depends on the respective third-party application.

Clear PIN cache after a certain time
Select this option to clear the PIN cache after a certain time. The PIN is kept at least a certain time span (given by **PIN cache timeout**), unless the respective cryptographic context is released by the application earlier, in

which case the PIN is cleared immediately. This option is available only when you select the **Cache PINs during cryptographic sessions** check box.

PIN cache timeout
Type the time span how long a PIN is kept by **VASCO CertiID Smart Card Crypto Provider**, before it is cleared. If the application releases the respective cryptographic context, the PIN cache is cleared immediately, even if the timeout has not been elapsed. The value is given in seconds. This option is available only when you select the **Clear PIN cache after a certain time** check box.

7.3.3 Initialize Token Options

Always require to acknowledge authentication codes after initializing/personalizing tokens
Select this option to always display the **Confirm Authentication Dialog** when a token has been initialized. If you clear this check box, the **Confirm Authentication Dialog** appears only, if at least one of the effective authentication codes (that is, default PIN, default PUK, and/or default administrator key) is selected to be generated automatically, but no respective PIN/PUK/Administrator key letter is printed.

Automatically personalize token on token insert
Select this option to launch the **Personalize Token Wizard** automatically when a pre-initialized token is inserted. This option requires **DP CertiID Tray Agent**.

7.4 PIN Policy

7.4.1 PIN Policy Rules

Override token hardware capabilities
Select these options, if you want to explicitly set the minimum and maximum PIN length, respectively, and to have them emulated, if the used token hardware does not support the specified values. If you clear these check boxes, the minimum and/or maximum PIN lengths are determined by what the particular token hardware supports.

Minimum PIN length
Enter the number of characters a PIN must have at least to be valid. A value MAX (if you increase the value via the spin control) specifies that the minimum PIN length to be equal the maximum value allowed by the token hardware. This value can't be greater than the value specified by **Maximum PIN length**.

Maximum PIN length
Enter the number of characters a PIN can have at most to be valid. A value MAX (if you increase the value via the spin control) specifies that the maximum PIN length to be equal the maximum value allowed by the token hardware. This value can't be less than the value specified by **Minimum PIN length**.

Enable PIN complexity rules
Select this option to enable certain complexity rules to enforce strong PINs.

Force non-successive character sequences
Select this option to disallow PINs that contain only a successive character sequence. This option is available only when you select the **Enable PIN complexity rules** check box.

EXAMPLE:
The following PINs are successive character sequences, i.e. the distance between each character is equal for all characters.

1234

1357

abcd

The following PINs are non-successive character sequences, because the distance between each character is not equal for all characters.

3856

12341234

12qwertz

PINs must contain at least this many digits
Enter the number of digits a PIN must contain at least to be valid. This option is available only when you select the **Enable PIN complexity rules** check box.

PINs must contain at least this many uppercase characters
Enter the number of uppercase characters (e.g. ABC…) a PIN must contain at least to be valid. This option is available only when you select the **Enable PIN complexity rules** check box.

PINs must contain at least this many lowercase characters
Enter the number of lowercase characters (e.g. abc…) a PIN must contain at least to be valid. This option is available only when you select the **Enable PIN complexity rules** check box.

Allow the following characters for PINs
This option specifies which characters a PIN can contain to be valid.

- **Numeric characters only**
  Select this option to allow only numeric characters.
- **Alpha characters only**
  Select this option to allow only alphabetic characters.
- **Alphanumeric characters**
  Select this option to allow numeric and alphabetic characters.
- **Unicode characters**
  Select this option to allow any valid Unicode (UTF-8) character.

7.4.2 PUK Policy Rules

Override token hardware capabilities
Select these options, if you want to explicitly set the minimum and maximum PUK length, respectively, and to have them emulated, if the used token hardware does not support the specified values. If you clear these check boxes, the minimum and/or maximum PUK lengths are determined by what the particular token hardware supports.

Minimum PUK length
Enter the number of characters a PUK must have at least to be valid. A value MAX (if you increase the value via the spin control) specifies that the minimum PUK length to be equal the maximum value allowed by the token hardware. This value can't be greater than the value specified by **Maximum PUK length**.

Maximum PUK length
Enter the number of characters a PUK can have at most to be valid. A value MAX (if you increase the value via the spin control) specifies that the maximum PUK length to be equal the maximum value allowed by the token hardware. This value can't be less than the value specified by **Minimum PUK length**.

Enable PUK complexity rules
Select this option to enable certain complexity rules to enforce strong PUKs.

Force non-successive character sequences
Select this option to disallow PUKs that contain only a successive character sequence. This option is available only when you select the **Enable PUK complexity rules** check box.

EXAMPLE:
The following PUKs are successive character sequences, i.e. the distance between each character is equal for all characters.

1234

1357

abcd

The following PUKs are non-successive character sequences, because the distance between each character is not equal for all characters.

3856

12341234

12qwertz

PUKs must contain at least this many digits
Enter the number of digits a PUK must contain at least to be valid. This option is available only when you select the **Enable PUK complexity rules** check box.

PUKs must contain at least this many uppercase characters
Enter the number of uppercase characters (e.g. A B C…) a PUK must contain at least to be valid. This option is available only when you select the **Enable PUK complexity rules** check box.

PUKs must contain at least this many lowercase characters
Enter the number of lowercase characters (e.g. a b c…) a PUK must contain at least to be valid. This option is available only when you select the **Enable PUK complexity rules** check box.

Allow the following characters for PUKs
This option specifies which characters a PUK can contain to be valid.

- **Numeric characters only**
  Select this option to allow only numeric characters.
- **Alpha characters only**
  Select this option to allow only alphabetic characters.
- **Alphanumeric characters**
  Select this option to allow numeric and alphabetic characters.
- **Unicode characters**
  Select this option to allow any valid Unicode (UTF-8) character.

7.5 Certificate Handling

7.5.1 Automatic Registering of Certificates

Register certificates of the following categories
These options specify which certificate categories are automatically registered by **DP CertiID Tray Agent** when a token is inserted.

Personal
Select this option to have personal certificates (certificates for personal use with associated key pair) automatically registered by **DP CertiID Tray Agent** when a token is inserted. Certificates of this type are added to the **Personal Store**.

Certificate Authorities (CA)
Select this option to have certificates of certificate authorities (CA certificates with no associated key pair) automatically registered by **DP CertiID Tray Agent** when a token is inserted. Certificates of this type are added to the respective certification authority's store.

NOTE
If you install a CA certificate, you confirm that you explicitly trust this CA and any certificate issued by it. Due to the impact (and security risks) of this, Microsoft Windows may display a security warning, when **DP CertiID Tray Agent** tries to register a certificate for a CA. Microsoft Windows registers the CA certificate only, if you confirm that you trust the respective CA.

Other
Select this option to have certificates of other people (certificates for non-personal with no associated key pair) automatically registered by **DP CertiID Tray Agent** when a token is inserted. Certificates of this type are added to the **Other People Store**.

7.5.2 Automatic Unregistering of Certificates

Unregister certificates of the following categories
These options specify which certificate categories are automatically unregistered by **DP CertiID Tray Agent** when a token is removed.

Personal
Select this option to have personal certificates (certificates for personal use with associated key pair) automatically unregistered by **DP CertiID Tray Agent** when a token is removed. This option is available only when you select the **Personal** check box under **Register certificates of the following categories**.

Certificate Authorities (CA)
Select this option to have certificates of certificate authorities (CA certificates with no associated key pair) automatically unregistered by **DP CertiID Tray Agent** when a token is removed. This option is available only when you select the **Certificate Authorities (CA)** check box under **Register certificates of the following categories**.

NOTE
Due to the impact (and security risks) of removing a CA certificate, Microsoft Windows may display a security warning, when **DP CertiID Tray Agent** tries to unregister a certificate for a CA. Microsoft Windows unregisters the CA certificate only, if you confirm to delete it from the certificate store.

Other
Select this option to have certificates of other people (certificates for non-personal with no associated key pair) automatically unregistered by **DP CertiID Tray Agent** when a token is removed. This option is available only when you select the **Other** check box under **Register certificates of the following categories**.

7.5.3 Certificate Expiry Date Reminder

Remind me, if a certificate is about to expire
Select this option to get a warning each time you insert a token containing a certificate that is about to expire. This option affects **DP CertiID Management Application** and **DP CertiID Tray Agent** only; other applications will not display a warning.

Days before certificate expires
Enter the number of days a certificate should at least still be valid before an expiration warning is displayed. This option is available only when you select the **Remind me, if a certificate is about to expire** check box.

7.5.4 Certificate Import

Automatically write certificate chain to token when a certificate is imported
If you select this option, each time a certificate is imported via **VASCO CertiID Smart Card Crypto Provider** or **VASCO Card Module** (e.g. during a rollout) the middleware will attempt to retrieve the complete certificate chain for the certificate being imported (i.e. all intermediate CA certificates up to and including the root CA certificate) from the current user and local machine certificate stores. If all certificates of the chain can be retrieved, they will also be written to the token. This option affects **VASCO CertiID Smart Card Crypto Provider** and **VASCO Card Module** only; it is not effective, if you import certificate using **DP CertiID Management Application**.

TIP
This option is useful, when working with IdenTrust, since signing data using an IdenTrust identity certificate requires the whole certificate chain to be present on the machine.

7.6 Access Configuration

These options allow you to restrict access to particular program options for users with non-administrative privileges, respectively. If you are running on a user account with restricted privileges and some program options are not available to you, the system administrator may have disabled the program options in question.

7.6.1 Administrator Override

Automatically enable all program features for administrative users
Select this option to ignore the specified access configuration and automatically enable all program features, if the user has administrative privileges. This option affects **DP CertiID Management Application** only; other applications will adhere to the access configuration settings.

7.6.2 Token Management

Rename tokens
Select this option to allow users to change token labels.

Reset tokens
Select this option to allow users to reset tokens. If a token is protected by a reset code, it is still required to reset the token, whether this option is selected or not.

Initialize tokens
Select this option to allow users to initialize tokens.

7.6.3 Personalization

Personalize tokens
Select this option to allow users to personalize pre-initialized tokens.

Personalize administrator authenticators
Select this option to allow users to personalize the default PUK or default administrator key of pre-initialized tokens.

Reset token personalization
Select this option to allow users to reset the personalization data of initialized tokens and set them to the pre-initialized state.

7.6.4 Certificates and Containers

Import certificates
Select this option to allow users to import certificates from disk to a token.

Export certificates
Select this option to allow users to export certificates from a token to disk.

Test key pairs
Select this option to allow users to test key pairs for correct encryption/decryption and signing/verifying operations.

7.6.5 Object Management

Delete certificates
Select this option to allow users to delete certificates from a token.

Delete containers
Select this option to allow users to delete key containers from a token.

Delete data objects
Select this option to allow users to delete data objects from a token.

Delete secret key objects
Select this option to allow users to delete secret key (and master administrator key) objects from a token.

Import OTP key objects
Select this option to allow users to import OTP key objects to a token.

Delete OTP key objects
Select this option to allow users to delete OTP key objects from a token.

7.6.6 Security Settings

Unblock PINs
Select this option to allow users to unblock PINs.

Change administrator authenticators
Select this option to allow users to change the value of PUKs and administrator keys.

Replace PUKs with administrator key
Select this option to allow users to replace PUKs with an administrator key.

Generate master administrator keys
Select this option to allow users to generate master administrator keys.

Change object security
Select this option to allow users to change the protection of data objects. It effectively disables the **Change Object Security Wizard**.

Create new PINs
Select this option to allow users to create and assign new PINs to a data object. It effectively disables the **Generate new PIN** option in the **Change Object Security Wizard**. This option is available only when you select the **Change object security** check box.

Create new PUKs to unblock
Select this option to allow users to create and assign new PUKs to unblock newly created PINs. It effectively disables the **Generate new PUK** option in the **Change Object Security Wizard**. This option is available only when you select the **Create new PINs** check box.

Remove PIN protection
Select this option to allow users to remove the PIN protection from data objects. It effectively disables the **Remove current PIN** option in the **Change Object Security Wizard**. This option is available only when you select the **Change object security** check box.

Rename PINs
Select this option to allow users to change PIN labels.

Rename PUKs
Select this option to allow users to change PUK labels.

7.7 Other

7.7.1 Display and User Experience

Show support contact information in 'Unblock PIN Dialog'
Select this option to display support contact information in the **Unblock PIN Dialog**, so users may discover who to contact if their PIN is blocked.

Support contact information
Type the support contact information to display in the **Unblock PIN Dialog**. This option is available only when you select the **Show support contact information in 'Unblock PIN Dialog'** check box.

Show icon in notification area
Select this option to enable the icon in the notification area. If you clear this option, the icon is disabled for all users. However, if you select this option, the icon is initially shown, but can be hidden by the user, by selecting **Hide Tray Icon** in the **DP CertiID Tray Agent** shortcut menu. This option requires **DP CertiID Tray Agent**.

Show status changes
Select this option to display the hover pane automatically, if the token status changes, e.g. when a token is inserted or removed. If you clear this option, the status hover pane is disabled for all users. However, if you select this option, it can be overruled by the user, by clearing the **View Status Changes** option in the **DP CertiID Tray Agent** shortcut menu. This option requires **DP CertiID Tray Agent**.

7.7.2 One-Time Password Options

OTP display timeout
Type the time span how long a one-time password (OTP) is displayed in the OTP field of the **Generate OTP Dialog**, before it is displayed to be expired. The value is given in seconds.

Require authentication before generating an OTP
Select this option to always require authentication before generating an OTP using a hardware token. This option affects hardware tokens only; software OTP key objects always require authentication on access.

8 Troubleshooting and Diagnostics

This chapter gives an overview of how to diagnose and troubleshoot issues using **DP CertiID Troubleshooting and Diagnostics**.

It covers the following topics:

- Using Troubleshooting
- Using Diagnostics
- Using Application Error Reports

8.1 Using Troubleshooting

Troubleshooting helps you to find and identify issues. It verifies the current state of the system, looks for running services, connected card readers and inserted tokens, and performs a basic middleware self-check.

This tool serves as a first level support assistant and is used, if a program error or crash occurred, or if you think that CertiID middleware is not working correctly.

8.1.1 Searching for issues

➢ To search for issues using troubleshooting

1. Switch to the **Troubleshooting** tab.

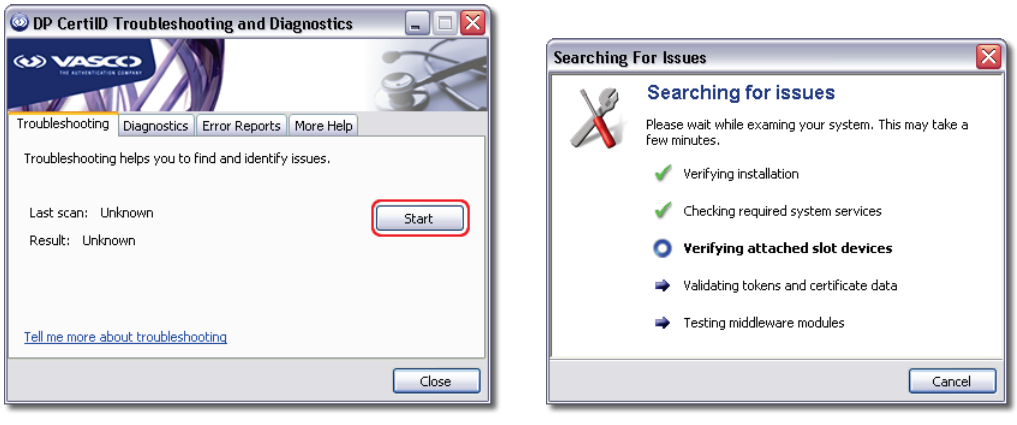

Figure 78: Troubleshooting

2. Click **Start**.

   The program examines your system. When finished the **Troubleshooting Report Dialog** appears.

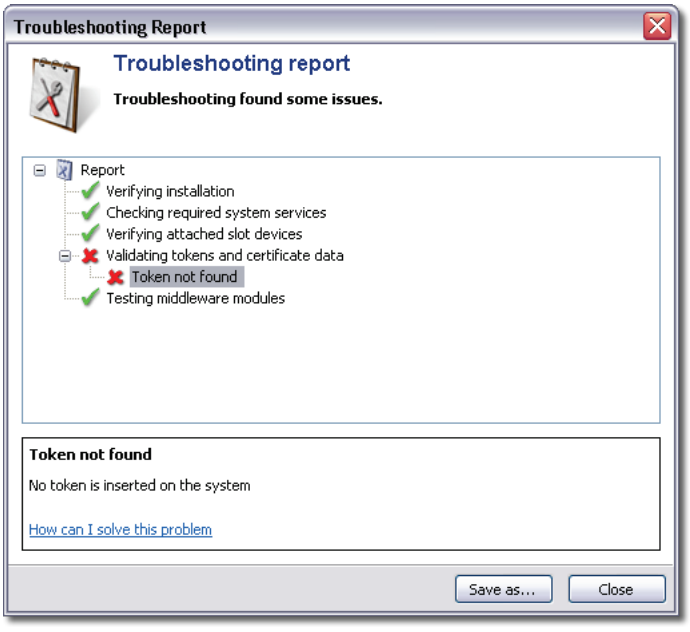

Figure 79: Troubleshooting Report

3. (OPTIONAL) Click **Save as** to save the troubleshooting report to disk.

   You can save the troubleshooting report for archiving purposes or to send it your support contact, if required.

4. Click **Close**.

   If you did not save the troubleshooting report, it is discarded.

8.1.2 Additional considerations

- Troubleshooting reports can be saved as a plain text file. If you do not save a report, it is discarded, when you close the **Troubleshooting Report Dialog**.
- If the troubleshooting report does not identify any issues and you still think, a problem exist, you may perform a diagnostics run.

8.1.3 Additional references

- Using Diagnostics

8.2 Using Diagnostics

Diagnostics is used, if you encounter problems such as application crashes and unexpected system behaviour, which you think may be caused by a CertiID middleware component, and a troubleshooting scan did not identify any issues.

Diagnostics tries to identify issues by recording all user actions and operations executed in the CertiID middleware.

There are two different types of diagnostics:

- System diagnostics

  System diagnostics records all actions and events of the system and all users in all sessions on a machine. It can only be activated and deactivated by a user with administrative privileges.

- User diagnostics

  User diagnostics records all actions and events by the user. It does not record system events, including system logon. It can be activated and deactivated by every user.

8.2.1 Performing a diagnostics run

➢ To enable system or user diagnostics

1. Switch to the **Diagnostics** tab.

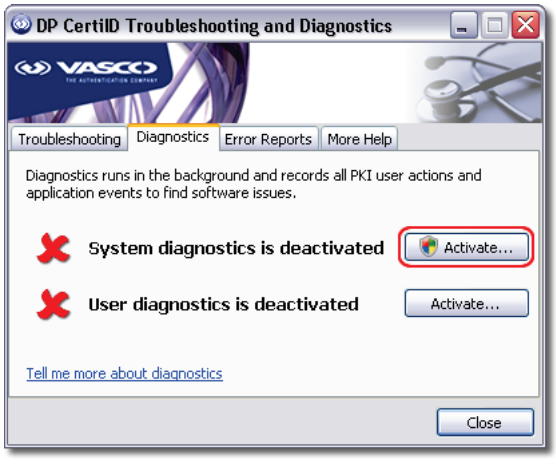

Figure 80: Diagnostics

2. Click **Activate** for the respective diagnostics type.

The **Set Diagnostics Options Dialog** appears.

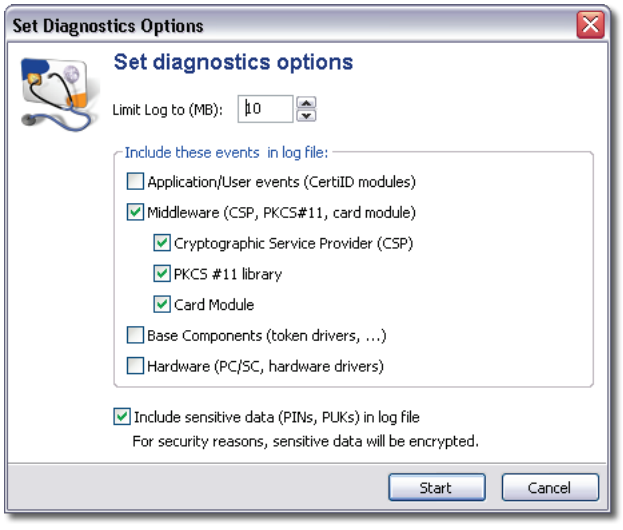

Figure 81: Setting Diagnostics Options

3. (OPTIONAL) Type a limit for the log file size and select which application layers should add log entries to the file.

   The log file will contain the latest records up to the specified file size. Once the specified file size is reached, logging continues and the oldest log entries will be overwritten.

   If you suspect a specific module to cause a problem, e.g. a specific hardware driver, you can include the respective application layer only and exclude everything else.

   If you select **Include sensitive data**, PINs and PUKs are included in the log file as this information may help analysing some issues.

NOTE
Sensitive data in diagnostics reports is always encrypted!

4. Click **Start** to activate diagnostics.

   Diagnostics is now activated and records the respective data until it is deactivated again.

➢ To disable system or user diagnostics in progress

1. Switch to the **Diagnostics** tab.
2. Click **Deactivate** for the respective diagnostics type.

   Diagnostics is now deactivated and the **Diagnostics Report Dialog** appears.

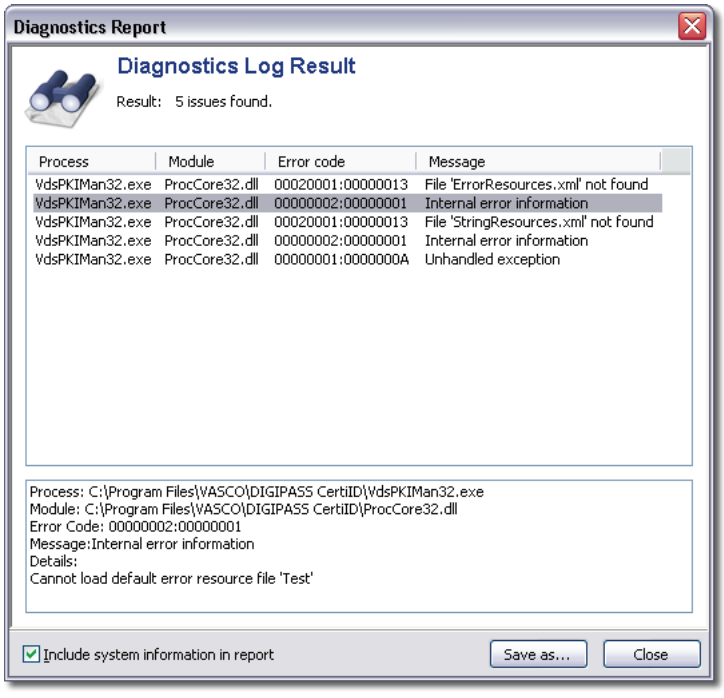

Figure 82: Diagnostics Log Result

3. (OPTIONAL) Click **Save as** to save the diagnostics report.

   You can save the diagnostics report for archiving purposes or to send it your support contact, if required.

   If you enable **Include system information in report**, Diagnostics collects information about system configuration that may help identifying issues.

4. Click **Close**.

   If you did not save the diagnostics report, it is discarded.

NOTE
The diagnostics report does contain a small portion of the contents of your machine's memory and some system information data necessary to examine potential issues. All collected data in diagnostics reports is encrypted.

VASCO will not track the diagnostics report back to you personally and treats this information confidential. Only individuals actively working on fixing problems have access to the information.

Diagnostics report data is used to find and fix problems in the software you use. It is not used for marketing purposes!

8.2.2 Additional considerations

- Diagnostics is deactivated by default and must be explicitly enabled. It remains activated until it is explicitly deactivated.
- Since diagnostics may considerably decrease system performance, you should enable it only when necessary.
- If no application layer is included, only error messages and warnings will be recorded.
- You can continue work, while diagnostics is activated.
- Diagnostics reports can be saved to disk. If you do not save a report, it is discarded, when you close the **Diagnostics Report Dialog**.

8.2.3 Additional references

- Using Troubleshooting

8.3 Using Application Error Reports

DIGIPASS CertiID provides a built-in error handler that automatically creates a memory dump when a middleware or application module terminates unexpectedly. You can check at any time whether application errors occurred and pending error reports are available via the **Error Report** tab.

8.3.1 Inspecting application error reports

➢ To inspect error reports

1. Switch to the **Error Report** tab.
2. If error reports are available, click **View**.

   The **Error Report List Dialog** appears.

You can decide what to do with them.

- Create error reports and save them to disk
- Discard error reports

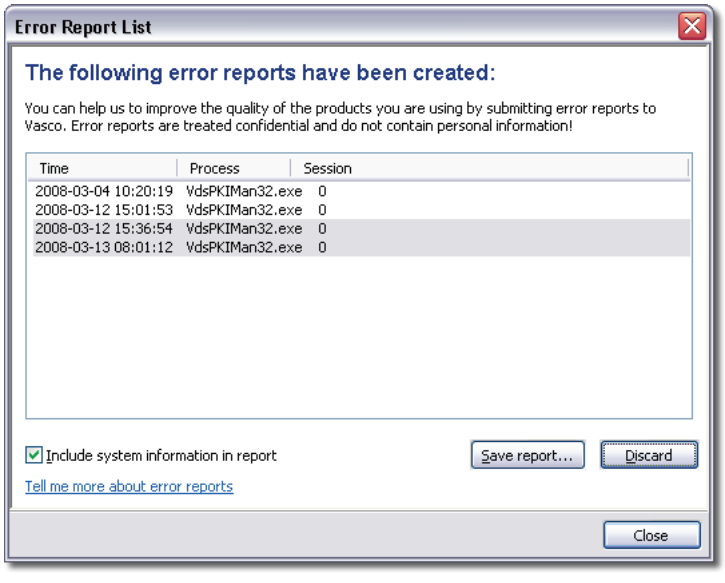

Figure 83: Error Report List

TIP
Error report data is usually handled using Windows Error Reporting (WER). In some cases when WER is not available and you need to contact your VASCO support contact, you may be required to explicitly save and submit an error report.

➢ To save an error report to disk

1. Select the respective error report in the **Error Report** list.
2. Click **Save report**.

   You can save the error report for archiving purposes or to send it to your support contact, if required.

   If you enable **Include system information in report**, Diagnostics collects information about system configuration that may help identifying issues.

NOTE
Error reports contain a small portion of the contents of your machine's memory and some system information data necessary to examine potential issues. Data in error reports is encrypted and does not contain sensitive data, such as PINs.

VASCO will not track error reports back to you personally and treats this information confidential. Only individuals actively working on fixing problems have access to the information.

Error report data is used to find and fix problems in the software you use. It is not used for marketing purposes!

➢ To discard an error report

1. Select the respective error report in the **Error Report** list.
2. Click **Discard**.

8.3.2 Additional considerations

- Error reports remain in the list until you explicitly discard them.

9 Appendix: Using DP CertiID with One-Time Passwords (OTP)

This chapter gives an overview of how to use DP CertiID to generate one-time passwords (OTP) using OTP-capable hardware tokens.

It covers the following topics:

- Generating One-Time Passwords (OTP)
- Generating One-Time Passwords (OTP) from Challenges
- Importing OTP Key Objects

9.1 Generating One-Time Passwords (OTP)

DP CertiID allows you to generate one time passwords (OTP) using OTP key objects. The OTPs, generated by the token, are displayed via the OTP software and can be copied to the clipboard for use in other software applications requiring OTP authentication.

9.1.1 Before you begin

To generate and view one-time passwords (OTP) you need:

- **DP CertiID Management Application** or **DP CertiID Tray Agent**
- a DP860 token

  -OR-

  a token containing an OTP key object valid to generate OTPs

9.1.2 Generating one-time passwords (OTP)

➢ To generate and view a one-time password (OTP)

1. Plug in your OTP token, e.g. DP860.
2. Select the respective OTP key object in the token explorer tree.

3. Select **Generate One-Time Password (OTP)** from the shortcut menu.

   -OR-

   Select **Tasks > Generate One-Time Password (OTP)** from the menu bar.

   The **Generate OTP Dialog** appears.

Figure 84: Generating One-Time Password (OTP)

4. If required, type the PIN and click **OK**.
5. Click **Generate** to generate a new OTP.

   The **OTP** box displays the current valid OTP. After a certain time span (default 30 seconds) the field changes to *Expired*.

6. (OPTIONAL) Click **Copy** to copy the current OTP to the clipboard.

TIP
You can select **Generate One-Time Password (OTP) to Clipboard** to generate and copy a one-time password directly to the clipboard without opening the **Generate OTP Dialog**.

9.1.3 Additional considerations

- Pressing the button on the DP860 token does not have any effect on the **Generate OTP Dialog**.
- You can set the OTP time span via **DP CertiID Configuration Center**.
- You can also use **DP CertiID Tray Agent** to generate and view OTPs.
- You can verify whether an OTP key object can be used to generate OTPs by inspecting its object properties in **DP CertiID Management Application**. If **Key Usage** includes Event-based OTP generation, the OTP key object can be used to generate OTPs.

9.1.4 Additional references

- Using the DP CertiID Tray Agent
- Configuring DIGIPASS CertiID
- Importing OTP Key Objects

9.2 Generating One-Time Passwords (OTP) from Challenges

VACMAN Controller-based servers (such as VACMAN Middleware and IDENTIKEY Server) can require clients to authenticate by dynamically calculating one-time passwords (OTP) based on a numerical challenge issued by the server.

You can use OTP key objects on your token to generate such OTPs from challenges.

9.2.1 Before you begin

To generate one-time passwords (OTP) from challenges you need:

- **DP CertiID Management Application** or **DP CertiID Tray Agent**
- a token containing an OTP key object valid to generate OTPs from challenges

9.2.2 Generating Responses using one-time passwords (OTPs)

➢ To generate a response using a one-time password (OTP)

1. Insert your OTP token.
2. Select the OTP key object in the explorer tree.
3. Select **Generate OTP from challenge** from the shortcut menu.

   -OR-

   Select **Tasks > Generate OTP from challenge** from the menu bar.

   The **Generate OTP from Challenge Dialog** appears.

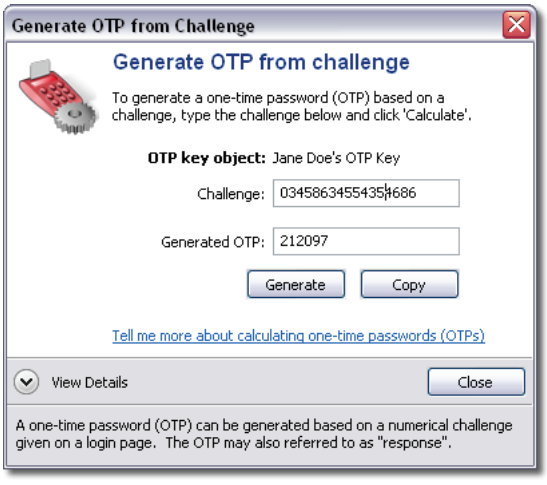

Figure 85: Generating One-Time Password (OTP) from Challenge

4. Type the challenge issued by your VACMAN Controller-based server in the **Challenge** box.
5. Click **Generate**.

   The **Response** box displays the calculated response.
6. If required, type your PIN.
7. (OPTIONAL) Click **Copy** to copy the response to the clipboard.

9.2.3 Additional considerations

- You can also use **DP CertiID Tray Agent** to generate OTPs from challenges.
- You can verify whether an OTP key object can be used to generate OTPs from challenges by inspecting its object properties in **DP CertiID Management Application**. If **Key Usage** includes Challenge/Response, the OTP key object can be used to generate OTPs from challenges.

9.2.4 Additional references

- Using the DP CertiID Tray Agent
- Configuring DIGIPASS CertiID
- Importing OTP Key Objects

9.3 Importing OTP Key Objects

The OTP key objects DP CertiID uses to generate one time passwords (OTP) or calculate OTP responses are abstract representations of any OTP generating mechanism provided by that token. This can be an OTP hardware token (e.g. DP860). You can also import OTP key object, i.e. creating a secret key object that can be used to calculate OTPs.

9.3.1 Before you begin

To import OTP key objects you need:

- **DP CertiID Management Application**
- depending on the OTP deployment mechanism either **activation data** and **activation password** or **serial number** and **activation code** information provided by your OTP service provider

9.3.2 Importing OTP key objects

➢ To import an OTP key object

1. Insert your token.
2. Select the **OTP Key Objects** folder in the token explorer tree.

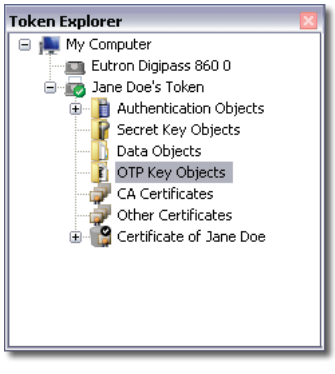

Figure 86: OTP Key Objects Folder

3. Select **Import OTP key object** from the shortcut menu.

   -OR-

   Select **Tasks > Import OTP key object** from the menu bar.

   The **Import OTP Key Object Dialog** appears.

Figure 87: Import OTP Dialog

4. Do one of the following:
   - If you are using offline activation
     (a) Select **Use online activation**.
     (b) Type the activation data and activation password information as provided by your OTP service provider.
   - If you are using online activation
     (a) Select **Use offline activation**.
     (b) Type the serial number and activation code information as provided by your OTP service provider.
5. Type a label for the OTP key object in the **OTP object label** box.
6. Type the name of your OTP service provider in the **Service identifier** box.

7. Click **Import**.

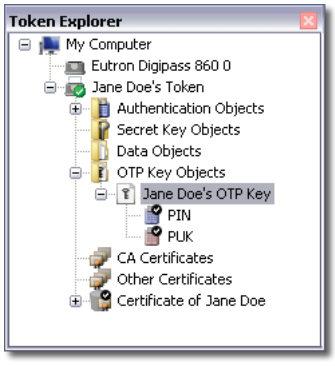

Figure 88: Inspecting Imported OTP Object

9.3.3 Additional considerations

- The system or token administrator may restrict access to certain program features. If a particular option is not available, you may not have the privileges to use it.
- The imported OTP key object is protected by the default PIN, if one is available on the token. You can change this via **DP CertiID Management Application**.
- The **OTP Key Objects** folder in the token explorer tree contains all OTP key objects on a token, i.e. abstract representations of any OTP generating mechanism provided by that token, e.g. OTP hardware or imported OTP key object.

9.3.4 Additional references

- Generating One-Time Passwords (OTP)
- Generating One-Time Passwords (OTP) from Challenges
- Changing the Security of Objects
- Configuring DIGIPASS CertiID

10 Appendix: PKI and Certificate Basics

This chapter gives an overview of how to manage digital certificates and key pairs on a token using **DP CertiID Management Application**.

It covers the following topics:

- Understanding PKI and Certificates
- Certificate Details
- Certificate Category
- Certificate File Formats

10.1 Understanding PKI and Certificates

Public Key Infrastructure (PKI) can be defined as the software and/or hardware components necessary to manage and enable the effective use of public key encryption technology. It binds public keys to respective user identities by means of certification authorities (CA).

Public key encryption technology in principle is asymmetric cryptographic using pairs of cryptographic keys. A key pair consists of a public key and a private key. The **private key** is kept secret and used to decrypt data that has been encrypted with the corresponding public key or to sign data. The **public key** is widely distributed and used to verify data that has been signed with the corresponding private key or to encrypt data.

A **digital certificate** is the digital equivalent of an ID card. It specifies the name of an individual, company, or other entity and certifies that the public key included in the certificate, belongs to that entity.

Digital certificates are issued by **certification authorities** that attest the public key contained in a certificate really belongs to the person or organization noted in the certificate. Certification authorities are usually hierarchically grouped, i.e. a root CA on top issuing certificates to other CAs below that hierarchy to confirm and certify the identities of these CAs and so on (chain of trust).

Certificates are usually valid only for a certain period of time, specified within the certificate itself.

10.2 Certificate Details

Certificate details include different fields, extensions, and properties.

- **Version**
  This is the X.509 version of the certificate.
- **Serial number**
  This is the unique serial number of the certificate.
- **Issuer**
  This is the certification authority that issued the certificate.
- **Valid from**
  This field gives the date from which on the certificate can be used.
- **Valid to**
  This field gives the date until which the certificate can be used.
- **Subject**
  This is the name of the person, machine, device, or certification authority to whom the certificate has been issued.
- **Public key**
  This field gives information about the type and key length of the associated public key.
- **Thumbprint algorithm**
  This is the algorithm used to calculate the **Thumbprint**.
- **Thumbprint**
  This is the thumbprint (digest) of the certificate data.
- **Friendly name**
  The common name for the name given in the **Subject** field.
- **Enhanced key usage**
  This field specifies the purposes for which the certificate may be used.

10.3 Certificate Category

The **certificate category** is determined by certain certificate attributes and purposes. It determines how the certificate is stored on the token and how applications will access it.

DIGIPASS CertiID distinguishes three different certificate categories:

- Personal
  Certificates of this category contain an associated private key on your token and hence, can be used for signing and encrypting. Such certificates are usually issued to you. They are displayed separately in a certificate container with a certificate and a key pair.
- Other People
  Certificates of other people are not meant for personal use (by you) and do not contain an associated private key. Such certificates are usually issued to people and end entities implicitly trusted in applications. They are displayed together with all non-personal certificates.
- Certification Authority (CA)
  Such certificates are also not meant for personal use (by you) and do not contain an associated private key. Such certificates are usually trusted root certificates from certification authorities.

> NOTE
> Note that the certificate storage on the token does not necessarily correspond one-to-one with the local certificate stores on the machine.

10.3.1 Additional references

- Registering and Unregistering Certificates
- Using the DP CertiID Tray Agent

10.4 Certificate File Formats

Certificates can be stored using various file formats, each based on different security and compatibility concerns. DIGIPASS CertiID supports the following certificate file formats:

- Personal Information Exchange (PKCS #12)
- Cryptographic Message Syntax Standard (PKCS #7)
- DER Encoded Binary (X.509)
- Base-64 Encoded Binary (X.509)

10.4.1 Personal Information Exchange (PKCS #12)

The **Personal inFormation eXchange (PFX)** or PKCS #12 format is used to exchange public and private objects in a single file, e.g. a certificate and its corresponding private key.

Such certificate files usually have a .PFX or .P12 file suffix.

Since private keys cannot be retrieved from a token, CertiID supports only import of PFX files.

> NOTE
> If you try to import a PFX file containing more than one certificate, only the first certificate will be imported.

10.4.2 Cryptographic Message Syntax Standard (PKCS #7)

The **Cryptographic Message Syntax Standard** or PKCS #7 format is used to transfer certificates and all certificates in its certification path.

Such certificate files usually have a .P7B file suffix.

CertiID supports import of and export to P7B files.

10.4.3 DER Encoded Binary (X.509)

The **Distinguished Encoding Rules (DER) Encoded Binary** format encodes data objects, such as X.509 certificates.

Such certificate files usually have a .CER file suffix.

CertiID supports export to CER files.

10.4.4 Base-64 Encoded Binary (X.509)

The **Base-64 Encoded Binary** format was developed for content transfer encoding for **Multipurpose Internet Mail Extensions (MIME)**, i.e. a popular standard method to transfer binary attachments over the internet.

Such certificate files usually have a .CER file suffix.

CertiID supports export to CER files.

10.4.5 Additional resources

- Importing Certificates
- Exporting Certificates

11 Appendix: Card Operating System Limitations

This chapter gives an overview of the limitations of the different card operating systems (COS) supported by DIGIPASS CertiID.

11.1 Overview

Feature	CardOS 4.3b	CardOS 4.01A	STARCOS 3.1	ID-One 1.0
Key pairs				
RSA key size (bits)	512 – 2048[1]	512 – 1024	768 – 2048	1024 – 2048
RSA maximum import key size (bits)	512 – 2048[2]	512 – 1024	768 – 2048	1024 – 2048
DSA key size (bits)	1024	n/a	n/a	n/a
Administrator key				
Key type	DES3	DES3	DES2	DES3
Key size (byte)	24	24	16	24
Key form	T1 T2 T3	T1 T2 T3	T1 T2 T1	T1 T2 T3
PIN				
Minimum length	4	4	6	4
Maximum length	15	15	8	15
PUK				
Minimum length	4	4	6	4
Maximum length	15	15	8	15
Reset protection				
No protection	Y	Y	Y	N
Reset code	Y	Y	Y	N
No reset	Y	Y	Y	Y
Miscellaneous				
Returns retry counter	N	N	Y	Y
Uses extended APDU[3]	Y	N	N	N

Table 3: Card Operating Systems Limitations (Overview)

[1] Cannot execute cryptographic functions with RSA keys > 2032 on DP 905 v0.0.0
[2] Cannot execute cryptographic functions with RSA keys > 2032 on DP 905 v0.0.0
[3] Extended APDUs may cause problems on various smart card readers when using RSA keys > 2032

12 Appendix: Using DIGIPASS CertiID with Keypad Hardware

This chapter gives an overview of how to use DIGIPASS CertiID with keypad hardware, including pitfalls and limitations.

12.1 Overview

Smart card reader hardware with keypad function, such as the DP855, introduces additional security, since the PIN is typed and verified directly on the device excluding any possibility for PIN eavesdropping. DIGIPASS CertiID supports keypad hardware for authentication. Instead of the **Enter PIN Dialog** requiring you to type the PIN on the computer keyboard, you are required to follow the instructions and type the PIN on the keypad hardware.

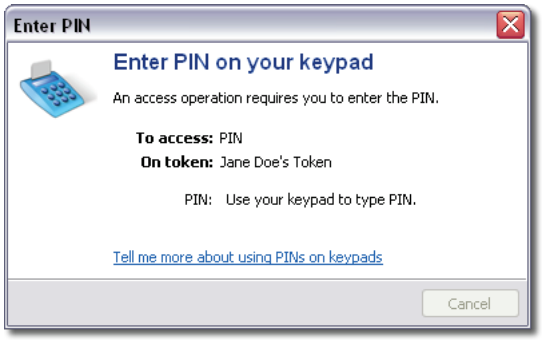

Figure 89: Entering PIN on keypad hardware

NOTE
Since the PIN is typed directly on the keypad device, no PIN caching is applied. In some cases you may be required to type the PIN more than once, e.g. when enrolling a certificate from a certification authority (CA).

12.1.1 Differences using Keypad Hardware with Middleware Modules

The keypad hardware support behaves differently depending on which middleware module the application uses for cryptographic operations.

12.1.1.1 VASCO CertiID Smart Card Crypto Provider

Applications that use CSP for cryptographic operations have two options to request authentication.

- The application displays its own authentication interface. Depending on whether the application is aware of the connected keypad hardware, it requires the user to type the PIN either on the keyboard or on the keypad. For instance, when authenticating to Microsoft Windows, you are required to type the PIN using the keyboard at the Windows Logon Screen, because the underlying process, winlogon.exe, is not aware of keypad hardware.
- The application depends on the middleware to authenticate the user. In this case you can determine the behaviour using the **Use keypad hardware capabilities when possible** option set via **DP CertiID**

Configuration Center. If this option is selected, keypad hardware is used whenever possible. If this option is not selected, the PIN is required to be typed on the keyboard. This option requires the particular tokens to be initialized with enabled keypad support.

12.1.1.2 DP CertiID PKCS#11 Library

Applications that use PKCS #11 for cryptographic operations always use their own authentication interface. Depending on whether the application is aware of the connected keypad hardware, it requires the user to type the PIN either on the keyboard or on the keypad.

12.1.1.3 VASCO Card Module

VASCO Card Module does currently not provide keypad hardware support.

12.2 Limitations

DIGIPASS CertiID keypad hardware support has currently the following limitations:

- Only user authentication is supported, i.e. enter PIN.
- PIN and PUK management is not supported, e.g. change or unblock.
- Only VASCO CertiID Smart Card Crypto Provider and DP CertiID PKCS#11 Library support keypad hardware.
- You cannot manage tokens on keypad hardware, i.e. initialize or reset tokens.

13 Appendix: Customizing PIN/PUK Letters

When you initialize a token, you can decide whether to print information regarding the authentication codes, i.e. PIN, PUK and/or administrator key. This information can be handed over to the user along with the token (PIN letter).

This chapter gives an overview of how to customize PIN and PUK letter templates used to print authentication code information when initializing tokens.

13.1 Customizing PIN/PUK Letter Templates

PIN letters are based on XHTML templates, located in the 1033\Templates folder in the DIGIPASS CertiID program folder.

The following templates are available:

- AdminKeyLetter.xhtml
  This template is used when printing an administrator key letter.
- PINLetter.xhtml
  This template is used when printing a PIN letter containing the PIN only.
- PINLetterWithAdminKey.xhtml
  This template is used when printing a PIN letter containing PIN and administrator key.
- PINLetterWithPUK.xhtml
  This template is used when printing a PIN letter containing PIN and PUK.
- PUKLetter.xhtml
  This template is used when printing a PUK letter.

The templates use HTML for text layout and placeholder (enclosed in curly braces { }) to insert specific information in the printed letter at runtime.

- TOKENSERIAL
  This placeholder is replaced with the token serial number. It is evaluated in all templates.
- CARDHOLDER
  This placeholder is replaced with the cardholder name of the token. It is evaluated in all templates.
- PIN
  This placeholder is replaced with the PIN value. It is evaluated in all templates containing PIN information.
- PUK
  This placeholder is replaced with the PUK value. It is evaluated in all templates containing PUK information.
- ADMINISTRATORKEY
  This placeholder is replaced with the administrator key value. It is evaluated in all templates containing administrator key information.

13.1.1 Example

```
[...]

<blockquote>
   <strong>Token Serial Number</strong>: {TOKENSERIAL}<br />
   <strong>Assigned Cardholder</strong>: {CARDHOLDER}<br />
   <strong>PIN</strong>: {PIN}<br />
</blockquote>
```

Index

P

R

S