



# DAS Customer Administration Guide

November 2007  
V1.03

## Executive summary

This document aims at providing information about DAS usage. You will learn how to get your machine ready for DAS, how to initialize and configure you DAS Controller, and how to manage your .NET devices.

## Table of contents

Executive summary .....	2
Table of contents .....	3
Table of figures .....	3
Introduction .....	5
Pre-requisites .....	5
Get your machine DAS ready .....	6
Overview of DAS portal.....	8
DAS Controller initialization.....	11
<b>DAS Administration Portal .....</b>	<b>15</b>
.NET Devices pre-personalization .....	15
Change DAS Controller PIN .....	16
Remote Unblock .....	17
Local Unblock .....	19
Reset Devices .....	20
Reset DAS Controller .....	21
<b>User portal .....</b>	<b>22</b>
Change PIN .....	22
Unblock PIN .....	23
Device information .....	23
Manage certificate .....	24
<b>Support and troubleshooting.....</b>	<b>29</b>
Frequently asked questions.....	29

## Table of figures

<i>Figure 1 - SConnect Install (part 1).....</i>	<i>6</i>
<i>Figure 2 - SConnect Install (part 2).....</i>	<i>7</i>
<i>Figure 3 - SConnect Install (part 3).....</i>	<i>7</i>
<i>Figure 4 – Connection encrypted .....</i>	<i>8</i>
<i>Figure 5 - DAS Security.....</i>	<i>9</i>
<i>Figure 6 – Contact information .....</i>	<i>10</i>
<i>Figure 7 - DAS Administration portal.....</i>	<i>11</i>
<i>Figure 8 - DAS Controller Setup Login .....</i>	<i>11</i>
<i>Figure 9 – Admin key rotation scheme selection.....</i>	<i>12</i>
<i>Figure 10 - Prepare DAS Controller.....</i>	<i>13</i>
<i>Figure 11 – DAS Controller personalized .....</i>	<i>13</i>
<i>Figure 12 - DAS Controller PIN .....</i>	<i>14</i>
<i>Figure 13 - Devices pre-personalization.....</i>	<i>15</i>

<b>Figure 14 – Change DAS Controller PIN</b> .....	16
<b>Figure 15 –DAS Controller PIN changed</b> .....	16
<b>Figure 16 - User Portal Remote Unblock PIN</b> .....	17
<b>Figure 17 – Admin Portal Remote Unblock PIN</b> .....	17
<b>Figure 18 - User Portal Unblock PIN</b> .....	18
<b>Figure 19 - Unblock PIN confirmation message</b> .....	18
<b>Figure 20 - Local Unblock</b> .....	19
<b>Figure 21 - Unblock PIN confirmation message</b> .....	19
<b>Figure 22 - Reset Devices</b> .....	20
<b>Figure 23 - Reset DAS Controller</b> .....	21
<b>Figure 24 - Reset DAS Controller confirmed</b> .....	21
<b>Figure 25 - Change PIN user portal</b> .....	22
<b>Figure 26 - Change PIN confirmation message</b> .....	22
<b>Figure 27 – Device information</b> .....	23
<b>Figure 28 – Certificate management</b> .....	24
<b>Figure 29 – Certificate viewer</b> .....	24
<b>Figure 30 – Certificate management</b> .....	25
<b>Figure 31 – Import P12 select</b> .....	26
<b>Figure 32 – Import P12 password</b> .....	26
<b>Figure 33 – Import P12 analyzing</b> .....	27
<b>Figure 34 – Import P12 PIN</b> .....	27
<b>Figure 35 – Import P12 completed</b> .....	27

## Introduction

DAS is a web hosted service that requires a minimal software installation on your machine. This document will describe step by step:

- ✚ How to install the software components to get your machine DAS ready
- ✚ How to configure your DAS Controller allowing you to get access to the DAS admin portal.
- ✚ How to use the DAS admin portal
- ✚ How to use the DAS user portal

## Pre-requisites

The following operating systems and web browsers are required in order to get access to DAS:

- ✚ Microsoft Windows 2000, XP or Vista
- ✚ Microsoft Internet Explorer v6 or higher

or

- ✚ Mozilla Firefox v2.x

As an Administrator you need to have two smart card readers (if you have .NET devices in smart card form factor) connected to your machine. If you have received a Gemalto smart card reader and if it hasn't been installed yet on your machine please go to the following web site to get the appropriate driver:

<http://support.gemalto.com/gemdownload/readers/index.aspx>

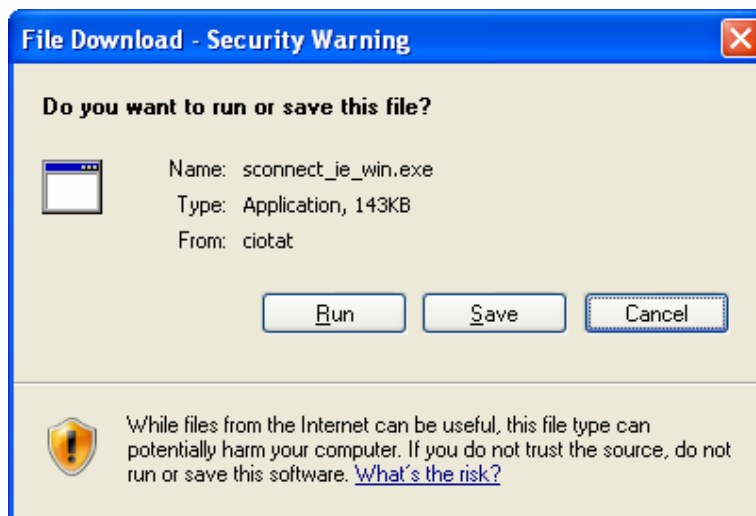
If it's not a Gemalto smart card reader please be sure that the product is certified by the Microsoft WHQL. You can have a list of certified product from the Microsoft WinQual web site at <http://winqual.microsoft.com/hcl/default.aspx> (select *Input Devices* and then *Smartcard Readers* to get the list of certified smart card readers).

## Get your machine DAS ready

The DAS Portal requires the use of **SConnect**, a browser extension developed by Gemalto that enables enhanced management of .NET devices through Web Services. SConnect is available for all the most common browsers (Internet Explorer, Firefox) and supported on Windows 2000, XP and Vista Operating Systems.

You need to have local administrator rights to install SConnect.

1. Go to the **DAS Admin Portal** (URL provided in the email you have received from the Gemalto partner).
2. If your browser is not yet SConnect enabled, you will see the following message, inviting you to install the SConnect extension.
  - a. Click on the **Run** button to install SConnect.  
NOTE: Instructions for SConnect setup on Internet Explorer. Setup is similar on other browsers



*Figure 1 - SConnect Install (part 1)*

- b. Review the S-Connect license agreement and click on the **I Agree** button. SConnect will install.

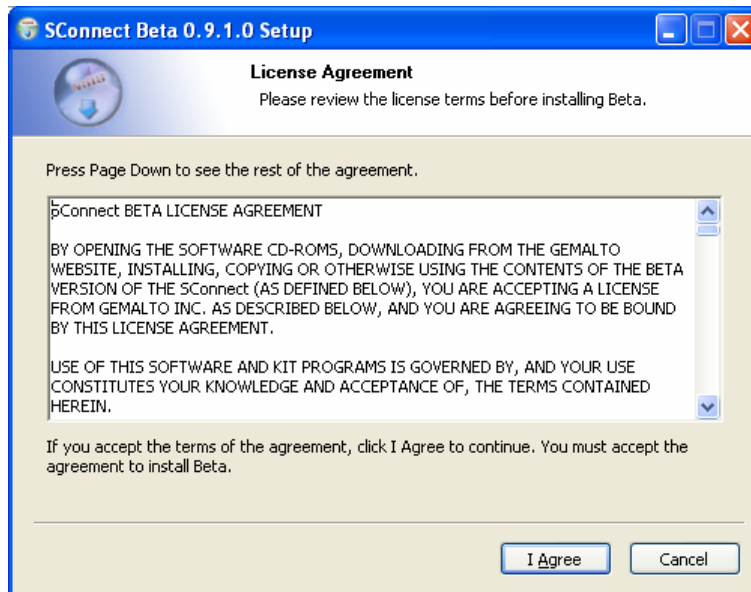


Figure 2 - SConnect Install (part 2)

- c. Once the installation is completed click the **Close** button. Despite the message, you will not need to restart Internet Explorer (this is not SConnect inherent but rather to the browser behavior).

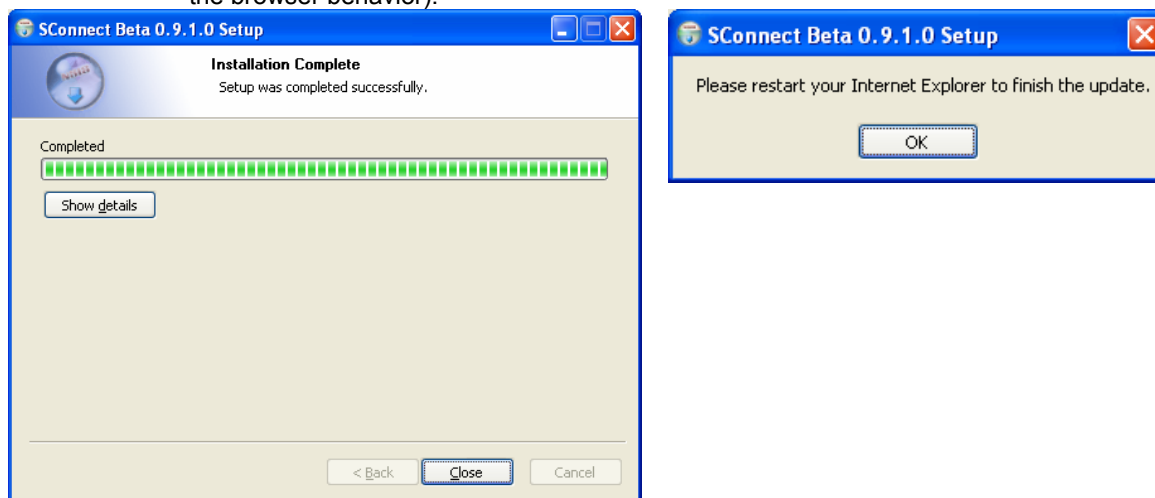


Figure 3 - SConnect Install (part 3)

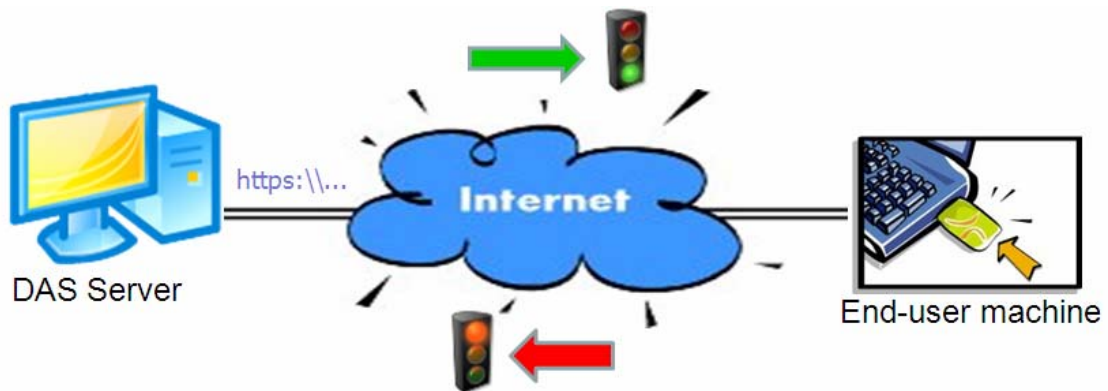
## Overview of DAS portal

Device Administration services portals, Administration and user, can only be accessed using a web browser. The web site you'll access is secured by SSL (high grade encryption RC4 128 bits).



*Figure 4 – Connection encrypted*

All the sensitive operations such as DAS Controller Configuration, Change/Unblock PIN and Import P12 file are performed locally thanks to the ASP.NET technology.



*Figure 5 - DAS Security*

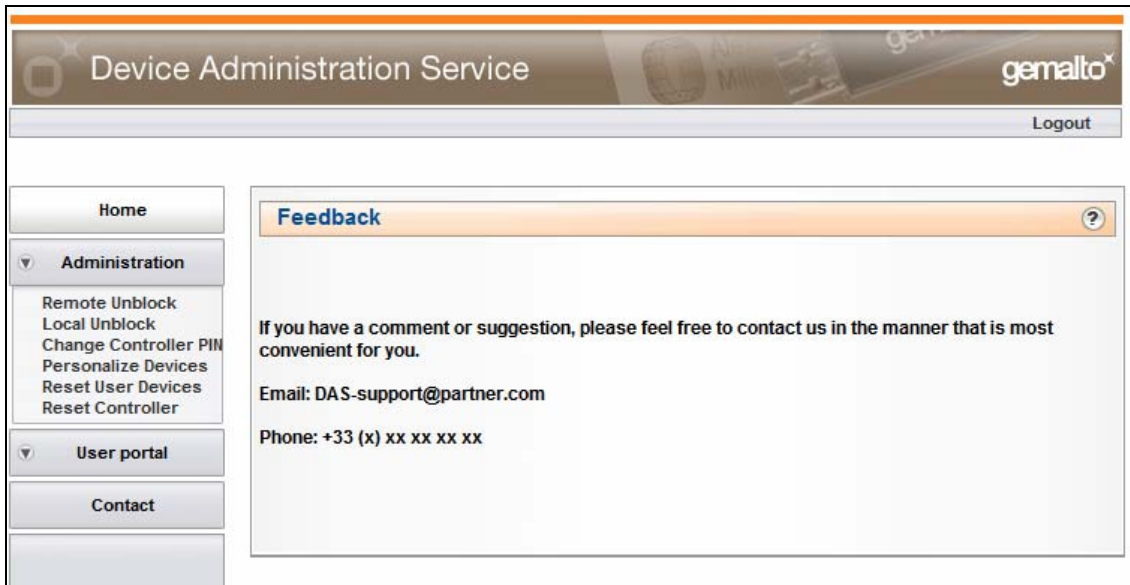
- ✚ No database for the DAS
- ✚ SSL connection → secure (server authentication and line encryption)
- ✚ No upload of customer information → DAS Server is not processing customer information at any stage
- ✚ Only download of script to be executed on end-user machine




**Important:** all the sensitive operations such as DAS Controller Configuration, Change/Unblock PIN and Import P12 file are performed locally thanks to the ASP.NET technology.

Both web portals have the same design. On the left side of the web page you have access to the different menus and actions.

- Home: a click on this button will bring you back to the main page
- Administration: a click on this button will list the operations accessible for the administrator (only accessible with a DAS Controller initialized)
- User portal: a click on this button will list the operations accessible for an end-user with a user device properly configured by the administrator (see Device configuration section).
- Contact: a click on this button will display support information (specific for each Gemalto partner)



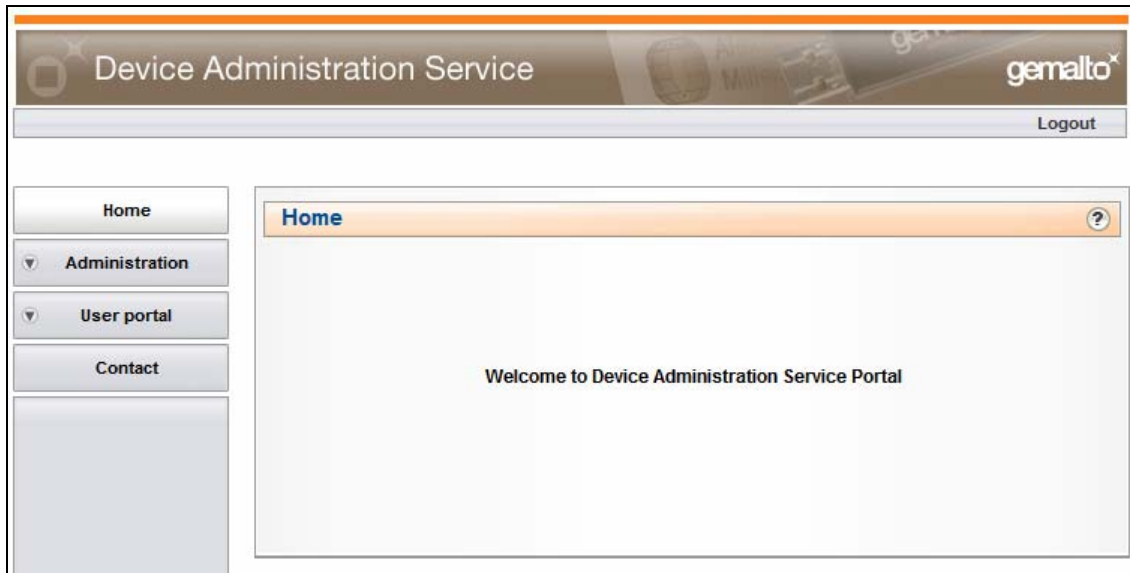
*Figure 6 – Contact information*

Should you need information about the operation you intend to perform click on the  button located on the right of the operation banner.

## DAS Controller initialization

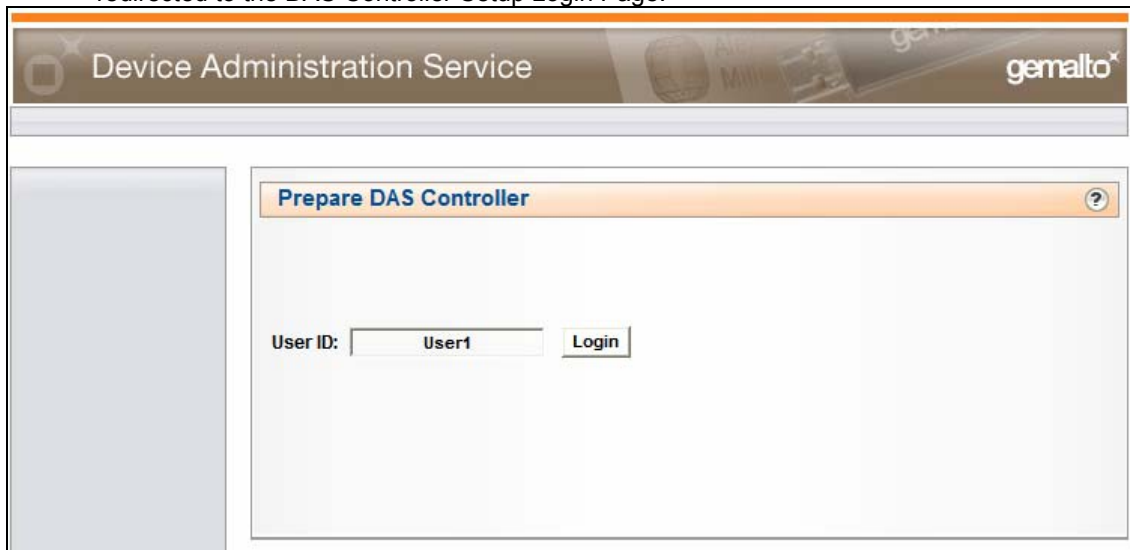
As an administrator you need now to prepare the DAS Controller devices that will allow you to securely manage your .NET devices. This section describes the different operations you have to perform in order to get your DAS Controller initialized.

1. Go to the DAS Admin Portal (URL provided in the email you have received from the Gemalto partner).



*Figure 7 - DAS Administration portal*

2. Insert now one of the DAS Controller devices. The device will be recognized and you will be redirected to the DAS Controller Setup Login Page.

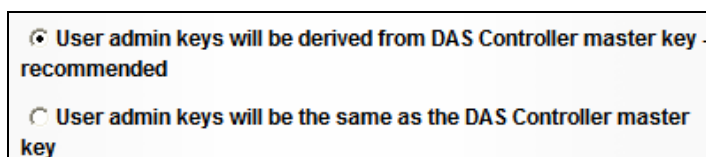


*Figure 8 - DAS Controller Setup Login*

Present the User ID (case sensitive) corresponding to the inserted device, then click on the **Login** Button

3. Once authenticated, you will reach the DAS Controller configuration page. Here you are prompted to enter:

- ✚ The Master Key of your DAS Controller (48 hexadecimal (0-9, A-F) digits). Enter and confirm (the master key value must be different from the factory value: 000000...)
- ✚ The PIN of your DAS Controller (4 to 8 ASCII characters)
- ✚ The maximum number of PIN presentation attempts before the DAS Controller is locked
- ✚ **End-users .NET devices Admin Keys rotation scheme** → the way the admin key will be set in the .NET device: it could be either the same value or a value derived from the Master key and the serial number of the .NET device making more complex to find the admin key value.



The screenshot shows a configuration window with two radio button options. The first option, "User admin keys will be derived from DAS Controller master key - recommended", is selected. The second option, "User admin keys will be the same as the DAS Controller master key", is unselected.

*Figure 9 – Admin key rotation scheme selection*

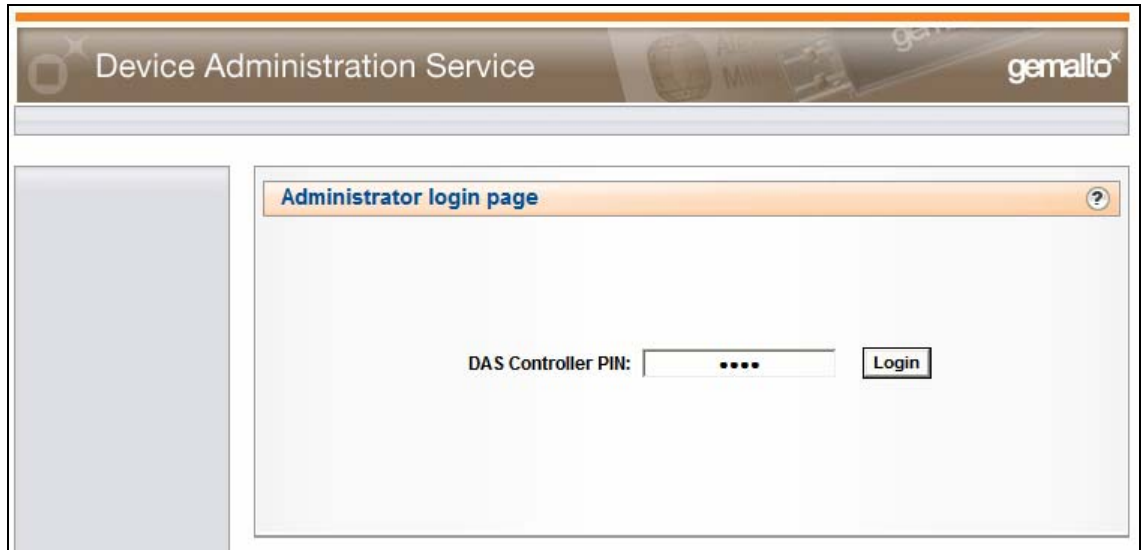


**Important:** we recommend using the same configuration (Master Key value and admin key format) for all the DAS Controller. It is also strongly recommended to save in a secure area this configuration in the case you need to create more DAS Controller or your current DAS controllers get compromised (lost, stolen or damaged).

Enter all values then click on the **Set DAS Controller** button. At this point, the DAS Controller assembly will download from the DAS Server to your device and it will be configured with your Master Key and PIN



5. Then you will be automatically logged into the DAS Admin Portal. DAS Controller PIN will be required.



*Figure 12 - DAS Controller PIN*

6. Repeat Steps 1 to 4 to setup your other DAS Controller. Keep it as a backup.



Congratulations! At this point you are ready to use the DAS Admin Portal to manage your End User Devices. From now on when you visit the DAS Admin Portal at [www.netsolutions.gemalto.com/dasdemo/admin](http://www.netsolutions.gemalto.com/dasdemo/admin) you will just have to connect your DAS controller and present its PIN, as shown above.

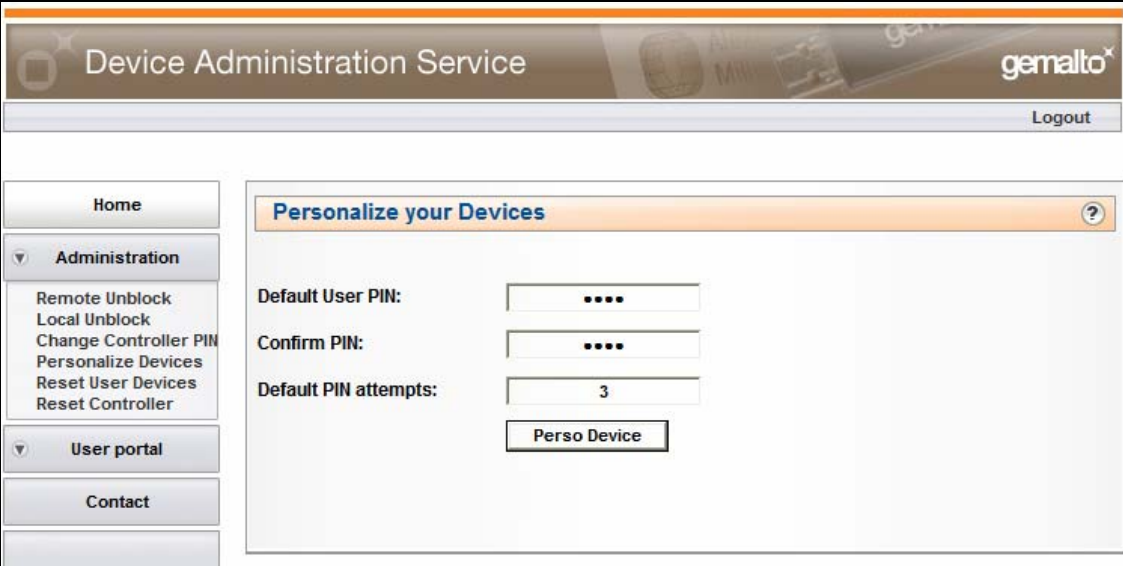
## DAS Administration Portal

The following section describes the different operations that an Administrator of DAS could have to operate. **The first and mandatory operation consists in pre-personalizing the .NET devices that will be managed by DAS.**

## .NET Devices pre-personalization

All the .NET devices that you'll obtain from a Gemalto partner are delivered with default values for the user PIN and the admin key. DAS allows you to change these values thus making your .NET devices unique and not useable by someone else.

1. From the **Administration** menu select **Personalize devices**. Insert/plug the first .NET device to your machine. Set the default user PIN and confirm it, then set the default PIN attempts (number of incorrect user PIN presented before the device will be blocked). Then click on the **Perso Device** button.



The screenshot shows the DAS Administration Portal interface. At the top, there is a header with 'Device Administration Service' and the 'gemalto' logo. A 'Logout' button is visible in the top right. On the left side, there is a navigation menu with 'Home', 'Administration', 'User portal', and 'Contact'. The 'Administration' menu is expanded, showing options like 'Remote Unblock', 'Local Unblock', 'Change Controller PIN', 'Personalize Devices', 'Reset User Devices', and 'Reset Controller'. The main content area is titled 'Personalize your Devices' and contains three input fields: 'Default User PIN:' with a masked input (four dots), 'Confirm PIN:' with a masked input (four dots), and 'Default PIN attempts:' with the value '3'. Below these fields is a 'Perso Device' button.

*Figure 13 - Devices pre-personalization*

2. Remove the device and repeat the same operation for all the .NET devices you want to pre-personalize.

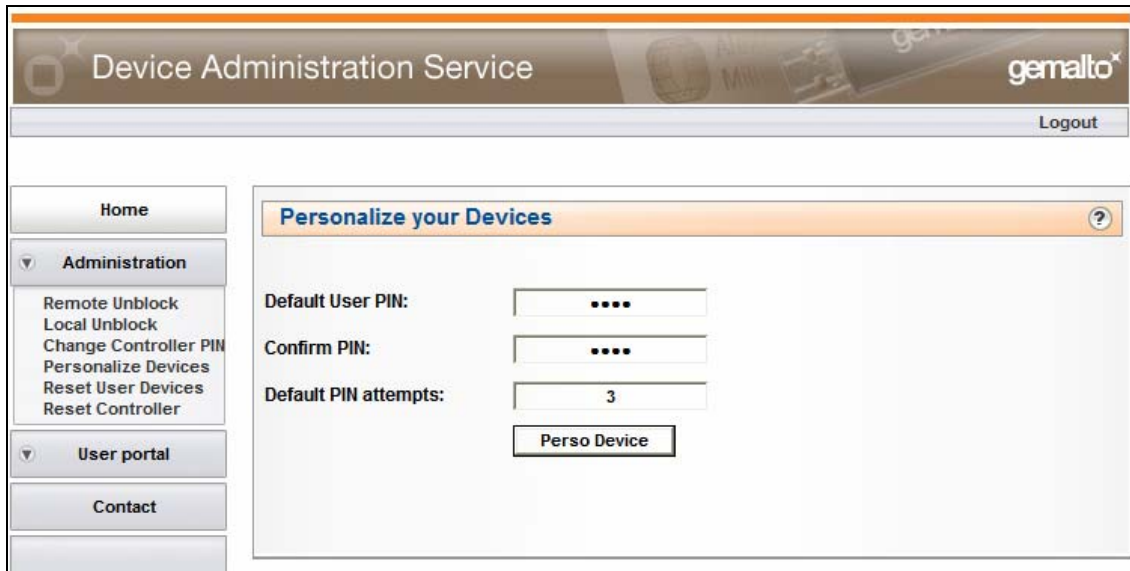


Your devices are now ready to be distributed to your customers/employees.

# Change DAS Controller PIN

You might decide to change the PIN of the DAS Controller if it has been compromised.

1. From the **Administration** menu select **Change DAS Controller PIN**. Enter the old PIN then the new PIN (up to 20 characters) and confirm it. Then click on the **Change PIN** button.



*Figure 14 – Change DAS Controller PIN*

2. A message will confirm that the PIN of the DAS Controller has been changed

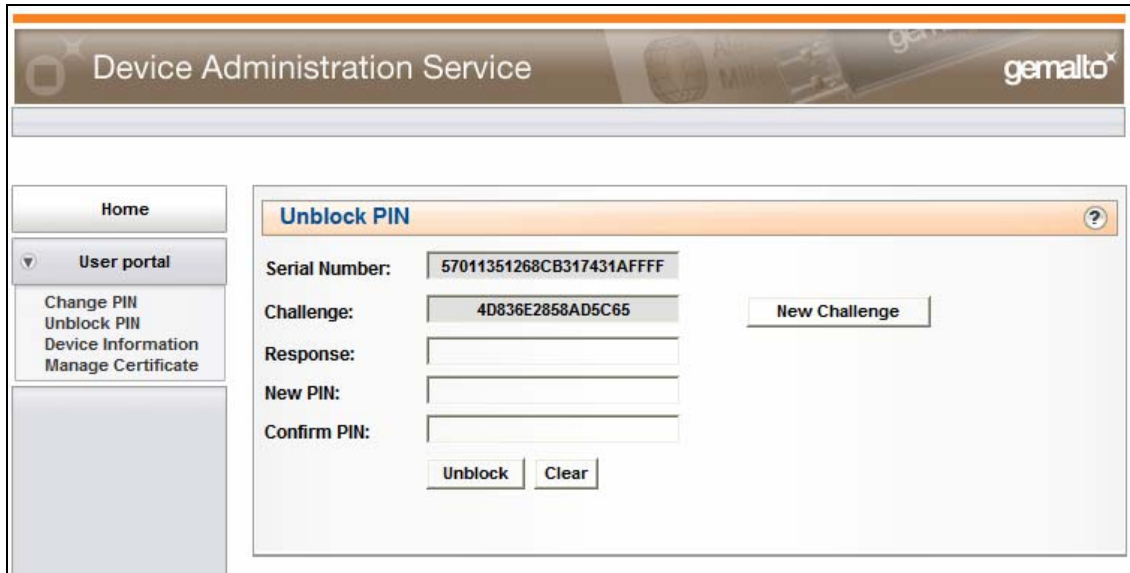


*Figure 15 –DAS Controller PIN changed*

## Remote Unblock

This function allows an administrator altogether with the concerned end-user to remotely unblock a .NET device of an end-user.

1. From the [User portal](#) menu the end-user must have his/her .NET device inserted and must select **Unblock PIN**. The end-user then provides you the responses obtained.

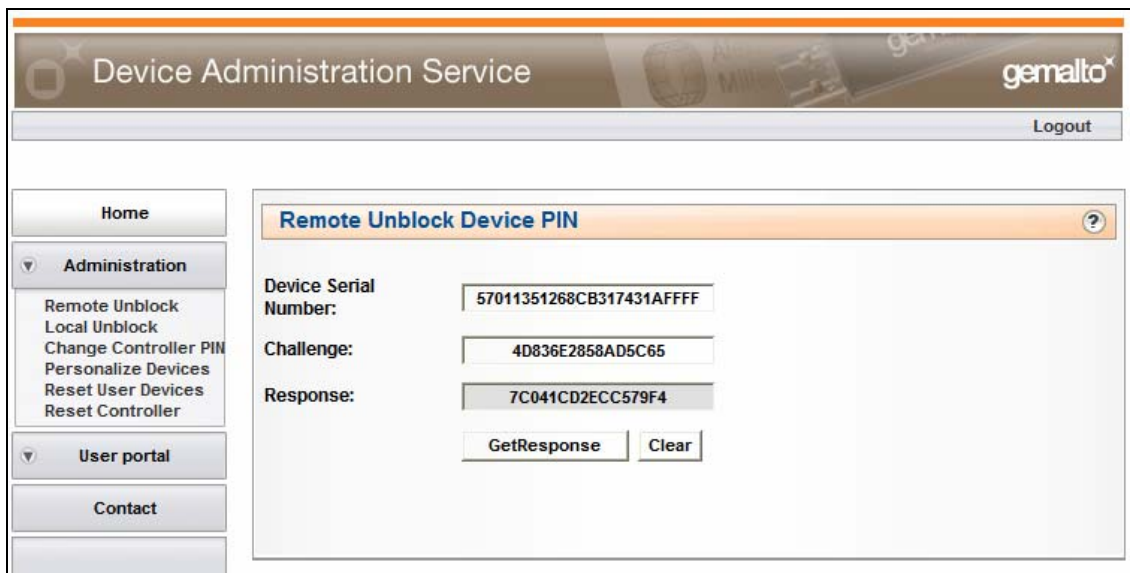


The screenshot shows the 'Device Administration Service' interface with the 'User portal' menu expanded. The 'Unblock PIN' form is displayed, featuring the following fields and controls:

- Serial Number:** 57011351268CB317431AFFFF
- Challenge:** 4D836E2858AD5C65
- Response:** (empty text input)
- New PIN:** (empty text input)
- Confirm PIN:** (empty text input)
- Buttons:** 'New Challenge', 'Unblock', and 'Clear'.

Figure 16 - User Portal Remote Unblock PIN

2. From the [Administration](#) menu select **Remote Unblock**. Enter the **Serial Number** and **Challenge** provided by the end-user. Click on the **Get Response** button



The screenshot shows the 'Device Administration Service' interface with the 'Administration' menu expanded. The 'Remote Unblock Device PIN' form is displayed, featuring the following fields and controls:

- Device Serial Number:** 57011351268CB317431AFFFF
- Challenge:** 4D836E2858AD5C65
- Response:** 7C041CD2ECC579F4
- Buttons:** 'GetResponse' and 'Clear'.

Figure 17 – Admin Portal Remote Unblock PIN

3. Provide the **Response** to the end-user. The end-user will have to enter this value to the appropriate field and then will enter a new PIN and will confirm it before clicking on the **Unblock** button.

The screenshot shows the 'Unblock PIN' interface within the Gemalto Device Administration Service. The page has a header with the service name and the Gemalto logo. A left-hand navigation menu includes 'Home' and 'User portal' with sub-options: 'Change PIN', 'Unblock PIN', 'Device Information', and 'Manage Certificate'. The main content area is titled 'Unblock PIN' and contains the following fields and buttons:

- Serial Number:** 57011351268CB317431AFFFF
- Challenge:** 4D836E2858AD5C65 (with a 'New Challenge' button to its right)
- Response:** 7C041CD2ECC579F4
- New PIN:** [masked with four dots]
- Confirm PIN:** [masked with four dots]
- Buttons: 'Unblock' and 'Clear'

*Figure 18 - User Portal Unblock PIN*

4. The following message will then be displayed to confirm the PIN change.

Your PIN has been successfully unblocked and changed.

*Figure 19 - Unblock PIN confirmation message*

## Local Unblock

This function allows an administrator altogether with the concerned end-user to locally unblock a .NET device of an end-user. In such situation the end-user must bring his/her .NET device to the administrator. The administrator must have the possibility to connect his/her DAS Controller and the end-user .NET device

1. From the **Administration** menu select **Local Unblock**. Connect the end-user .NET device. The **Serial Number** and the **Challenge** will be automatically retrieved. The end-user will enter a new PIN and will confirm it before clicking on the **Unblock** button.



The screenshot shows the 'Device Administration Service' web interface. The header includes the service name and the Gemalto logo. A 'Logout' link is in the top right. A left sidebar contains navigation options: Home, Administration (with a dropdown menu listing Remote Unblock, Local Unblock, Change Controller PIN, Personalize Devices, Reset User Devices, and Reset Controller), User portal, and Contact. The main content area is titled 'Local Unblock device PIN' and contains the following fields and controls:

Device Serial Number:	57011351268CB317431AFFFF
Challenge:	EAA9F8E6A1C26909
Response:	DC89500934816542
New PIN:	.....
Confirm PIN:	.....

Below the fields is an 'Unblock' button.

*Figure 20 - Local Unblock*

2. The following message will then be displayed to confirm the PIN change.

Your PIN has been successfully unblocked and changed.

*Figure 21 - Unblock PIN confirmation message*

## Reset Devices

This function allows an administrator to set a .NET Device to its original state (default Admin key and user PIN values) for future re-use of the device.

1. From the **Administration** menu select **Reset User Devices**. Insert/connect the .NET device to your machine. You are prompted to confirm the operation. Click on the **Yes** button to confirm the operation.



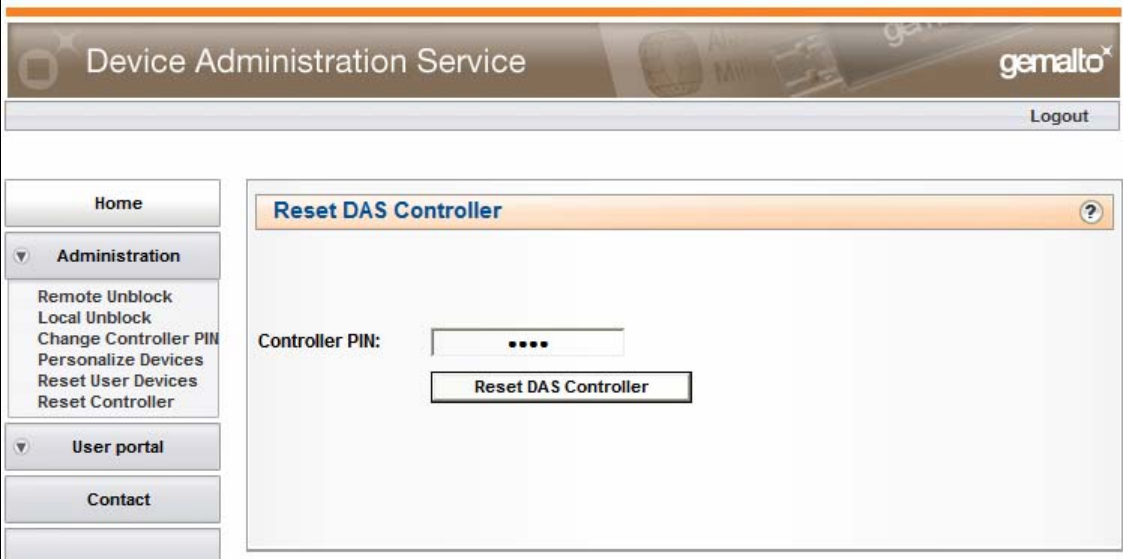
*Figure 22 - Reset Devices*

2. Remove/disconnect the device and insert the next one to reset.

## Reset DAS Controller

This function allows an administrator to set a DAS Controller to its original state (default Admin key and user PIN values) for future re-use of the device. This operation should normally only be performed during testing phases.

1. From the **Administration** menu select **Reset DAS Controller**. Enter your PIN and click on the **Reset DAS Controller** to confirm the operation.



The screenshot shows the 'Device Administration Service' web interface. The header includes the title 'Device Administration Service' and the 'gemalto' logo. A 'Logout' link is visible in the top right. A left-hand navigation menu contains 'Home', 'Administration' (with a dropdown arrow), 'User portal', and 'Contact'. Under 'Administration', the following options are listed: 'Remote Unblock', 'Local Unblock', 'Change Controller PIN', 'Personalize Devices', 'Reset User Devices', and 'Reset Controller'. The main content area is titled 'Reset DAS Controller' and contains a form with the label 'Controller PIN:', a text input field with four dots, and a 'Reset DAS Controller' button.

*Figure 23 - Reset DAS Controller*

2. The following message will then be displayed to confirm that your DAS Controller is no longer personalized. You need to use your User ID information to personalize it again.

**Your DAS Controller has been resetted.**

*Figure 24 - Reset DAS Controller confirmed*

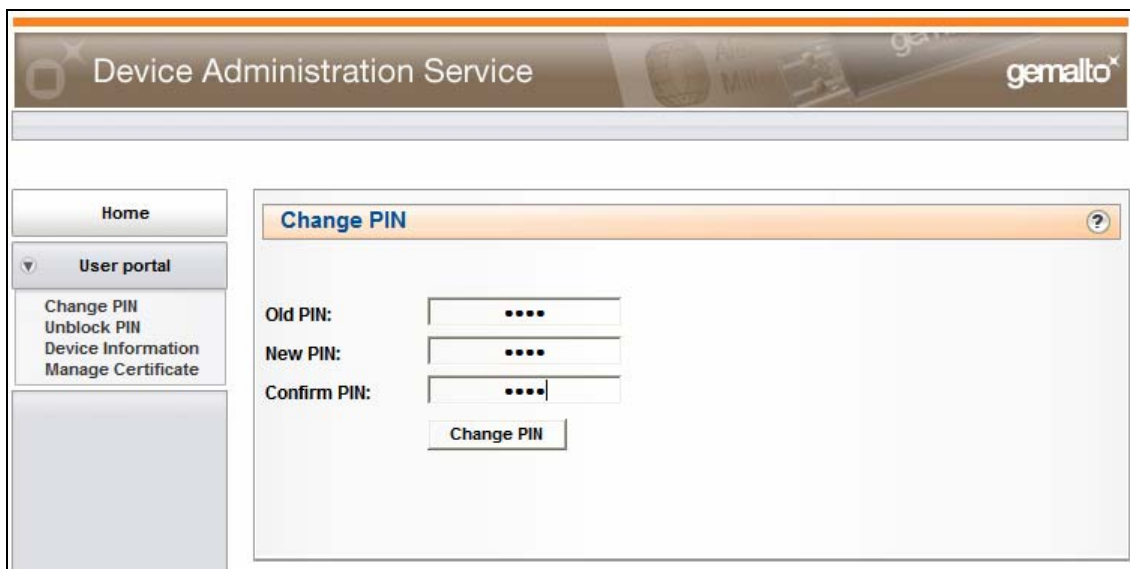
## User portal

The following section describes the different operations that an end-user could have to operate. It is advised that the user changes his/her .NET device PIN prior to use it (all the .NET devices have been pre-configured with the same PIN).

## Change PIN

This function allows an end-user to change his/her .NET device PIN.

1. From the [User portal](#) menu select **Change PIN**. Enter your **Old PIN** (current PIN), the **New PIN** and **confirm** it. Then click on the **Change PIN** button.



The screenshot shows the 'Device Administration Service' user portal. The header includes the service name and the Gemalto logo. A left-hand navigation menu contains 'Home' and 'User portal' (expanded to show 'Change PIN', 'Unblock PIN', 'Device Information', and 'Manage Certificate'). The main content area is titled 'Change PIN' and features three input fields for 'Old PIN', 'New PIN', and 'Confirm PIN', each containing four dots. A 'Change PIN' button is positioned below the fields.

*Figure 25 - Change PIN user portal*

2. The following message will then be displayed to confirm the PIN change.

Your PIN has been successfully unblocked and changed.

*Figure 26 - Change PIN confirmation message*

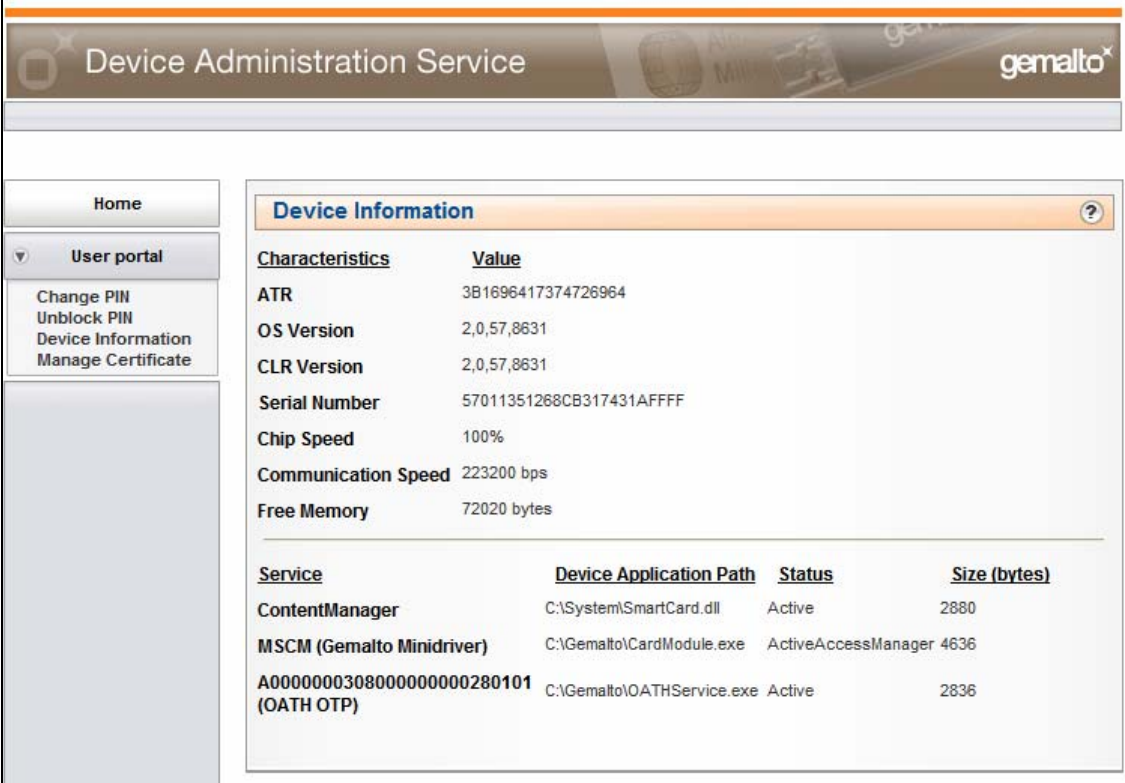
## Unblock PIN

See the [Remote Unblock](#) section in the Administration chapter.

## Device information

This function allows an end-user to view detailed information about his/her .NET device.

1. From the [User portal](#) menu select **Device information**. All the technical characteristics of your .NET device and the services running on it are displayed.



The screenshot displays the 'Device Administration Service' web interface. The main content area is titled 'Device Information' and contains two tables. The first table lists technical characteristics and their values. The second table lists services running on the device, including their application paths, status, and size.

Characteristics	Value
ATR	3B1696417374726964
OS Version	2,0,57,8631
CLR Version	2,0,57,8631
Serial Number	57011351268CB317431AFFFF
Chip Speed	100%
Communication Speed	223200 bps
Free Memory	72020 bytes

Service	Device Application Path	Status	Size (bytes)
ContentManager	C:\System\SmartCard.dll	Active	2880
MSCM (Gemalto Minidriver)	C:\Gemalto\CardModule.exe	Active	AccessManager 4636
A000000030800000000280101 (OATH OTP)	C:\Gemalto\OATHService.exe	Active	2836

Figure 27 – Device information

# Manage certificate

This function allows an end-user to manage certificates (view, delete and import) on his/her .NET device.

## View certificate

1. From the [User portal](#) menu select **Manage certificate**. All the certificates present on your .NET device will be listed.

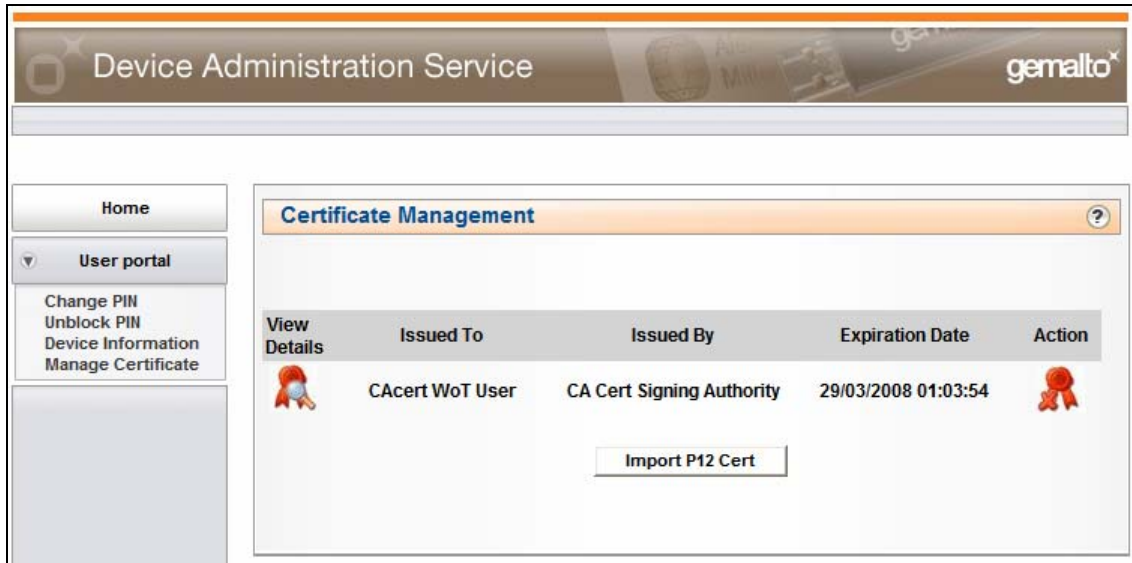


Figure 28 – Certificate management

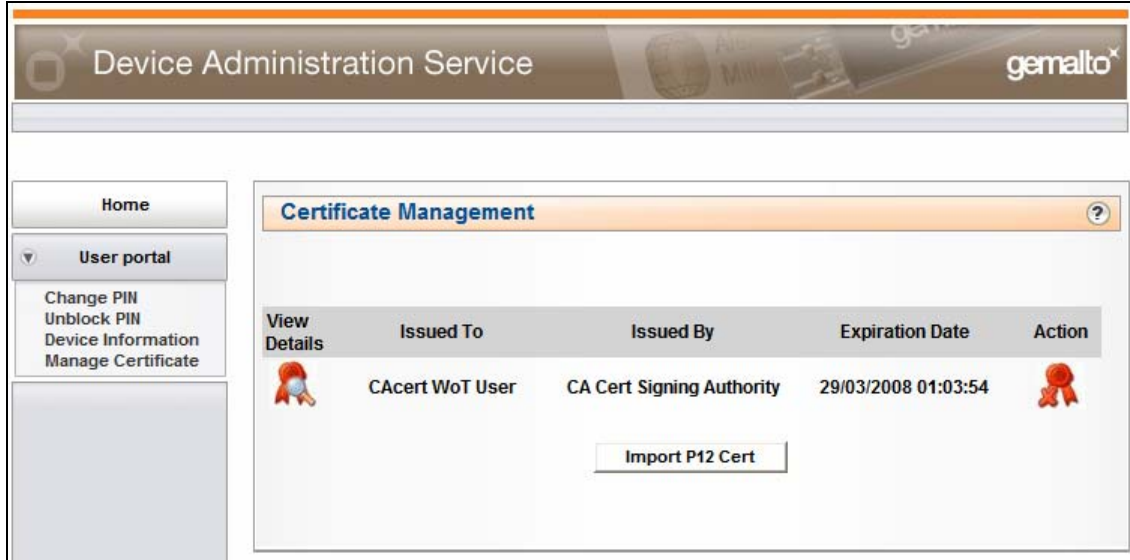
2. Click on the icon to view the details of the certificate.




Figure 29 – Certificate viewer

## Delete certificate

1. From the [User portal](#) menu select **Manage certificate**. All the certificates present on your .NET device will be listed.




*Figure 30 – Certificate management*

2. Click on the  icon located in front of the certificate you want to delete.

## Import certificate

1. From the [User portal](#) menu select **Manage certificate** then click on the Import P12 cert button. Click on the **Browse** button to select the P12 file you want to import on your .NET device. Once selected click on the **Import P12 cert** button.



The screenshot shows a window titled "Certificate Management" with a help icon in the top right corner. The main text reads: "Please select the P12 file and press the 'ImportP12 Cert' button again." Below this, there is a text input field for the "P12 File:" containing the path "d:\Documents and Settings\gpauzie\My Dc" and a "Browse..." button to its right. Below the input field is a button labeled "Import P12 Cert".

Figure 31 – Import P12 select

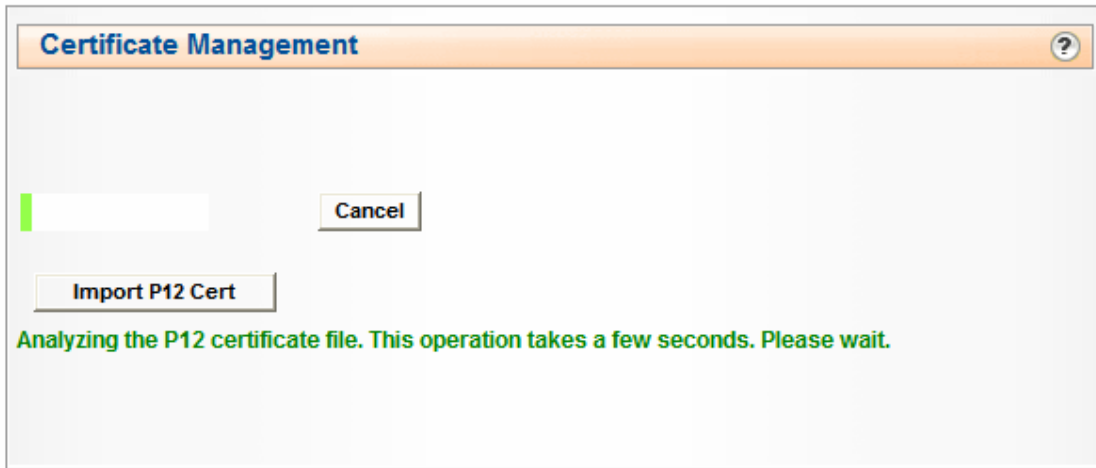
2. Enter the password protecting the P12 file and click on the **Next** button.



The screenshot shows the same "Certificate Management" window. The main text reads: "Please enter your P12 file password and press Next button." Below this, there is a "Password:" label followed by a text input field containing four dots and a "Next" button to its right. Below the input field is a button labeled "Import P12 Cert". At the bottom, there is a table with three columns: "Issued To", "Issued By", and "Expiration Date". The table contains one row with the following values: "CAcert WoT User CA Cert Signing Authority", "29/03/2008 01:03:54", and "Delete". Below the table, it says "There are 1 certificate(s)".

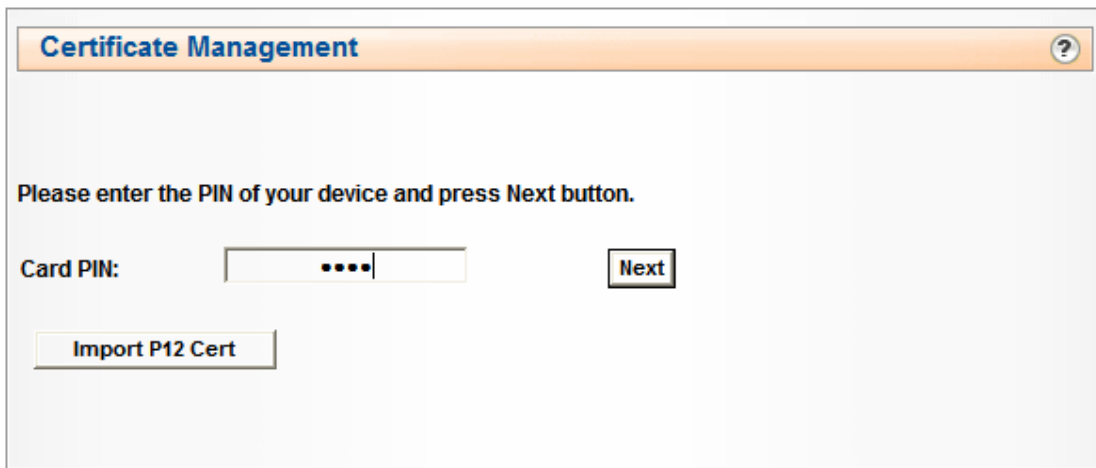
Figure 32 – Import P12 password

The P12 file is analyzed. This operation takes few seconds.



*Figure 33 – Import P12 analyzing*

3. Enter the PIN of your .NET device and click on the **Next** button.



*Figure 34 – Import P12 PIN*

4. The following message will then be displayed to confirm the import of the P12 file into the .NET device.

**The P12 certificate is now imported into the card**

*Figure 35 – Import P12 completed*



**Important:** *In cryptography, PKCS#12 is one of the family of standards called Public-Key Cryptography Standards (PKCS), published by RSA Laboratories. It defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key, and is the successor to PFX.* Source: Wikipedia.

The private key is very sensitive information; consequently a careful management of the P12 file is strongly advised.

For instance the transfer of a P12 file through email requires at the minimum encryption of the email particularly if the password protecting the P12 file is part of the content of the email. Similarly the storage of a P12 file is sensitive operation, every precaution must be taken so the P12 file does not get compromised as a brute force attack is possible to guess the password protecting it.

## Support and troubleshooting

Should you need assistance on the use of DAS please contact your Gemalto partner. Contact information can be found from the Administration portal on the Contact menu.

This appendix lists answers to some questions you may have about DAS and the way to use it.

## Frequently asked questions

### **I don't know where to get a digital certificate**

You can consult a Certificate Authority via Internet, telephone, or e-mail to request a digital certificate. The Certificate Authority may offer services to work with you to determine the type of certificate that best suits your security needs. Afterward, you can purchase the certificate that is appropriate for your needs. Some Certificate Authorities even offer trial certificates for no cost. Typically, trial certificates only require you to provide your name and e-mail address. Certificate Authorities typically do not invest in validating your identity when you obtain a trial certificate. Consequently, the level of trust assigned to your certificate is minimal. Certificate Authorities may deliver your digital certificate to you via e-mail, post, or the Internet. The most popular means of distribution is via the Internet.

### **I have an expired certificate in Internet Explorer and I can't delete it.**

To delete a certificate with Internet Explorer 6.0 or later:

- 1 Click **Tools > Options** to open the **Internet Options** dialog box.
- 2 In the **Internet Options** dialog box, click the **Content** tab
- 3 Click **Certificates** to open the **Certificate Manager** dialog box.
- 4 Select the certificate you want to remove.
- 5 Click **Remove**.

### **I tried to send a secure e-mail but received a message that something was wrong with the recipient's certificate.**

Check the validity of the user certificate. You may also want to contact the user directly to inquire about the status of their certificate. The user can always send a new signed message to you so that you can refresh or add the valid certificate.

### **I tried to send a secure e-mail but received a message that something was wrong with my certificate.**

Check the following:

- Verify that a valid certificate is linked to your e-mail account.
- Use the **Manage Certificate** tool to make sure the certificate you are using to send secure e-mail has not expired.

If the previous conditions are met and you still get the message that something is wrong with your certificate, contact your Certificate issuer for further assistance.

### **When I try to send secure e-mail, I get the message that there is no certificate associated with my e-mail account.**

Before you can send secure e-mail using the digital certificate stored on your .NET device, you must link your certificate to your e-mail account.

### **When I try to send secure e-mail, I get a message that says I don't have a certificate for the person I'm trying to e-mail.**

You could have one of three problems:

- **You do not have a certificate for this person** If you do not have a certificate for the user, you can add the user certificate by receiving a signed e-mail from the user or by obtaining the user's certificate from a public directory.
- **You do not have a certificate linked to the user's e-mail address** If you already received a signed e-mail from the user but the certificate is not associated with the user's e-mail address, you must open the signed e-mail and add the user's certificate to your Address Book (Outlook Express) or Contacts folder (Outlook 2003). If you are using Mozilla Thunderbird, you should not encounter this problem because when you receive a signed message from a user, their digital certificate is automatically linked to their e-mail address.
- **The certificate that you have for this user is not valid** You can view the user certificate to determine if it is valid using your e-mail software.

### **The recipients of my e-mail cannot decrypt my messages or attached files.**

Your contacts may not be able to decrypt the e-mail or attachments that you send to them because of the session key length specified in your browser. A session key is the cryptographic secret key that is used to encrypt the actual message text of your e-mail and attachments. (The RSA key pair is used to decrypt/encrypt the session key). Until recently, Mozilla and Microsoft browsers and e-mail applications were subject to cryptographic export regulations. As such, if you were sending e-mail to international contacts outside of the United States and Canada, you could have been using a session key that was too long or too strong. The session key length limitation for all versions of Internet Explorer and Mozilla Firefox is 128-bits. For some countries, the limit used to be 40-bits for the international versions of both products. In order to decrypt your e-mails, your recipients should be instructed to install Microsoft's High Encryption Package.

### **When I try to connect to a secure Web site that requests client authentication, it takes an exceptionally long time to connect if it ever connects.**

If you experience an extremely slow connection when you are trying to connect to a secure server, the problem could be related to the Web server, your computer, or your digital certificate. The best thing to do is to disconnect and try again. You may have simply had a bad connection. You can test connections to other secure Web sites to determine if the problem is related to a specific Web server. To rule out problems related to your computer, verify your hardware connections, communication settings, and security settings. Finally, view your certificate to make sure it is valid and make sure your Classic Client smart card is properly inserted into your smart card reader.

### **When I try to connect to a secure Web site that requests client authentication, I am rejected.**

If your certificate is rejected, try again. If your certificate is rejected again, investigate. You could be rejected if your certificate is not valid. Check the validity of your certificate using the **Manage Certificate** tool. The certificate might be getting rejected because:

- The Web server does not have an entry for the Certificate Authority that issued and signed the certificate.
- Your smart card reader is not properly connected or you do not have the appropriate reader driver installed.
- Your digital signature is temporarily corrupt, as in the case of an intruder trying to spy on your secure connection.

### **I am not warned prior to entering a secure Web site.**

You can tell a Web site is secure when its address starts with the characters **https**. If you want, you can set your browser to warn you before entering a secure Web site.

#### ***In Internet Explorer 6.0 or later:***

- 1 Click **Tools > Options** to open the **Internet Options** dialog box.
- 2 In the **Internet Options** dialog box, click the **Security** tab

- 3 Select a Web content zone to specify its security settings.
- 4 Click **Custom Level**.
- 5 Select **Prompt** under the actions for which you want to be warned.

**In Firefox 2.0:**

- 1 Click **Security** to open Firefox's security window.
- 2 Click **Navigator** on the left side of the window.
- 3 Select the options you want under **Show a warning before**.

### **If your smart card stops working**

If your smart card stops working, consider the following reasons:

- **Your smart card's PIN may be blocked** You can unblock your smart card as described in the section about unblocking a PIN.
- **Your smart card's certificate may have expired** You need to get a new certificate. See information about getting a new certificate.
- **You may be experiencing hardware failure** Ask your Administrator for help.

***END OF THE DOCUMENT***