

BACS payment services

Contact's guide



About this guide

Welcome to payment services. You have received this document as you have been registered as a contact to use one or more payment services or facilities.

The payment services web channel allows you and other contacts to access information about the services and maintain certain reference information held for these services.

This guide tells you all about what being a contact means, what you can do over the web channel, the security method(s) you will need to access the web channel and how you can alter information held about you.

This guide is divided into six parts:

Part I - Contacts: What a contact is and what it means

Part II - Payment services web channel: What it is & how it looks

Part III - Security overview: Methods available

Part IV - Security information and procedures: PKI

Part V - Security information and procedures: ASM

Part VI - Your details: How to change the information held for you.

This guide should be used in conjunction with the other guides you have received in relation to the payment services.

Contact information

t 0870 010 0698

t 0870 165 0018

e service.desk@bacs.co.uk

w www.bacs.co.uk

Telephone calls may be recorded for security or monitoring purposes.

Contents

Part I	7
Contacts	
1 What is a contact?	7
Security methods	7
Contact types	8
Privilege groups	8
Communication information	9
Part II	11
Payment services web channel	
2 What is the payment services web channel?	11
Connections	12
Security	12
Functionality	13
Notifications	13
3 Availability	14
4 Software requirements	15
4.1 Web browsers	15
4.2 Operating systems	15
5 Connection methods	16

5.1	Internet.....	16
5.2	Extranet.....	16
	Fixed extranet, DSL Connect and Broadband Direct	16
	Dial-up extranet	16
6	Payment services web channel – Features and tools	18
6.1	Navigating payment services	18
6.2	System notices.....	18
6.3	Online help.....	19
6.4	Areas of the web channel screen.....	19
6.5	Selection methods	21
6.6	Find functionality	22
6.6.1	Full text search	22
6.6.2	Part text search	22
6.7	Request messages, commands and error messages.....	23

Part III 25

Security overview

7	Overview	25
----------	-----------------------	-----------

Part IV 27

Security information & procedures – PKI

8	Security information: PKI	27
8.1	What are PKI credentials?	27
8.2	Storage of PKI credentials	28
8.3	Using PKI with payment services.....	29
8.3.1	What PKI is used for	29
8.3.2	What you need	29
8.3.3	How PKI security works with payment services	30
	Logging on	30
	Confirming an action	31
9	Security procedures: PKI	32
9.1	Overview	32
	What you will need	32
9.2	Smartcard activation	32
9.2.1	Overview	32
9.2.2	Smartcard initialisation	34
9.2.3	DN registration	34
	Manual registration	34
	Automated registration process	34
9.2.4	System checks	36
9.2.5	Welcome email and first log on	37

First log on	37
9.3 Logging on	39
9.4 Actioning changes	40
10 Protecting your smartcard and PIN	41
11 PKI statuses	42
12 Issues with your PKI security	43

Part V 47

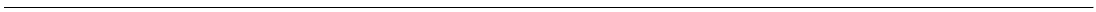
Security information & procedures – ASM

13 Security information: ASM	47
13.1 What is ASM security?	47
13.2 Using a contact ID and password with payment services	47
13.2.1 What ASM is used for	47
13.2.2 What you need	48
13.2.3 How ASM security works with payment services	48
Logging on	48
Confirming an action	48
14 Security procedures: ASM	49
14.1 Overview	49
14.2 Contact ID and password activation activities	49
14.2.1 Overview	49
14.2.2 Contact ID and password retrieval	52
14.2.3 Welcome email and first log on	54
First log on	54
14.3 Logging on	56
14.4 Actioning changes	58
14.5 Your password	59
14.5.1 Changing your password	59
14.5.2 Password specifications and guidelines	60
14.5.3 Protecting your password	60
14.5.4 Changing your security information and hint	60
15 Issues with your ASM security	61
16 ASM statuses	63

Part VI 65

Your details

17 Changing your details	65
17.1 Overview	65



17.2 How to change your details..... 66

Part I

Contacts

1 What is a contact?

A contact is an individual who has been registered to use payment services or facilities.

As a registered contact you will have a unique contact ID. Against your contact ID the following must be set up:

- Security method(s)
- Contact type
- Privilege groups
- Communication information.

The following sections provide more information about each of these.

Security methods

In order to access the payment services and facilities, all contacts must have one or more security methods assigned to them.

There are two security methods that can be used to access the payment services and facilities: PKI credentials (PKI), including a digital certificate, and contact ID and password (alternative security method – ASM). For more information, see Part IV and Part V.

As a contact you can be assigned PKI, ASM or both. Each security method you have assigned to you will have a status, for example “active”, “suspended”. Depending on the status of the security method, you will be able to use that security method to log on to the payment services web channel and perform actions you have been assigned the privileges to do. For more information on the payment services web channel see Part II, starting on page 11.

Contact types

There are two different types of contact:

- Primary security contacts (PSCs)
- Additional contacts (ACs).

A primary security contact (PSC) can normally carry out more functions than an additional contact, and there are some functions only a PSC can carry out. All contacts registered to access payment services and facilities must be set up as either a PSC or an additional contact. The decision as to whether you are a PSC or an additional contact will depend on the role you have when using payment services. The functions a PSC or an additional contact can perform will depend on the privileges they are given.

Privilege groups

All contacts must be assigned one or more privileges groups. Privilege groups contain one or more privileges which will allow you, as a contact, to carry out specific activities and functions with payment services. If you have a specific privilege group assigned to you, you will be able to carry out the functions allowed by the privileges in that group.

Privilege groups are assigned to you when you are registered as a contact for payment services, but these can be amended at any time. The privilege groups available for assigning to you depend on:

- Contact type (PSC or additional contact)
- Security method (PKI or ASM).

More privileges are available to PSCs and to contacts who have PKI credentials. There are no privilege groups that are exclusively available to additional contacts with ASM. In other words, all privilege groups that can be assigned to an additional contact with ASM could be assigned to any contact type. The privilege groups a contact is assigned will depend on the role they will have when using the payment services.

Communication information

Communication details are held for each contact registered to use the payment services, namely:

- Email address – mandatory
- Office telephone number, extension number and associated information – optional
- Out of hours telephone number – optional
- Mobile telephone number and associated information – optional
- Fax number – optional.

Part II

Payment services web channel

2 What is the payment services web channel?

As a registered contact for payment services and facilities, you can use your security method(s) to log on to the payment services web channel. The web channel is your way of accessing the payment services and facilities you have been set up to use and carry out the actions you have been given the privileges to do. The following diagram shows an example of the payment services web channel homepage. The exact features of your homepage will depend on what type of contact you are and what you can use the web channel for.



Figure 1: An example of the payment services web channel homepage

Connections

To connect to the payment services web channel you will require the following:

- An internet browser
- A connection method (normally internet, but can be an extranet connection)
- A security method.

For information on software requirements, including internet browsers, see section 4, page 15. For more information on connection methods see section 5, page 16.

Security

You can log on to the web channel using PKI or ASM. If you have both PKI and ASM you can log on using either, however, if you log on with ASM, you may not be able to carry out all the functions you have been given the privileges to do.

For information on the privilege groups available for allocation to you and the security methods and contact types they can be assigned to see the guide(s) you have received regarding the services you have been set up to use.

Functionality

The payment services web channel can be used to access various features of the payment services and facilities you have been set up to use.

In addition to the features and facilities you have been set up to use, all contacts can use the payment services web channel to view and amend their own communication details

For more information on how to perform these actions on the web channel see Part VI.

Notifications

When many actions are carried out on the web channel, email notifications are generated and sent to relevant contacts. For example, if any of your contact details are changed by another contact, you will receive an email notification telling you that your details have been changed.

To make full use of the payment services and facilities you have been registered to use there may be additional requirements. If this is the case, the guide(s) you receive detailing the services and features will provide information on these additional requirements.

3 Availability

The web channel is available during the payment services window. This window normally opens at 07:00 hours on a Monday and closes at 23:00 hours on a Friday. English bank/public holidays also affect the opening times. The following table shows how the window opens and closes:

If the window is...	it will...
...open	...close at 23:00 hours the night before a nonprocessing day (a bank/public holiday, a Saturday or a Sunday).
...closed	...open at 07:00 hours on the first processing day after a nonprocessing day.

When the payment services window is open you can log on to the web channel. Once you are logged on, you can perform the functions you are set up to do over the web channel. For details of nonprocessing days see the processing calendar available from:

<http://www.bacs.co.uk/resources/calendar.php>

4 Software requirements

There are certain hardware and software requirements you must fulfil to access the web channel. The following sections detail the operating system and web browser requirements for connecting the BACS payment services web channel.

4.1 Web browsers

It is recommended that you use the latest version available of your chosen web browser. For information about browsers suitable for accessing the web channel using PKI contact your supplier of signing software. If you are using Internet Explorer you should ensure that your browser checks for newer versions of stored pages automatically. This is the default for your browser, but to check this setting and amend it if necessary carry out the following steps.



To set Internet Explorer page checking

You must have Internet Explorer installed.

1 **Open Internet Explorer.**

Open Internet Explorer on the computer you will use to access the web channel.

2 **Access your internet options.**

From Internet Explorer's *Tools* menu select *Internet Options...*

An *Internet Options* window will open. On the *General* tab, in the *Temporary Internet files* section, click the *Settings* button.

3 **Amend your settings.**

A *Settings* window will open. Ensure that the stored pages setting is set to *Automatic*. If not, click in the radio button, next to the word *Automatic*. Click *OK*, then click *OK on the Internet Options* screen.

4.2 Operating systems

In addition to a suitable browser, you must be running a suitable operating system on the computer you use to access the web channel. The following operating systems have been tested for connecting to the payment services web channel:

- Windows NT4 with service pack 5+
- Windows 98 SE
- Windows ME
- Windows 2000
- Windows XP.

5 Connection methods

Access to the payment services web channel will normally be via the internet. However, the web channel can also be accessed via the extranet. The following sections provide information for connecting via these two methods.

5.1 Internet

The normal method for connecting to the payment services web channel is via the internet. To access the payment services web channel over the internet, you should be connected to the internet and then go to the payment services web address (URL). When you receive your welcome email from BACS payment services, this will provide you with the web address (URL) that you should use.

5.2 Extranet

If required, you can connect to the payment services web channel via the extranet. Voca offers a fixed extranet, DSL connection, Broadband Direct and a dial-up extranet.

Fixed extranet, DSL Connect and Broadband Direct

If you would like more information about connecting to Voca over a fixed extranet, DSL Connect or Broadband Direct connection visit:

www.voca.co.uk/connectivity

Dial-up extranet

Although connecting to the payment services web channel is normally done over the internet, it can also be done via the dial-up extranet facility.

When connecting to the dial-up extranet one of two numbers¹ is dialled:

- 0870 241 6764
- 0870 163 6300.

An extranet ID and password are also required for connecting to the web channel via the dial-up extranet. An extranet ID and password can be used to connect to payment services by up to 10 different contacts at the same time. That is, up to 10 computers can be connected to the dial-up extranet at the same time using the same extranet ID and password.

¹ These numbers are subject to change. Your system should allow for these numbers to be altered when necessary.

If you have the use of more than one extranet ID and password you can use any of them to connect. However, the maximum number of concurrent connections with the same extranet ID and password is still 10. If 10 contacts are connected to the dial-up extranet using the same extranet ID and password, you will not be able to connect. There is no check made between the person logging on and the extranet ID that has been used to establish the dial-up connection.

If you require more information about how to go about utilising the dial-up extranet contact the service desk or your sponsor, if you have one.

6 Payment services web channel – Features and tools

The following sections provide an overview of how you can navigate around the web channel and the features and tools you will use when carrying out activities on the web channel.



Note: Fields shown on a page on the payment services web channel that are marked with an asterisk () are compulsory. You must complete these fields to successfully carry out the activity.*

6.1 Navigating payment services

Navigating payment services is much the same as other websites, with buttons and hyperlinks providing access to different areas and screens.

Most screens have on-screen navigation buttons that should be used for going “back” and for cancelling actions. You must not use the browser’s own buttons when logged on to the web channel as some pages may not load correctly. For example, do not use the browser’s back, forward, refresh or home buttons.

6.2 System notices

System notices are used to provide you with service and operational information. If a system notice has been marked as urgent, it will appear on the payment services homepage; to view it, just click on the title and the *View system notice* screen loads, showing you the full system notice. For a printer friendly view, click *collect*; the notice will open in a new window.

In some cases, a PDF may be attached to the system notice. To view this, on the *View system notice* screen, click on the file name; the PDF will open in another window. You will need Acrobat Reader to view this.

Where a system notice is not marked as urgent, to be able to view it, select *System notices* from the menu, then click *Collect system notices*. Under *Search by details*, click *find* (you can enter search criteria if you want to limit your search). A list of available system notices is displayed. To view one, click on the sequence number and the *View system notice* screen loads.

6.3 Online help

There is help available on the web channel. To access the help information available, click the *Help* button on the top right hand corner of the page. The help information should be used in conjunction with any other documentation you have received.

Clicking the *Help* button will open a new window, in which the help information will be displayed. Along with any help information, there will be a link to the help main menu. From the help main menu you can browse to help information for other pages.

6.4 Areas of the web channel screen

All web channel screens have some areas that are the same or similar. The following figure shows a typical web channel screen, highlighting the key areas that are the same or similar across all screens. The names of these areas, and details of their functions, are provided in the table that follows.

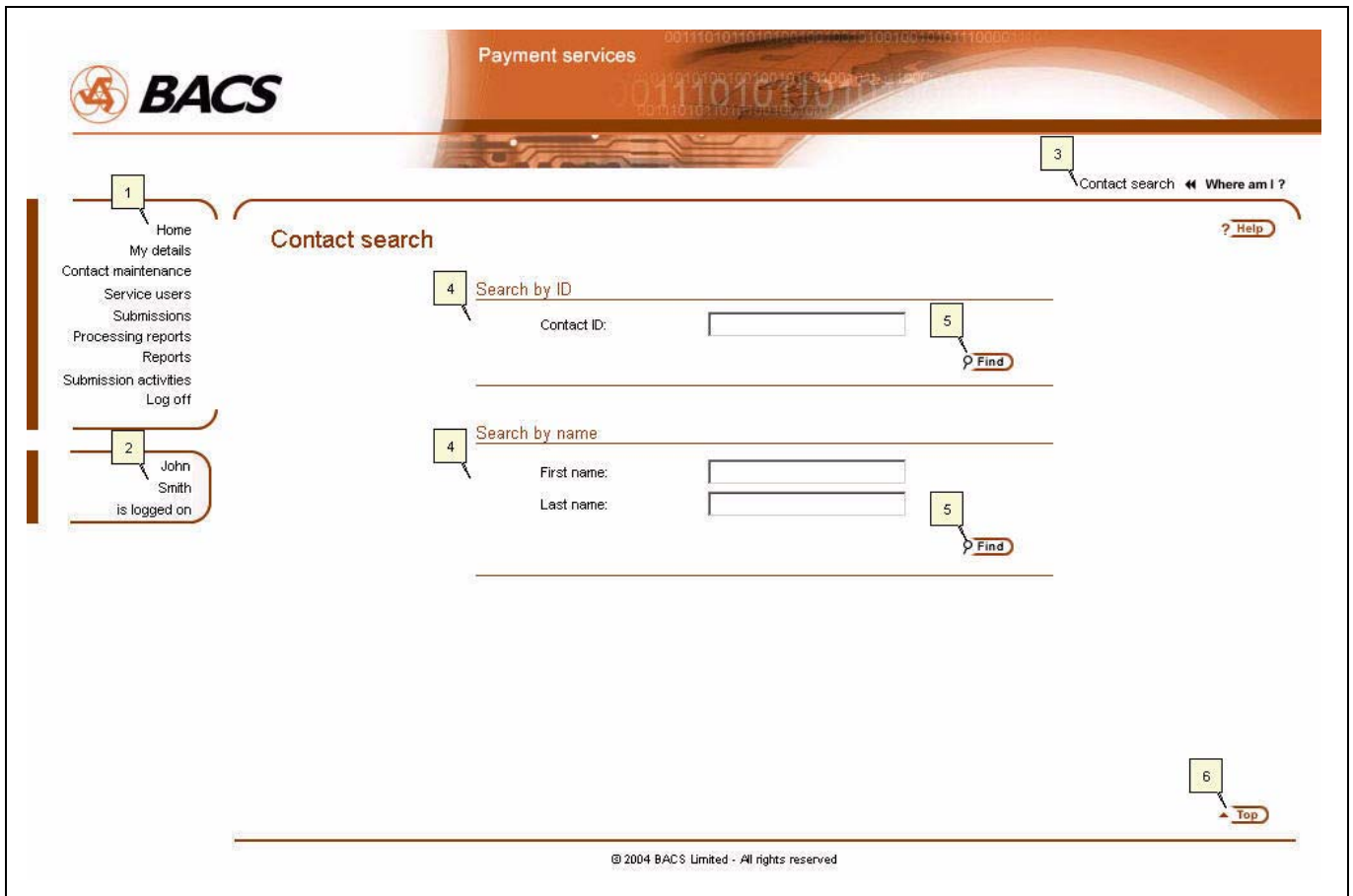







Figure 2: The areas of a web channel screen

Area	Name	Function	When seen
1	Menu	Selecting a menu option takes you to that area of the web channel.	Same on all pages.
2	Contact identification	Shows the first name and surname of the contact who is logged on.	Same on all pages.
3	“Where am I?” bar	Shows where in the web channel you are at that moment.	Differs on each page to reflect where you are.
4	Section block	The area of the screen where you can action something or view/confirm information. Some screens have several section blocks.	Different blocks appear on different pages.
5	Action buttons	There are a variety of different buttons on the web channel. The icon and the wording illustrates what each button does. To carry out the function a button provides, click the cursor on the button.	Different buttons appear on different pages.
6	Top button	Takes you to the top of the screen you are on. If you are at the bottom of a long screen you can click this button to take you back to the top.	Same on all pages.

6.5 Selection methods

The web channel uses standard selection methods for choosing options, dates etc. The following table details the different selection methods you will come across on the web channel and how to use them.

Type and example	What you can select	How to use the selection method
Radio button 	One option only.	To select, click in the circle next to the option you want (in the example “Live” is selected). To select a different option, click in the circle next to the new option you want. This will deselect the original option.
Check box 	One or more options.	The selected option(s) is shown as a box with a tick. In the example, “Arrival Report” and “Live Input Report” are selected. To select options, click in the box next to the options required. Ticks will appear in all boxes you click in. To deselect an option click in the box again. This will remove the tick.
Drop down list 	One option only.	The selected option is shown in the box next to the drop down list. In the example “2002” has been selected. To select an option click on the arrow on the right side of the box. A list of options appears. Move the cursor until the option you want is highlighted and click it. The option you selected will be displayed in the box. To select a different option, repeat the above steps.
Pick list 	One or more options.	Selected options are highlighted. In the example, “Arrival Report”, “Withdrawal Report” and “Test Input Report” are selected. To select, click on the option. This will highlight it. To select a different option, click on it. This will highlight the new option and deselect all other options. To select more than one option, hold down the “ <i>Ctrl</i> ” key on your keyboard which clicking each of the options you want. Clicking on a highlighted option will deselect it (hold down the “ <i>Ctrl</i> ” key to keep the other options selected). To select a group of options, hold down the “ <i>Shift</i> ” key on your keyboard and click on the first and the last options from the group that you want. This will highlight the two you clicked and all options in between. Alternatively, to select several options together, click on the first option you want and, while holding down the mouse button, drag the cursor down the list until all the options you want are highlighted.
Action button 	Used to perform a function.	To carry out an action, click on the button. Many buttons have additional information about the functioning of the button which can be viewed by hovering the cursor over the button. If additional information is available, a box of text will appear.

6.6 Find functionality

A number of activities on the web channel require a “find” to be done to look for the required information. Search types that are used on the web channel include:

- Name searches (name, first name or surname)
- ID searches.

These search types use different searching methods. The different search methods are “full text” and “part text” searches.

6.6.1 Full text search

A “full text” search means that you enter all the characters that you are searching for. For example, if you are looking for a contact whose contact ID is *smith123456* you would type each character of the contact ID into the find box.

6.6.2 Part text search

A “part text” search means that you can enter just some of the characters you are searching for. For example, if you are looking for someone whose surname is *Smith* you could type *Smi* or just *S* into the find box. The only constraint is that you must start your part text with the first character – you could not search by typing *mith* to find *Smith*.

Only some search types can use part text. The following table illustrates which search types can be done using part text searching, and provides additional notes on each search type.

Search type	Full text searching	Part text searching	Notes
Name search	✓	✓	Not case sensitive.
First name search	✓	✓	You can search for the first name, surname or both. Not case sensitive.
Surname search	✓	✓	
Organisation ID	✓	✗	Case sensitive.
Contact ID	✓	✓	Not case sensitive.

6.7 Request messages, commands and error messages

On the web channel, red text will sometimes appear above section blocks. This text may be:

- A request message; or
- A command; or
- An error message.

The text will provide you with an instruction on how to complete the screen you are on, or explain why your last request was not successful, or advise you of the action you have completed.

Part III

Security overview

7 Overview

Access to payment services is controlled with high levels of security. To access payment services as a registered contact, you must identify yourself and pass security checks. There are two security methods that can be used to access the payment services web channel:

- Public key infrastructure (PKI)
- Contact ID and password (alternative security method – ASM).

As a contact, you must have at least one of these security methods. Fewer privileges can be given to contacts who only have a contact ID and password. If you have both security methods (PKI and ASM) you may not be able carry out all the functions you have been set up to carry out if you access the payment services using your contact ID and password.

When you carry out actions on the payment services web channel you will have to authorise the actions. For details on how to confirm actions see section 9.4, page 40. You must confirm actions using the same security method that you used to log on to the web channel.



Note: When using PKI to log on to the web channel, this guide assumes these PKI credentials are on a smartcard. It is not expected that contacts will log on to the web channel using an HSM. For information about HSMs please contact your solution supplier.

Part IV provides information about PKI security and some fundamental PKI procedures. Part V provides information about ASM security and some fundamental ASM procedures. The information in these parts includes how the security methods work, what the different methods are used for and what you will receive if you are set up for that method.

Security information & procedures – PKI

8 Security information: PKI

8.1 What are PKI credentials?

PKI uses digital keys and digital certificates to provide security for electronic communications and data transfers. This security provides authenticity and integrity.

A contact's PKI credentials are made up of their digital keys and their digital certificate. These PKI credentials are issued (directly or indirectly) by a certification authority.

The following introduces some of the common terms you will hear in relation to PKI security:

Term	Definition
Certification authority (CA)	A trusted third party that issues and manages digital keys and certificates. During secure communications, the CA associated with a contact's digital certificate is contacted to confirm if the name given on the digital certificate is the one that is associated with the public key on the certificate.
Digital keys	A contact has two sets of digital keys: a private key and a public key. A contact's private key is only known to the contact. A contact's public key can be known by anyone.
Digital certificate	A "document" that contains, among other things, a copy of the contact's public key, details of the contact's name, the contact's assigned "distinguished name" and the expiry details of the certificate. The certificate is signed by the certification authority's own private key as proof that the contact's digital certificate is genuine.
Distinguished name (DN)	A unique piece of information allocated to a contact, partly based on their name, which is held on the contact's digital certificate. This information is recorded by BACS for all registered PKI credentials.

In this guide, "PKI" is used to refer to all aspects of a contact's PKI credentials required to carry out the security processes described in Part V.

8.2 Storage of PKI credentials

A contact's PKI credentials are normally issued and held on a smartcard. The following diagram provides an overview of a smartcard and how a contact's PKI credentials are held on it.

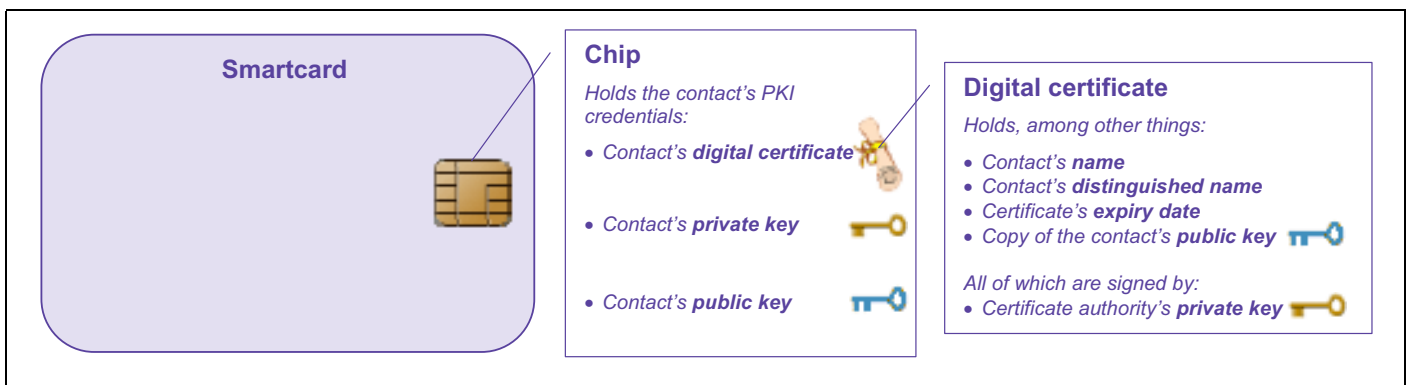


Figure 3: A stylised diagram of a smartcard and PKI credentials

PKI credentials can also be held on a hardware security module (HSM). An HSM is used by companies who require a high volume of automated digital signing and verification.

8.3 Using PKI with payment services

8.3.1 What PKI is used for

You can use your PKI credentials to do the following:

- Log on to the payment services web channel
- Confirm actions you have carried out on the payment services web channel.

You will also be able to use your credentials to perform specific activities you have been given the privilege group(s) to do for the payment services and functions you can use.

If you have PKI credentials, you are obliged to use them when invited to do so by the payment services web channel.

8.3.2 What you need

If you have a PKI credentials stored on a smartcard, you will need the following to use your credentials to create digital signatures and authenticate yourself when using payment services:

- Smartcard reader
- Signing and decryption software
- PIN (personal identification number)¹.

Your PIN is used to control the security of your smartcard, and your PKI credentials stored on it. Your PIN is specific to your smartcard and is issued when your smartcard is issued to you. The PIN (which may contain alpha characters as well as numbers) must be entered each time you use your smartcard to digitally sign data.

Similar security measures exist for the operation of HSMs. However, once activated, the signing and decryption are generally fully automated and do not require further human intervention until the HSM is shut down.

¹ Some signing software refers to PINs as a "passphrase".

8.3.3 How PKI security works with payment services

If you have PKI credentials on a smartcard, you can use these for logging on to payment services and authorising actions on the web channel. The following describes how PKI security works with payment services.

Logging on

To authenticate you as a contact, when you log on to payment services with your PKI credentials, the BACS payment services system will send you a string of random text. Your signing software will load on your computer and will display this string of random text.

To authenticate yourself, you will have to “digitally sign” the random string of text. To do this, you must insert your smartcard into your smartcard reader attached to the computer and enter your PIN into the software. Your software will then “digitally sign” the string of text by processing the data using your private key. This produces a digital signature. The digital signature is then sent back to the BACS payment services system along with a copy of your digital certificate.

If the BACS payment services system is unable to validate your digital signature, the system will reject the data and terminate the action. This may be because:

- The data may have been altered since being digitally signed, either intentionally or accidentally; or
- The private key used to create the digital signature does not match the public key contained within the copy of your digital certificate that was appended to the data; or
- The BACS payment services system was not able to verify with the certification authority that your digital certificate is still valid (ie that it has not been revoked or is unknown) and that there is a valid link to the root certification authority (the highest level of trust within the PKI scheme).

The following diagram gives an overview of the processes involved in logging on to payment services with PKI security. A similar process is carried out when confirming an action on the payment services web channel, except the text to be digitally signed details the nature of the action being confirmed.

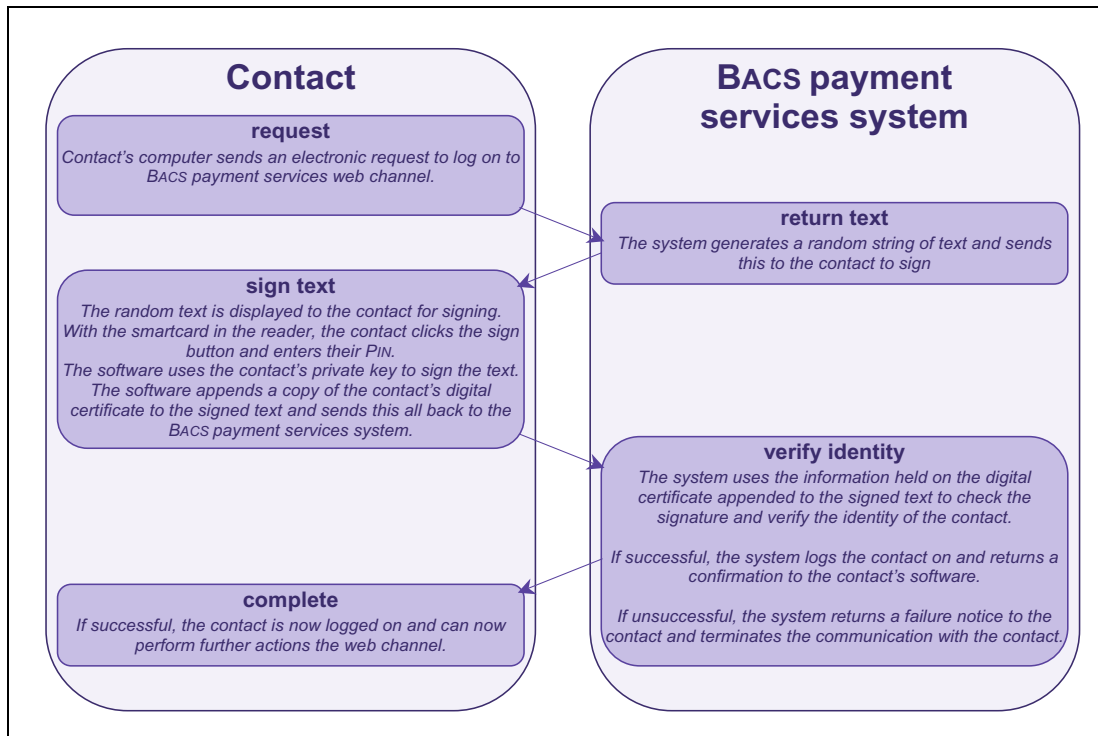


Figure 4: An overview of PKI security processes for logging on to BACS payment services

Confirming an action

To confirm an action on the payment services web channel using your PKI credentials, you will have to carry out a similar process as that described for logging on. However, instead of the BACS payment services system sending you a string of random text, the system will send you data that relates to the information you are confirming you want processed. It is this data that you will digitally sign to confirm the action.

9 Security procedures: PKI

9.1 Overview

PKI credentials stored on a smartcard can be used to access payment services. Before you can use your smartcard it must be activated. The following sections detail how to activate your smartcard for use with payment services, and then how to use your smartcard to log on to the payment services web channel and perform activities and functions on the web channel.

What you will need

Before you can start using PKI security to access payment services, you will need to wait until you have the following:

- Your smartcard
- A smartcard reader
- Signing and decryption software
- Your PIN.

How you receive your PIN will vary depending on your card supplier. Your card supplier may be your sponsor, if you have a sponsor. Your PIN may arrive before your smartcard (or vice versa). You must ensure that you keep both securely and separately until you are ready to get started.

9.2 Smartcard activation

9.2.1 Overview

Before you can use your PKI credentials on your smartcard to carry out any function, there are certain activation activities that need to be carried out. The following list details the activities that must be carried out before you can use your smartcard for the first time:

- Smartcard initialisation
- DN registration
- System checks
- Welcome email and first log on.

The following flow diagram provides an overview of these activation activities.

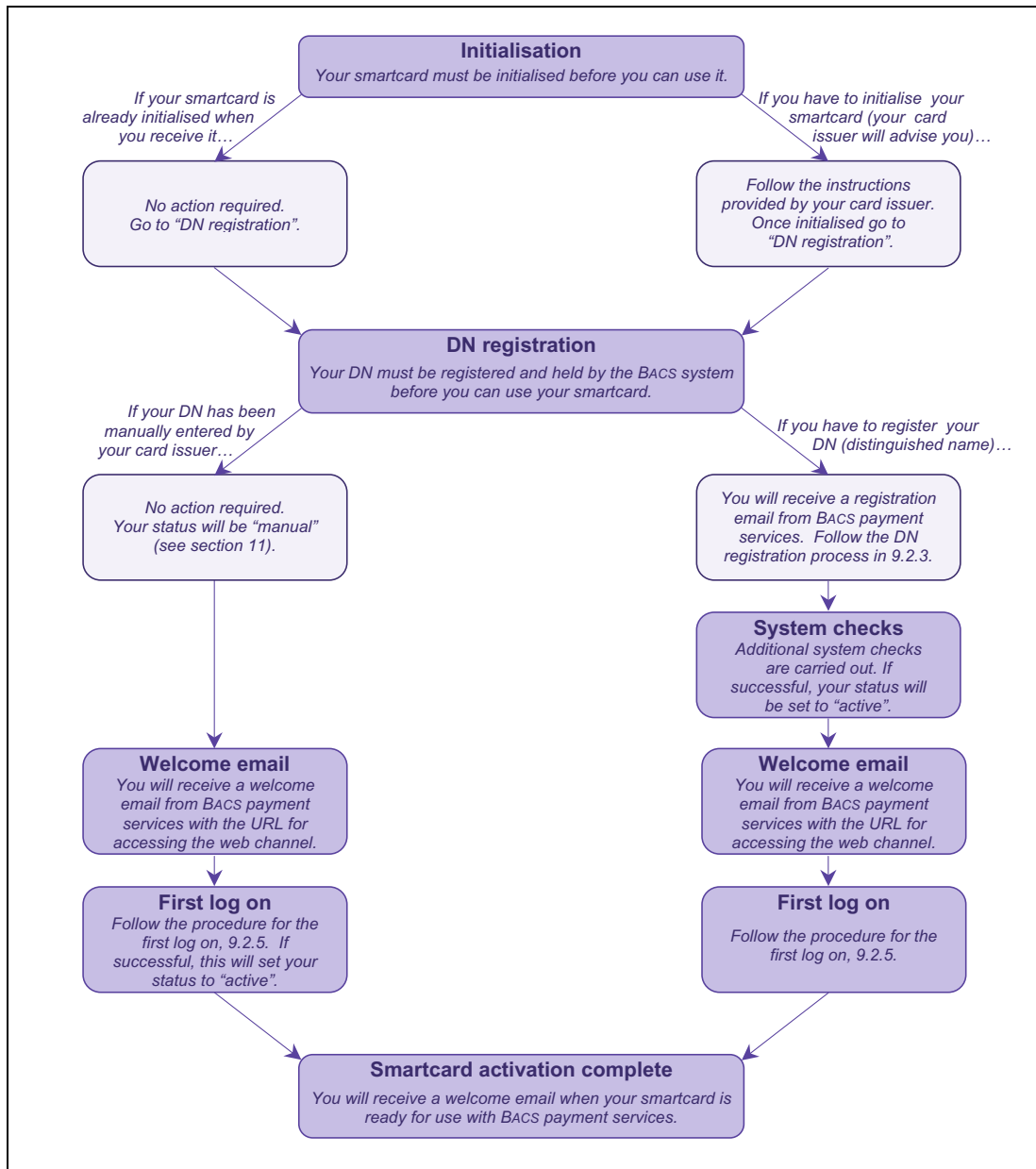


Figure 5: Overview of the smartcard activation process

The above diagram is an overview, and exact processes may differ depending on the smartcard issuer. For specific details of the actions you must carry out, please refer to any instructions you have received from your card issuer.

You can find more information about each of these activities in the following sections. If you are issued with a replacement smartcard you must check with your card supplier which of these activities you will need to carry out.

9.2.2 Smartcard initialisation

A smartcard must be initialised before it can be used. Your card supplier may provide you with a smartcard that has already been initialised. If not, you may have to carry out an initialisation procedure. Your card supplier will advise you as to whether you need to initialise your smartcard, and if you do will provide you with details of the initialisation process.

9.2.3 DN registration

Before you can use your initialised smartcard, the DN or “distinguished name” on your digital certificate must be registered with and stored on the system.

Your DN can be registered with on the system, or by an automatic process. The following sections explain each of these.

Manual registration

Your card supplier may register your DN manually on the system. This means that you will not have to carry out the automated registration process described below. If your card supplier does register your DN manually, you will have a PKI status of “manual”. For more information on statuses see section 11, page 42.

Your card supplier should inform you whether your DN has been registered manually, or whether you have to carry out the automated registration process. However, if you receive an email from BACS payment services with a subject of “BACS Payment Services – Registering your smartcard” you will have to carry out the automated registration process. If you do not receive this email, but do receive a “Welcome to BACS payment services” email your DN has been manually registered and you can go straight to section 9.2.5, page 37.

Note: All DNs for PKI credentials held on HSMs will be manually registered.

Automated registration process

You may need to carry out the automated registration process to register your DN on the system. Your card supplier should inform you whether you need to carry out this registration process. However, if you receive an email from BACS payment services with a subject of “BACS Payment Services – Registering your smartcard” you will have to carry out this automated registration process. If you do not receive this email, but do receive a “Welcome to BACS Payment Services” email your DN has been manually registered (see above) and you can go straight to section 9.2.5, page 37.

If you need to carry out the automated registration process, your “BACS Payment Services – Registering your smartcard” email will contain a unique URL (web address). These instructions should be used in conjunction with the following procedure.

Your registration email should be on, or easily transferred to, the computer that you will use to access the payment services web channel. If this cannot be done, you can find instructions in the following procedure on how to copy the URL from the email to the computer that will be used to access the web channel.

If you accidentally delete your registration email you can have it resent. To organise having it resent, contact a PSC who can maintain your details, your sponsor, if you have one, or the service desk.

Note: Do not attempt to carry out the following procedure if you do not have the following:

- *Your registration email with registration URL*
- *Your initialised smartcard*
- *Your PIN*
- *A smartcard reader and associated signing software on the computer that you will use to access the web channel.*



To register your DN

You must have your registration email, your initialised smartcard and your PIN.

1 Establish a connection to the internet (or extranet).

Connect to the internet, or the extranet if this will be used to access the web channel.

2 Go to your registration URL.

Open the email “BACS Payment Services – Registering your smartcard” and click on the URL (web address). Your web browser will open and the *Digital certificate registration* screen will load.

Alternatively, copy the registration URL from the email, open a web browser and paste the URL into the address bar. Press the *Enter/Return* key on your keyboard.

If your registration email is on a different computer, than that used to access the web channel, and it cannot easily be transferred, copy the URL from the email and paste it into a Microsoft Word, Notepad or other document and save it to a disk. Open this document on the computer that will be used to access the web channel. Copy the URL from the document and paste it into your web browsers address bar. Press the *Enter/Return* key on your keyboard.

To register your DN (continued)

3 Confirm your name.

The *Digital certificate registration* screen displays the contact name associated with the URL.

If this is your name, click *confirm*.

If this is not your name, check that you have used the correct email. If you are using the correct email and your name is incorrect, contact a PSC who can maintain your details. The PSC should check your details on the web channel.

4 Signing software opens. Insert your smartcard and sign the random text.

Your signing software will automatically open. Insert your smartcard into your reader.

A random string of text will be displayed in the signing software window. To authenticate yourself, you must digitally sign this string of text. To do this, click the *sign* or *sign and submit* button on your signing software. You will need to enter your PIN.

5 A screen loads stating that you have successfully registered your digital certificate.

If the registration process was successful, a screen loads informing you. You can now close your browser.



Note: Although your registration process may have been completed successfully, system checks need to be carried out. You must now wait until those checks are complete and you have received your welcome email before you use your smartcard for anything.

9.2.4 System checks

Once your DN is registered on the system, additional system checks are carried out. If your DN was manually registered you will still have a status of “manual” after successful completion of system checks. If you registered your DN through the automatic process, your status will become “active” if system checks are successful.

When the system checks have been successfully completed, you will receive a welcome email from BACS payment services.

9.2.5 Welcome email and first log on

When the system checks have been successfully completed, you will receive your “Welcome to BACS payment services” email. Your welcome email contains the web address you must use for accessing the web channel with your smartcard.

You can now carry out the procedure for logging on to the web channel for the first time. If your DN was manually registered (you have received your welcome email and have not had to carry out the automatic registration procedure) carrying out the first log on procedure successfully will change your status from “manual” to “active”.

First log on

You must carry out the following procedure, once your welcome email arrives, before you use your smartcard for anything else. The following procedure details how to log on for the first time, and how to create a shortcut to BACS payment services for ease of logging on in the future.



To log on for the first time with PKI

You must have your welcome email, your initialised/registered smartcard and your PIN.

1 Establish a connection to the internet (or Voca extranet).

Connect to the internet, or the Voca extranet if this will be used to access the web channel.

2 Go to your welcome URL.

Open the email “Welcome to BACS payment services” and click on the URL (web address). Your web browser will open and the *Log on* screen will load.

Alternatively, copy the welcome URL from the email, open a web browser and paste the URL into the address bar. Press the *Enter/Return* key on your keyboard.

If your email is on a different computer, than that used to access the web channel, and it cannot easily be transferred, you can write the URL down and type it into your web browser’s address bar. Press the *Enter/Return* key on your keyboard.

To log on for the first time with PKI (continued)

3 Create a shortcut to the web address.

When the *Log on* screen loads, and your signing software opens, click your mouse on the web browser window. This will ensure that it is the web browser window that is active, and not the signing software. The signing software will stay open in front of the web browser, but will be the inactive window.

Press *Ctrl + D*. This will create a shortcut to BACS payment services that can be accessed through the *Favourites* menu of Internet Explorer and the *Bookmarks* menu of Netscape Navigator.

4 Sign the random text.

Click your mouse on the signing software window to make it the active window. Your signing software will present you with a random string of text to sign that will authenticate you to the web channel. Sign the text by doing the following:

- Insert your smartcard into your reader (if it is not already inserted)
- Click the *sign* or *sign and submit* button on your signing software
- Enter your PIN.

5 BACS payment services web channel homepage loads.

If the authentication process was successful, the web channel homepage will load into your browser, and your name will appear in the contact identification area of the page (see section 6.4, page 19 for details of the screen areas).

You can now carry out activities on the web channel, and your smartcard is now ready to use for all the activities and functions you have been given the privileges to do.

9.3 Logging on

After you have completed the first log on procedure (*First log on*, page 37) you can use your smartcard to log on to the payment services web channel and perform the functions you have been given the privileges to do. The following section describes how to log on to the web channel using your PKI credentials which involves authenticating yourself to the web channel.



To log on to the web channel with PKI (after first log on)

You must have carried out the first log on procedure for PKI.

1 Establish a connection to the internet (or Voca extranet).

Connect to the internet, or the Voca extranet if this will be used to access the web channel.

2 Open your web browser.

If you already have a browser open, you should close it and open a new browser window.

3 Go to your BACS payment services web channel shortcut.

If your browser is Internet Explorer, click on the *Favourites* menu and choose BACS payment services from the drop down list.

If your browser is Netscape Navigator, click on the *Bookmarks* menu and choose BACS payment services from the drop down list.

The *Log on* screen will load.

4 Sign the random text.

Your signing software will present you with a random string of text to sign that will authenticate you to the web channel. Sign the text by doing the following:

- Insert your smartcard into your reader (if it is not already inserted)
- Click the *sign* or *sign and submit* button on your signing software
- Enter your PIN.

5 BACS payment services web channel homepage loads.

If the authentication process was successful, the web channel homepage will load into your browser, and your name will appear in the contact identification area of the page (see section 6.4, page 19 for details of the screen areas).



Note: If you log on to the web channel and you do not perform any activity on the web channel (the session is idle) for 10 minutes, the session will time out. You will have to reauthenticate yourself before you can perform any more activities on the web channel. To reauthenticate yourself, carry out the log on procedure from step 4 onwards.

9.4 Actioning changes

When you change or add/delete information on the web channel, you will be asked to confirm that you wish to make the change(s). You must confirm the changes using the security method you logged on to the web channel with. The following procedure details how to confirm changes using your PKI credentials. For information on how to confirm changes using your contact ID and password, see section 14.4, page 58.



To action changes using PKI credentials

You must have logged on using your PKI credentials and made changes on the web channel.

1 Review a summary of your changes and accept them.

A *Summary* screen is displayed detailing the changes you are making. If the summary is correct, click *confirm* to start the process of actioning the changes.

2 Authorise the changes by signing the text displayed.

A confirmation screen will be displayed where you authorise the changes by entering your security credentials. If you logged on to the web channel with your PKI credentials, and are therefore authorising the changes with your PKI credentials, your signing software will load, displaying text detailing the change(s) you are going to make. Enter your PIN to sign the text. You will “digitally sign” the text displayed, and hence sign the change(s) you are making.

If the changes were made successfully, a *Success* screen will load. In some circumstances, eg your browser crashing, you may not see the success screen. Should this occur, you should check whether the changes you input have been applied.

If at any point, before signing the text, you decide you do not want to make the change(s) click the *cancel* or *back* action buttons on the screen. Depending on the stage you are at you may be taken to:

- A screen asking “Are you sure” you want to cancel the activity
 - Click *yes* to lose any changes that have not been confirmed, or
 - Click *no* to go back to confirm the changes or to make further changes.
- A maintenance screen where you can
 - Make further changes, or
 - Click *cancel* to be taken to the cancel activity screen (see first bullet point).



Note: Following many changes actioned on the payment services web channel, email notifications are sent by BACS payment services to the PSCs associated with the contact making the changes. The email notifications detail what was changed, who made the change(s) etc.

10 Protecting your smartcard and PIN

As your PIN is not known to anyone other than yourself, if you forget your PIN you will need to contact your card supplier as your smartcard may need to be replaced.

Some smartcards will allow you to change your PIN, others will only allow you to change it the first time you use it, others will not allow you to change it at all. If you would like to change your PIN you should read the documentation that accompanied your signing software.



Note: Contact your card issuer immediately if you have any smartcard problems.

- *Do NOT write your PIN down.*
- *If you think your PIN has been compromised, contact your card supplier immediately. Do not use your smartcard until your card supplier has advised you of what action to take.*
- *If you lose your smartcard you must contact your card issuer immediately.*

11 PKI statuses

If you have been set up for PKI security, you will have a PKI security status. To use your smartcard, you will need to have a PKI status of “Active”. There are other possible statuses that you could have. The following table details the possible statuses that you may have for your PKI security, and what it means if you have that status.

Status	What it means
Not set	You have not been set up to have PKI credentials for accessing payment services.
Active	You can use your PKI credentials for everything you have been set up to do. If you are set up to use the BACS electronic funds transfer service, you must have a status of active before you can sign payment files or submissions.
PKI pending	You have not yet registered your DN. For details of how to register your DN see section 9.2.3, page 34.
Suspended	<p>You cannot log on or perform any action using your PKI credentials.</p> <p>The status of “Suspended” may have been automatically generated by the BACS payment services system following an incident (eg you have logged on to BACS payment services but your digital certificate has been revoked).</p> <p>The status of “Suspended” may have been set by your card issuer, your sponsor (if you have one), Voca or a PSC who can amend your details, through the process of suspending a contact.</p> <p>If you also have a contact ID and password, providing your ASM status is “active”, you can continue to carry out everything you have been set up to do using your contact ID and password, providing it is not a PKI only activity.</p> <p>If you only have PKI security, or if your ASM status is also “Suspended”, you will no longer receive any notification emails.</p>
Suspended - Pending	<p>As for “Suspended”, you cannot log on or perform any action using your PKI credentials.</p> <p>You were in a state of “PKI pending” before you were suspended, and, if you are reinstated, your status will revert to “Pending”.</p> <p>If you also have a contact ID and password, providing your ASM status is “active”, you can continue to carry out everything you have been set up to do using your contact ID and password, providing it is not a PKI only activity.</p> <p>If you only have PKI security, or if your ASM status is also “Suspended”, you will no longer receive any notification emails.</p>
Manual	Your DN has been manually registered on the system. Your status will automatically change to “Active” the first time you log on the BACS payment services using your PKI credentials, providing the DN on your smartcard matches the DN held by on the system.
Review	You have registered your DN and your sponsor (if you have one) is going to review your DN. Providing the DN registration process was successful, your sponsor will set your status to “Active”.

12 Issues with your PKI security

This section details the possible issues you may experience with your PKI security, and actions you can take to overcome them.

Issue and description	Action
DN registration issues	
<p>Email deleted/cannot be accessed You have deleted/cannot access your email with your unique URL for DN registration, and have not registered your DN.</p>	<p>You will need to arrange to have the email resent. To do this, in the first instance you should inform a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor if you have one or the service desk.</p>
<p>Email on a different computer You cannot access your email, with your unique URL for DN registration, on the computer that you are going to use to access the web channel.</p>	<p>It is recommended that the email is available on the same computer as the one you will use to access the web channel (which must have a smartcard reader and related software installed). If this is not possible:</p> <ul style="list-style-type: none"> • Copy the URL from the email and paste it into a document (eg Microsoft Word, Notepad). • Save the document containing the URL to a disk. • Open the document on the computer with the web channel access. • Copy the URL from the document and paste it into your web browser. • Press <i>Enter/Return</i> key on your keyboard to go to the link.
<p>URL does not work Your web browser returns an error saying the page cannot be found when you try use your unique URL for registering your DN.</p>	<p>You should ensure that you are properly connected to the internet (or Voca extranet, if this is used). If the URL has been copied, or cut and pasted, ensure the correct URL is in the address bar or your browser. If this URL still does not work, contact the Voca service desk.</p>
<p>Name displayed is not correct After going to your unique URL, the name displayed on the first page is not yours.</p>	<p>You should check you are using the correct email (and correct URL). If you are, in the first instance contact a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor if you have one or the service desk. They must ensure your name and email address are correct on the web channel. If they are, they should contact the service desk.</p>
<p>Technical error During DN registration, the web channel returns a “technical error”.</p>	<p>You should reattempt the action using the same URL.</p>
<p>“Try again later” message During DN registration, the web channel returns a “try again later” message.</p>	<p>You should reattempt the action using the same URL.</p>
<p>Failure message You attempt to register your DN. The web channel returns a “Digital certificate – registration failure” message.</p>	<p>You should reattempt the action using the same URL. If it still does not work, you should contact a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor if you have one or the service desk.</p>

Issue and description	Action
First log on issues	
Failure message You attempt to log on for the first time and the web channel returns a failure message.	You should reattempt the action. If it still does not work, you should contact a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor, if you have one, or the service desk.
No welcome email Your welcome email has not arrived.	Contact a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor, if you have one, or the service desk.
Smartcard and/or PIN issues	
PIN forgotten You have forgotten your PIN.	You must inform your card issuer immediately.
Incorrect PIN entered You have entered an incorrect PIN. Your signing software has returned an error saying the PIN was incorrectly entered.	You must enter your PIN again.
Incorrect PIN entered repeatedly You have entered the wrong PIN consecutively and the card has become locked. Your signing software returned a message saying a PIN had been entered incorrectly, but there may not have been a message saying the card is locked.	You must inform your card issuer immediately. You may have to be issued with a replacement card and/or PIN. You may have to be reinstated over the web channel (your PKI status may be “Suspended” or “Suspended – pending”) before you can use your new smartcard/PIN. <i>Note: The number of times the PIN needs to be entered incorrectly before the card is locked depends on the card issuer.</i>
Card lost You have lost your smartcard.	You must inform your card issuer immediately. You will then be suspended for PKI until your new smartcard is available.
Card cannot be read Your smartcard cannot be read. This may be due to damage.	Try to identify any equipment problem by trying the card on another computer, if one is available. If the card still does not work, you must inform your card issuer immediately. You will be issued with a new smartcard.
Other smartcard issues	
New smartcard with new DN You have been issued with a new smartcard with a new DN.	You may have to register your new DN. If you do, you will receive an email containing a new unique URL to carry out the registration process. If you do not receive your email, contact a PSC who can maintain your details. If a PSC cannot maintain your details contact your sponsor, if you have one, or the service desk. If you need to initialise the smartcard, your card issuer will give you the details.
New smartcard You have been issued a new smartcard.	You will not have to carry out the DN registration process if your DN has not changed. If you were suspended for PKI, you will have to be reinstated for PKI. If you need to initialise the smartcard, your card issuer will give you the details.
Digital certificate expired You attempt to log on and the web channel returns a failure message.	You should contact your card issuer. You will be issued with a new smartcard. Your card issuer will advise you whether you have to initialise your smartcard, and whether your new smartcard has a new DN.

Issue and description	Action
Suspended for PKI security You have been suspended automatically for PKI. This can occur for a number of reasons, eg digital certificate invalid, digital certificate expired etc.	You will need to be reinstated for PKI by a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor, if you have one, or the service desk. Any other issues must be resolved before you can log on again with your smartcard.
All other issues	You should contact your card issuer, a PSC who can maintain your details, your sponsor (if you have one) or the BACS service desk.

Security information & procedures – ASM

13 Security information: ASM

13.1 What is ASM security?

The “alternative security method” (ASM) uses a contact ID and password to provide security for electronic communications and data transfers. The contact ID and password are issued by payment services, and the password is then changed by the contact to one of their choice.

In this guide, “ASM” is used to refer to a contact using their contact ID and password to carry out the security processes described in this guide.

13.2 Using a contact ID and password with payment services

13.2.1 What ASM is used for

You can use your contact ID and password to do the following:

- Log on to the payment services web channel
- Authorise actions you have carried out on the BACS payment services web channel.

You will also be able to use your contact ID and password to perform specific activities you have been given the privilege(s) to do for the payment services and functions you can use.

13.2.2 What you need

If you have a been registered for ASM, you will need the following to use payment services:

- Contact ID
- Password.

To obtain your contact ID and password, you will need the following:

- A piece of security information, eg *Smith*
- A hint to your security information, eg *Mother's maiden name*
- Unique URL (web address) in an email from BACS payment services.

13.2.3 How ASM security works with payment services

If you have a contact ID and password, you can use these for logging on to BACS payment services and confirming actions on the web channel.

Logging on

To authenticate you as a contact, when you log on to the payment services web channel with your contact ID and password, you must enter your contact ID and password in the required fields. If the password you have entered is correct for that contact ID you will be logged on to the web channel.

Confirming an action

To confirm an action on the payment services web channel using your contact ID and password, you will have to carry out the same process as that described for logging on.

14 Security procedures: ASM

14.1 Overview

Before you can use ASM to log on to the payment services web channel you will need to retrieve your contact ID and password. This is done using the web channel. The following sections detail how to retrieve your contact ID and password, and then how to log on to the payment services web channel and perform activities and functions on the web channel.

14.2 Contact ID and password activation activities

14.2.1 Overview

Before you can use ASM to access payment services you must carry out the following activities:

- Retrieve your contact ID and temporary password, using your unique web address
- Log on for the first time
- Change your password.

The following diagram provides an overview of these activities.

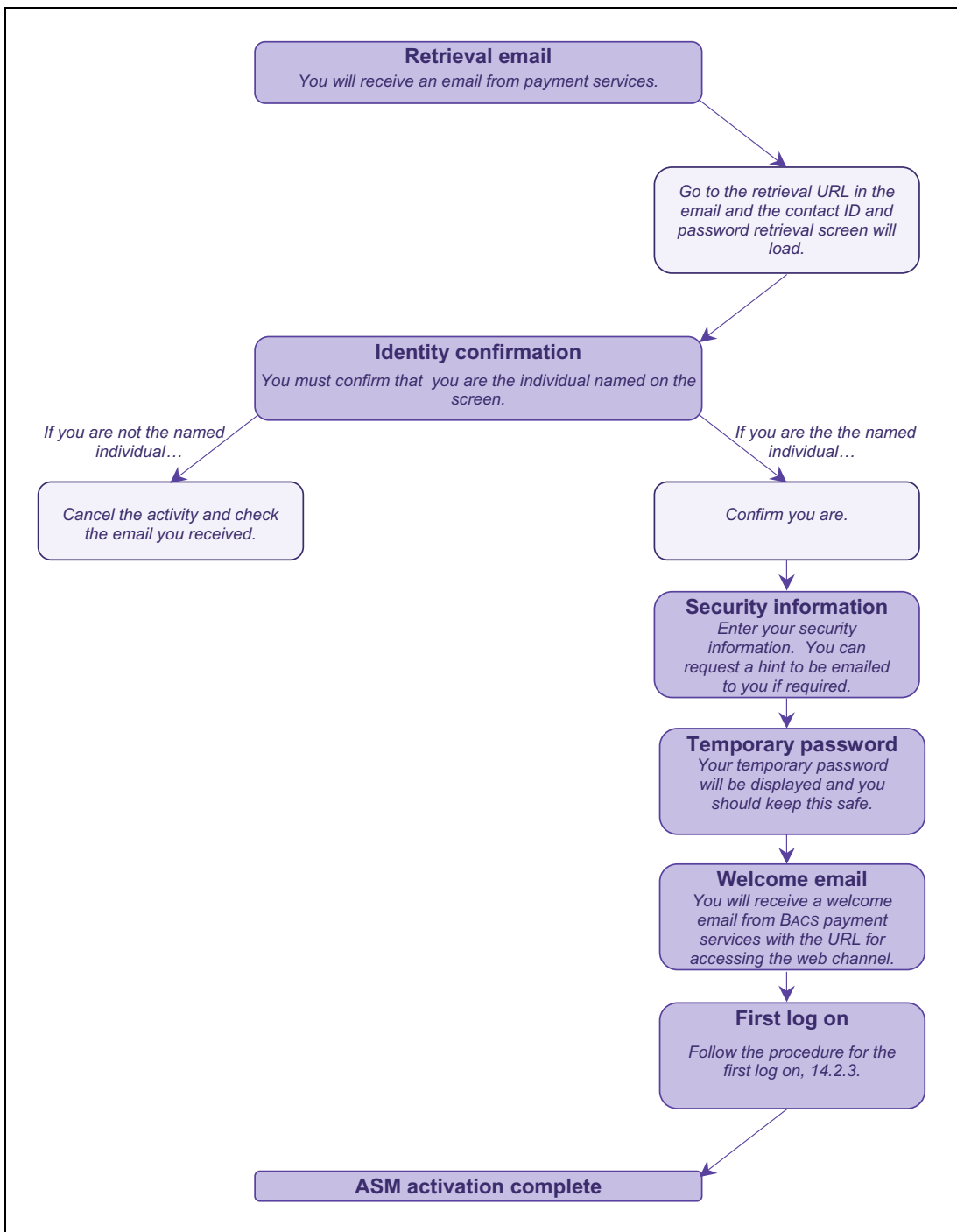


Figure 6: Overview of the ASM retrieval process

You can find more information about each of these activities in the following sections.

When you are set up with ASM security, to access payment services, a piece of security information and a hint for that information is registered for you. This could be for example:

Security information *Smith*

Hint *Mother's maiden name*

When you retrieve your contact ID and temporary password you will need to enter your security information. This information is not case sensitive. If you cannot remember your security information, you can request to have the hint emailed to you before you try to retrieve your ASM details again.

Once you have carried out the above activities you can use your contact ID and password to access BACS payment services. If you wish to change your password you can do this over the web channel. For details on how to change your password see section 14.5.1, page 59.

If your password is ever reset by someone, which is different from you changing your password, you will receive a new retrieval email. You will have to use this to retrieve your new password, but your contact ID will remain the same. If your password is reset you will have to carry out all of the activation activities as described in the following sections.

14.2.2 Contact ID and password retrieval

To use ASM to access payment services, you must first retrieve your contact ID and a temporary password. To retrieve your contact ID and password you will receive an email from BACS payment services with a subject of “BACS Payment Services – Your contact ID and password”. This email will contain a unique URL (web address).

Your ASM retrieval email should be on, or easily transferred to, the computer that you will use to access the BACS payment services web channel. If this cannot be done, you can find instructions in the following procedure on how to copy the URL from the email to the computer that will be used to access the web channel.

If you accidentally delete your ASM retrieval email you can have it resent. To organise having it resent, contact a PSC who can maintain your details or, if you have a relationship with a sponsoring bank, contact your sponsor or the service desk.

Note: Do not attempt to carry out the following procedure if you do not have your email containing your contact ID and password retrieval URL and your security information. If you have forgotten your security information, you can elect to have the hint emailed to you. How to do this is explained in the following email. If you still cannot remember your security information even with the hint, a PSC who can maintain your details, your sponsor, if you have one, or the service desk change your security information and hint for you.



To retrieve your contact ID and password

You must have your ASM retrieval email and you must know your security information.

1 Establish a connection to the internet (or Voca extranet).

Connect to the internet, or the Voca extranet if this will be used to access the web channel.

2 Go to your security retrieval URL.

Open the email “BACS Payment Services – Your contact ID and password” and click on the URL (web address). Your web browser will open and the *Contact ID and password registration* screen will load.

Alternatively, copy the retrieval URL from the email, open a web browser and paste the URL into the address bar. Press the *Enter/Return* key on your keyboard.

If your retrieval email is on a different computer, than that used to access the web channel, and it cannot easily be transferred, copy the URL from the email and paste it into a Microsoft Word, Notepad or other document and save it to a disk. Open this document on the computer that will be used to access the web channel. Copy the URL from the document and paste it into your web browsers address bar. Press the *Enter/Return* key on your keyboard.

To retrieve your contact ID and password (continued)

3 Confirm your name.

The *Contact ID and password registration* screen displays the contact name associated with the URL in the *Confirmation* block.

If this is your name, click *confirm*.

If this is not your name, check that you have used the correct email. If you are using the correct email and your name is incorrect, contact a PSC who can maintain your details. The PSC should check your details on the web channel.

4 Enter your security information.

A new screen will load. You must enter your security information. Your security information is *not* case sensitive and when you type it, it will appear on screen as asterisks (*). Click *confirm*.

If you cannot remember your security information, you can have the hint emailed to you. To do this, click the *sent hint* button. You will then receive an email from BACS payment services which includes the hint to your security information. Once this email arrives you should restart this procedure.

5 Make a note of your contact ID and temporary password.

If you entered your security information correctly, the screen will reload with your contact ID and temporary password displayed. You must make a note of these carefully. Your temporary password is case sensitive but will only contain capital letters and numbers.

KEEP YOUR CONTACT ID AND TEMPORARY PASSWORD SECURE until your welcome email arrives.

Your ASM status will now be set to "Active" but you must now wait until you receive your welcome email before logging on to the payment services web channel for the first time. Keep your contact ID and temporary password securely.

14.2.3 Welcome email and first log on

When you have retrieved your contact ID and temporary password you will receive a “Welcome to BACS Payment Services” email. Your welcome email contains the web address you should use for accessing the web channel with your ASM details.

First log on

You can now carry out the procedure for logging on to the web channel for the first time. The following procedure details how to log on for the first time, how to change your temporary password, and how to create a shortcut to payment services for ease of logging on.



To log on for the first time with ASM

You must have your welcome email, your contact ID and password.

1 **Establish a connection to the internet (or extranet).**

Connect to the internet, or the extranet if this will be used to access the web channel.

2 **Go to your welcome URL.**

Open the email “Welcome to BACS Payment Services” and click on the URL (web address). Your web browser will open and the *Log on* screen will load. Alternatively, copy the welcome URL from the email, open a web browser and paste the URL into the address bar. Press the *Enter/Return* key on your keyboard.

If your email is on a different computer, than that used to access the web channel, and it cannot easily be transferred, you can write the URL down and type it into your web browser’s address bar. Press the *Enter/Return* key on your keyboard.

3 **Create a shortcut to the web address.**

The *Log on* screen loads. If you do not have a smartcard reader installed on your computer, press *Ctrl + D*. This will create a shortcut to BACS payment services that can be accessed through the *Favourites* menu of Internet Explorer and the *Bookmarks* menu of Netscape Navigator. If you have a smartcard reader installed on your computer your signing software will open. Click your mouse on the web browser window. This will ensure that it is the web browser window that is active, and not the signing software. The signing software will stay open in front of the web browser, but will be the inactive window. press *Ctrl + D*. This will create a shortcut to BACS payment services that can be accessed through the *Favourites* menu of Internet Explorer and the *Bookmarks* menu of Netscape Navigator. Now close the signing software window.

Note: If there is a shortcut to BACS payment services on your computer already you can use that rather than the URL in your email, and you do not have to create a new shortcut.

To log on for the first time with ASM (continued)**4 Enter your contact ID and password.**

Type your contact ID and temporary password into the correct fields. Note that your contact ID and password are case sensitive.

Click the *log on* button. This process will authenticate you to the web channel.

5 Password change screen loads. Change your password.

Type your temporary password into the correct field. Then enter your new password into the correct fields. You will have to enter your new password twice. This is also case sensitive. For details of the required format for passwords see section 14.5.2, page 60.

Click *done* to change your password.

6 BACS payment services web channel homepage loads.

If the password change process was successful, the web channel homepage will load into your browser, and your name will appear in the contact identification area of the page (see section 6.4, page 19 for details of the screen areas).

You can now use your contact ID and password to carry out activities and functions on the web channel.

14.3 Logging on

After you have completed the first log on procedure you can use your contact ID and password to log on to the payment services web channel and perform the functions that you have been given the privileges to do that can be done with ASM security. The following sections describe how to use your contact ID and password to log on to the web channel, which involves authenticating yourself to the web channel.



To log on to the web channel with ASM (after first log on)

You must have carried out the first log on procedure for ASM.

1 Establish a connection to the internet (or extranet).

Connect to the internet, or the extranet if this will be used to access the web channel.

2 Open your web browser.

If you already have a browser open, you should close it and open a new browser window.

3 Go to your BACS payment services web channel shortcut.

If your browser is Internet Explorer, click on the *Favourites* menu and choose BACS payment services from the drop down list.

If your browser is Netscape Navigator, click on the *Bookmarks* menu and choose BACS payment services from the drop down list.

The *Log on* screen will load.

4 Enter your contact ID and password.

When the *Log on* screen loads, if you have a smartcard reader installed on your computer your smartcard signing software will load. If you wish to continue logging on with your contact ID and password, close the signing software.

To log on with your contact ID and password, enter your contact ID and password (both are case sensitive) into the correct fields and click the *log on* button. This process will authenticate you to the web channel.

5 BACS payment services web channel homepage loads.

If the authentication process was successful, the web channel homepage will load into your browser, and your name will appear in the contact identification area of the page (see section 6.4, page 19 for details of the screen areas).

If the authentication process was unsuccessful an error message will appear on the screen and you should try again.



Note: If you log on to the web channel and you do not perform any activity on the web channel (the session is idle) for 10 minutes, the session will time out. You will have to reauthenticate yourself before you can perform any more activities on the web channel. To reauthenticate yourself, carry out the log on procedure from step 4 onwards.

If you repeatedly enter your password incorrectly, you will become suspended for ASM. You should contact a PSC who can maintain your details or your sponsor, if you have one. If you know your password, they will be able to reinstate you for ASM and you can continue using your password. If you have forgotten your password it will they will need to reset it for you as well as reinstating you. If your password is reset you will have to carry out the procedure detailed in section 14.2.2, page 52.

If you password becomes compromised you must immediately contact Bacs or your sponsor, if you have one.

14.4 Actioning changes

When you change or add/delete information on the web channel, you will be asked to confirm that you wish to make the change(s). You must confirm the changes using the security method you logged on to the web channel with. The following procedure details how to confirm changes using your contact ID and password. For more information on how to confirm changes with PKI credentials, see section 9.4, page 40.



To action changes using ASM

You must have logged on using your ASM details and made changes on the web channel.

1 Review a summary of your changes and accept them.

A summary screen is displayed detailing the changes you are making. If the summary is correct, click *confirm* to start the process of actioning the changes.

2 Authorise the changes by signing the text displayed.

A confirmation screen will be displayed where you authorise the changes by entering your security credentials. If you logged on to the web channel with your contact ID and password, and are therefore authorising the changes with your ASM details, you must enter your password. Enter your ASM details in the correct fields.

If the changes were made successfully, a *Success* screen will load. In some circumstances, eg your browser crashing, you may not see the success screen. Should this occur, you should check whether the changes you input have been applied.

If at any point, before entering your password, you decide that you do not want to make the change(s) click the *cancel* or *back* action buttons on the screen. Depending on the stage you are at you make be taken to:

- A screen asking “Are you sure” you want to cancel the activity
 - Click *yes* to lose any changes that have not been confirmed, or
 - Click *no* to go back to confirm the changes or make further changes
- A maintenance screen where you can
 - Make further changes, or
 - Click *cancel* to be taken to the cancel activity screen (see first bullet point).



Note: Following many changes actioned on the payment services web channel, email notifications are sent by BACS payment services to the PSCs associated with the contact making the changes. The email notifications detail what was changed, who made the change(s) etc.

14.5 Your password

14.5.1 Changing your password

The following section describes how to change your password for logging on to the web channel with ASM security. When choosing a new password, choose something that others will not be able to guess. For example, do not use your name and date of birth. If you forget your password you should contact a PSC who can maintain your details, your sponsor (if you have one) or the service desk to have your password reset.



Note: If your password has been compromised you must immediately contact the service desk or your sponsor, if you have one. See section 14.5.3, page 60 for more information.



To change your password

You must have logged in to the web channel and you can view the menu.

1 *Select **My details** from the menu.*

Click on the *My details* menu option to load the *My details* screen.

2 *Click the **change password** button.*

The *My details* screen loads. Click the *change password* button.

3 ***Change password** screen loads. Enter your current and new passwords.*

In the *Change password* block there are three fields (existing password, new password and re-enter new password).

- Enter you current password into the first field
- Enter what you would like to be your new password in the second field (for details of the format for passwords see section 14.5.2, page 60)
- Enter you new password again into the third field
- Click *OK* to change your password.
- If successful, go to step 4. If unsuccessful, carry out this step again to change your password.

If you decide that you do not want to change your password click *back* instead of clicking *OK*.

To change your password (continued)

- 4 *My details* screen loads and your password has been changed. Click *confirm* or *cancel* or select a new menu option.

If required you can make other changes to your details (see section 17.2, page 66). Otherwise click *cancel* or select a new menu option.

Note: After changing your password, if you click confirm from the My details screen, the actioning sequence runs. If you logged on with your contact ID and password you must use your NEW password to authorise the changes.

14.5.2 Password specifications and guidelines

The password for ASM is case sensitive. When selecting a new password it should meet the following specifications:

Specification	Example
Password must be at least seven characters in length	
Password must contain at least two numeric characters	incorrect <i>december31</i> correct <i>dec3mber1</i>
The numeric characters must not all be at the start and/or end of the password	
Password must not contain two consecutive identical characters	incorrect <i>logg1ng7</i> correct <i>log3ing1</i>
Password must not be the same as any of the past 12 passwords used	
Password must not be the same as your contact ID	

14.5.3 Protecting your password

You must ensure that your password is something you will remember, and you must always keep it safe. Do not write your password down.

If you think that your password has been compromised, you must immediately contact the service desk or your sponsor, if you have one. You must not then log in until the service desk or your sponsor has advised you that you can. Your password will need to be reset before you can log on again and this will involve you retrieving a new password (see section 14.2.2, page 52).

14.5.4 Changing your security information and hint

If you need to change your security information and hint, you must contact a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor if you have one, or the service desk.

15 Issues with your ASM security

This section details the possible issues that you may experience with your ASM security, and actions you can take to overcome them.

Issue and description	Action
Contact ID and password retrieval issues	
<p>Email deleted/cannot be accessed You have deleted/cannot access your email with your unique URL for ASM retrieval, and have not retrieved your ASM details.</p>	<p>You will need to arrange having the email resent. To do this, you should inform a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor, if you have one, or the service desk.</p>
<p>Email on a different computer You cannot access your email, with your unique URL for ASM retrieval, on the computer that you are going to use to access the web channel.</p>	<p>If it is recommended that the email is available on the same computer as the one you will use to access the web channel (which must have a smartcard reader and related software installed). If this is not possible:</p> <ul style="list-style-type: none"> • Copy the URL from the email and paste it into a document (eg Microsoft Word, Notepad). • Save the document containing the URL to a disk. • Open the document on the computer with the web channel access. • Copy the URL from the document and paste it into your web browser. • Press <i>Enter/Return</i> key on your keyboard to go to the link. <p>Alternatively, you can write the URL down, and type it into your web browser address bar, and press <i>Enter</i>.</p>
<p>URL does not work Your web browser returns an error saying the page cannot be found when you try use your unique URL to retrieve your ASM details.</p>	<p>You should ensure that you are properly connected to the internet (or BACS extranet, if this is used). If the URL has been copied, or cut and pasted, ensure the correct URL is in the address bar or your browser. If this URL still does not work, contact the service desk.</p>
<p>Name displayed is not correct After going to your unique URL, the name displayed on the first page is not yours.</p>	<p>You should check you are using the correct email (and correct URL). If you are, contact a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor, if you have one, or the service desk. They should ensure your name and email address are correct on the web channel. If they are, they should contact the service desk.</p>
<p>Technical error During ASM retrieval, the web channel returns a “technical error”.</p>	<p>You should reattempt the action using the same URL.</p>
<p>“Try again later” message During ASM retrieval, the web channel returns a “try again later” message.</p>	<p>You should reattempt the action using the same URL.</p>
<p>Security information is not accepted You attempt to retrieve your ASM details. Your security information is not accepted by the web channel and an error is returned.</p>	<p>You should reattempt the action using the same URL. Ensure that you are using the correct case (the security information is case sensitive). If you have forgotten your security information, you can have the hint emailed to you (see section 14.2.2, page 52). If you attempt the retrieval three times without success, your password will need to be reset by a PSC who can maintain your details. If a PSC cannot maintain your details, you should contact your sponsor, if you have one, or the service desk.</p>

Issue and description	Action
Password issues	
<p>Password forgotten You cannot remember your password.</p>	<p>You should inform a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor, if you have one, or the service desk. They will be able to reset your password. You will receive a new email with a unique URL to retrieve your new password. If you have also forgotten your security information that is required for the retrieval you will have to have this reset as well.</p>
<p>Incorrect password entered You have entered an incorrect password. The web channel returned an error.</p>	<p>You must enter your password again. Check you are using the correct case (the field is case sensitive).</p>
<p>Incorrect password entered repeatedly You have entered the wrong password consecutively and you are automatically suspended for ASM.</p>	<p>If you know your password, you should contact a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor (if you have one) or the service desk to get reinstated. If you have forgotten your password, they will have to reinstate you and reset your password. If you have also forgotten your security information they will have to reset your security information and hint reset.</p>
<p>Password has been compromised You know or think that someone else knows your password.</p>	<p>You must contact the service desk or your sponsor, if you have one, immediately. Your password should be reset.</p>

16 ASM statuses

If you have been set up for ASM security, you will have an ASM security status. To use your contact ID and password, you will need to have an ASM status of “Active”. There are other possible statuses that you could have. The following table details the possible statuses that you may have for ASM security, and what it means if you have that status.

Status	What it means
Not set	You have not been set up to have ASM details for accessing BACS payment services.
Active	You can use your contact ID and password for everything you have been set up to do that can be accessed with ASM.
ASM pending	You have not yet retrieved your contact ID and password. For details of how to retrieve your contact ID and password see section 14.2.2, page 52.
Suspended	<p>You cannot log on or perform any action using your contact ID and password.</p> <p>The status of “Suspended” may have been automatically generated by the BACS payment services system following an incident, or may have been set by your sponsor (if you have one) or a PSC who can amend your details, through the process of suspending a contact.</p> <p>If you also have a smartcard, providing your PKI status is “active”, you can continue to carry out everything you have been set up to do using your smartcard.</p> <p>If you only have ASM security, or if your PKI status is also “Suspended”, you will no longer receive any notification emails.</p>
Suspended - Pending	<p>As for “Suspended”, you cannot log on or perform any action using your contact ID and password. You were in a state of “ASM pending” before you were suspended, and, if you are reinstated, your status will revert to “ASM Pending”.</p> <p>If you also have PKI credentials, providing your PKI status is “Active”, you can continue to carry out everything you have been set up to do using your smartcard.</p> <p>If you only have ASM security, or if your PKI status is also “Suspended”, you will no longer receive any notification emails.</p>

Part VI

Your details

17 Changing your details

17.1 Overview

As a contact, certain information is registered on the payment services web channel about you. This information is used in relation to your use of the payment services and includes contact information, privileges, and security information.

You can view some of this information, and change some of it. The following sections detail the information that is held about you, what that information is used for and how you can change some of that information.

17.2 How to change your details

The following procedure details how to change your contact details and your security information and hint (if you have ASM security).



To view and amend your details

You must have logged in to the web channel (with PKI or ASM) and you can view the menu.

1 Click *My details* in the left hand menu. *My details* screen loads.

The *My details* screen loads showing *Contact details* and *Privileges*.

The *Contact details* block contains, amongst other things, the following information:

- Title, first name and surname
- Security method, PKI status and ASM status
- Type
- Email address
- Office telephone number and additional information
- Out of office telephone number
- Mobile telephone number and additional information
- Fax number
- If you have ASM, there will also be a *change password* button.

The *Privileges* block(s) show the privilege groups you have been allocated.

Having viewed the information, if you wish to exit this screen, click the *cancel* button. You will be asked if you want to abandon this activity. Click *yes* to exit the contact details section.

To change any of this information go to step 2.

2 Make the required changes

To change you contact information (email address, telephone number etc):

- Highlight the information in the field you want to change
- Type the new contact information in the field
- Make further alterations (see below) or go to step 3.

To view and amend your details (continued)

To change your password (applicable to contacts with ASM):

- Click the *change password* button
- The *Change password* screen loads
- Enter your current password
- Enter what you would like as your new password in the two separate fields. For more information on the required format for your password see sec 14.5.2, pg 60
- Click *OK*
- *My details* screen reloads and your password has been changed
- Make further alterations (see below) or go to step 3.

3 Confirm your changes

Once you have made your changes, click *submit*. Go to step 4.

If you do not want to make any changes, or you want to lose the changes you have made, or all you have changed is your password (which took immediate effect), click *cancel*. You will then be asked if you wish to abandon the activity.

4 A summary screen loads. Check the details and, if correct, click *confirm*

A summary screen loads displaying the details that will be applied. If these are correct, click *confirm*. Go to step 5.

If they are not correct, or you wish to make further changes, click *back* to return to the *My details* screen and go back to step 2.

5 Confirmation screen loads. Authenticate yourself to make the changes.

In order to action the changes, you must authenticate yourself using the same security method you used to log on to the web channel.

If you logged on using your smartcard you must sign the text, that details the changes you are making, using your signing software.

If you logged on using your contact ID and password, enter your password and click *submit*.
Note: if you changed your password during this procedure you must use your new password.

6 Success screen loads.

If the changes were made successfully, the *Success* screen loads.

Change history

Version	Date	Details
1.00	1 June 2005	Baseline release of this guide.
1.10	17 March 2006	Release incorporating information about system notices.

This document is designed to be printed double-sided, therefore some pages will be blank. An electronic version of this document is available in pdf format, which can be read using the free Acrobat Reader software (version 5.0 and above).

