# Bacs Payment Services

Contacts' Guide

**Version** 2.40 | 16/12/2024

**Reference** MNSI21095 (PN5000)

# Contents

pay.uk

# Document information

## Version history

Detailed changes in this version since version 2.3:

| Section | Description |
|---------|-------------|
| Version history | Amended the service desk email from servicedesk@BacsServices.co.uk to service.desk@BacsServices.co.uk |

Full version history:

| Version | Date | Description |
|---------|------|-------------|
| 1.00 | 1 June 2005 | Baseline release of this guide. |
| 1.10 | 17 March 2006 | Release incorporating information about system notices. |
| 1.20 | 17 July 2007 | Updated guide with new Bacs branding. |
| 1.30 | 11 April 2014 | Minor updates to remove reference to specific email subject lines. Removed references to DSL Connect. |
| 1.40 | 10 November 2014 | Updated document branding. Removed outdated references to dial-up extranet. Updated screenshots of the payment services website to reflect rebrand. |
| 1.50 | 15 April 2015 | Update to include new procedure to reset your own password (section 3.5). The other ASM procedures have been amended to align them and simplify them. |
| 1.51 | 3 May 2016 | Sections 3.1, 3.3, 3.4, 3.5: Updated to indicate that the password criteria are available on the payment services website. Also updated the "Change my password" screen shots to include the "Password Rules" link. |
| 1.60 | 1 July 2016 | Baselined version. |
| 1.61 | 18 August 2016 | • Section 3.1.1: Added statement that when ASM contacts login to PSW for the first time following a password reset/change, they are asked to complete the security information and security hint details. <br>• Section 3.1.2: Changed password length from seven characters to eight characters. <br>• Section 3.4, 3.5: Added note that the password criteria display on the PSW and following the first password change/reset you will be asked to complete the security information and security hint details. |
| 1.70 | 26 September 2016 | Baselined version. |

| Version | Date | Description |
|---|---|---|
| 1.71 | 1 June 2018 | Sections 1.2.1, 1.2.6: Updated sections to indicate that Internet Explorer is the recommended web browser to enable access to the Bacs payment services website. |
| 1.80 | 25 June 2018 | Baselined version. |
| 1.81 | 14 July 2020 | Section 1.1.2: Updated sections to include that It is the responsibility of the service user to add and maintain additional contacts for their organisation and that service user contacts must not be managed by a Bureau |
| 1.90 | 29 July 2020 | Baselined version. |
| 1.91 | 1 November 2021 | Re-branded document as per latest Pay.UK guidelines. Updated terminology throughout the guide as follows: <br>• Changed "bank" to payment service provider (PSP)". |
| 2.0 | 12 November 2021 | Baselined version. |
| 2.01 | 1 February 2022 | • Sections 1.1.1, 1.2.1, 1.2.6: Updated list of supported web browsers and signing solutions. <br>• Section 2.2.6: Added note on the signing software that will be available depending on the web browser used. |
| 2.1 | 4 March 2022 | Baselined version. |
| 2.11 | 8 March 2022 | • Sections 1.1.1, 1.2, 1.2.9, 1.3, 1.9, 1.10, 2.2.6, 2.2.7, 3.2, 3.3, 3.5, 3.6, 4: Existing sections updated to reflect the new payment services website. <br>• Sections 1.3.1, 1.4.1, 1.4.2, 1.4.3, 1.10.1, 1.11, 3.4: New sections added to reflect the new payment services website. |
| 2.2 | 1 April 2022 | Baselined version. |
| 2.21 | 20 September 2023 | Section 3.1.2: Updated section "Password expiry" to include that passwords expire after a configured period of 90 days. |
| 2.30 | 6 October 2023 | Baselined version. |
| 2.31 | 16 December 2024 | Version history <br>• Amended the service desk email from servicedesk@BacsServices.co.uk to service.desk@BacsServices.co.uk |
| 2.40 | 16 December 2024 | Baselined version. |

## Copyright statement

pay.uk

# 1  Payment services website overview

## 1.1  What is a contact?

A contact is an individual who has been registered to use payment services. Contacts are also the entities set up to use the Bacstel-IP service and to submit and collect data over the ETS and STS services.

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

- Security methods
- Contact type
- Privilege groups
- Communication information

### 1.1.1  Security methods

To access the payment services website, 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 website:

- Public Key Infrastructure (PKI): using a smartcard and PIN
- Alternative Security Method (ASM): using a contact ID and password

As a contact, you must have at least one of these security methods. Fewer privileges are usually given to contacts who have ASM security. If you have both PKI and ASM you can log on using either. However, if you log in with ASM, you may not be able to carry out all the functions you have been given PKI privileges for.

SEE ALSO

### 1.1.2  Contact types

There are two types of contact:

- Primary Security Contacts (PSCs)
- Additional Contacts (ACs)

Some privileges are only available to PSCs. The decision as to whether you are a PSC or an additional contact depends on the role you have when using the payment services website. The functions a PSC or an additional contact can perform depend on the privileges they are given.

pay.uk

It is the responsibility of the service user to add and maintain additional contacts for their organisation.

**NOTE:** *Service user contacts must not be managed by a Bureau.*

### 1.1.3  Privileges

Contacts are given privileges that allow them to perform certain activities. Some privileges can only be given to contacts with PKI security and/or to contacts that are PSCs. Privileges are assigned to you when you are first set up as a contact; they can be changed. You cannot maintain your own privileges.

For information on the available privileges, refer to the guides you have received for the services you have been set up to use.

### 1.1.4  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

SEE ALSO

## 1.2   What is the payment services website?

As a registered contact for the payment services website you can use your security methods to log in to the payment services website. The payment services website provides you with access to the services that you have been set up to use and enables you to carry out the actions you have been given the privileges for.

The following image shows an example of the payment services website *Dashboard* that displays when you have logged in.

Figure 1.   An example of the payment services website Dashboard
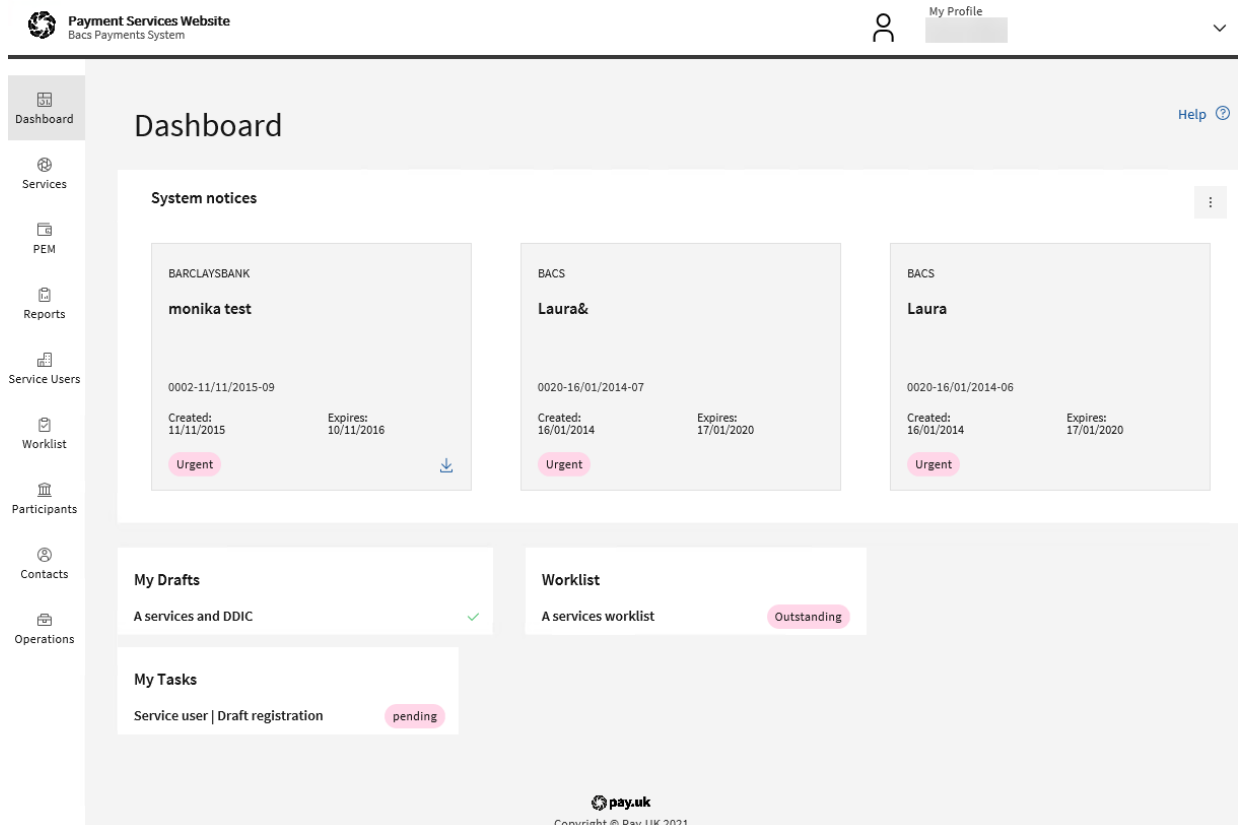
## 1.3 Connections

To connect to the payment services website you need the following:

- A compatible web browser

- A connection method (normally the Internet, but can also be an extranet connection)

- A security method

SEE ALSO

[“Connection methods” on page 12](#)

### 1.3.1 Compatible web browsers

To access the payment services website, use any of the following browsers:

- Internet Explorer 11

  **NOTE:**  *Support for Internet Explorer 11 will be removed from June 2022.*

- Chrome

- Edge

- Firefox

- Safari

**NOTE:**  *The Thales Gemalto eSigner PKI signing solution only runs on Internet Explorer. The Thales Gemalto Websigner PKI signing solution should be used for all non-Internet Explorer browsers.*

## 1.4 Security

You can log in to the payment services website using PKI or ASM. If you have both PKI and ASM you can log in using either, however, if you log in 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 guides you have received regarding the services you have been set up to use.

### 1.4.1 Security method statuses

Each security method you have assigned to you has a status, for example "active", "suspended". Depending on the status of the security method, you can use that security method to log in to the payment services website and perform actions you have been assigned the privileges to do.

### 1.4.2 Authorising actions

When you carry out actions on the payment services website you must authorise the actions. For details on how to confirm actions see “Action changes using PKI” on page 25. You must confirm actions using the same security method that you used to log in to the payment services website.

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

### 1.4.3   Timeouts

For security purposes, when you are logged in to the payment services website and are inactive for eight minutes, a timeout countdown displays.
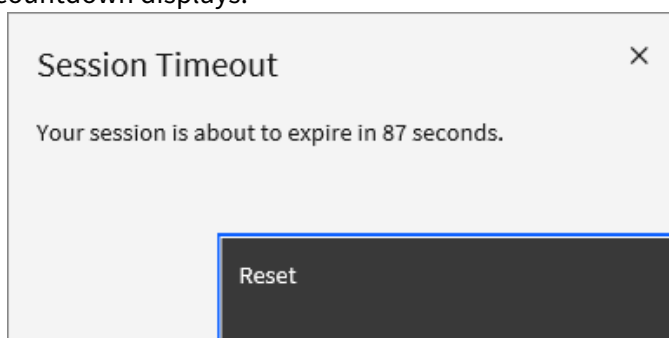


If after a further two minutes no activity is detected, the session times out, any unsaved work is lost, and you are logged out of the payment services website.

Use your smartcard and PIN or contact ID and password to log in again (the same method you used to originally log in). Following successful log in, the *Dashboard* displays. You may need to re-enter any information that you entered before you were timed out.

## 1.5   Functionality

The payment services website can be used to access the various features of Bacs services that you have been set up to use. Additionally, all contacts can use the payment services website to view and amend their own communication details.

SEE ALSO

## 1.6   Notifications

Many of the actions that can be carried out on the payment services website, cause email notifications to be generated and sent to the 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 website that 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.

## 1.7   Availability

The payment services website 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 payment services website. Once you are logged on, you can perform the functions you are set up to do over the payment services website. For details of nonprocessing days see the processing calendar available from: http://www.bacs.co.uk/

## 1.8    Connection methods

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

### 1.8.1    Internet

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

### 1.8.2    Fixed Extranet

For more information on how to connect using the Vocalink Fixed Extranet visit: www.vocalink.com

## 1.9    Navigating the payment services website

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

Most screens have on-screen navigation buttons that can be used for going "back" and for cancelling actions. You must not use the browser's own buttons when logged on to the payment services website as some pages may not load correctly.

There are four main menus on the payment services website:

- Global menu: displays on the left of the screen, and shows the main options.

- Local menu: display on selecting a global menu option, and show the available local options.

- Breadcrumb menu: displays a hyperlinked navigational history at the top of each screen.

- My Profile: provides links to your details, privileges, and sign out. Always available at the top of the page when you are logged in to the payment services website.

For further details, see *In-house Maintenance - Direct Participants' Guide Volume 2*.

## 1.10   System notices

System notices provide you with service and operational information for some services accessed on the payment services website. If a system notice has been marked as urgent, it displays on the **Dashboard**. To view it, click the title and the *View system notice* screen displays the full system notice.

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 opens in another window. Acrobat Reader is required to view this.

To view non-urgent system notices, see section "Access system notices" on page 14.

### 1.10.1 Access system notices

System notices that are not marked as urgent, must be manually searched for by a contact. Urgent system notices can be accessed by clicking on the link on the homepage (urgent system notices can also be searched for using this procedure).

PREREQUISITE

You must be logged in to the payment services website with PKI or ASM.

STEPS

1. From the global menu, click **Dashboard**, if the Dashboard is not already displayed.

2. Click the three vertical dots beneath the **Help** icon on the top right of the screen.

3. Select **View more system notices** from the three vertical dots menu.
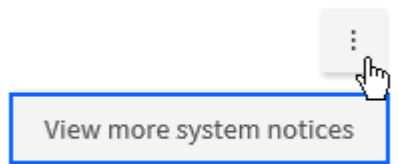


STEP RESULT

The *System notices* screen displays.

4. Click a system notice that already displays or filter the list.

   You can filter the list by:
   - **Sequence number**: as you enter the first few digits of the sequence number, the system notices are filtered to match.
   - **Status**: all statuses are selected by default. Click **x** to clear all selected statuses.
     Select from the **Status** drop-down list - approved, draft, deleted or pending.
   - **Effective from** and/or **Effective to** date: enter the dates or use the calendar picker.
     As you filter the list, the list of system notices automatically updates.

5. Click a system notice to select it.

STEP RESULT

The *View system notice* screen displays the full details of the notice including the recipients, the priority and the expiry date. If a PDF is attached, there will be a hyperlink that can be clicked on. The PDF will open in a new browser window; this can be saved.

## 1.11    Log out of the payment services website

PREREQUISITE

You must be logged in to the payment services website.

STEPS

1.  Open the **My Profile** menu at the top right of any screen.

    STEP RESULT

    *My Profile* menu displays.
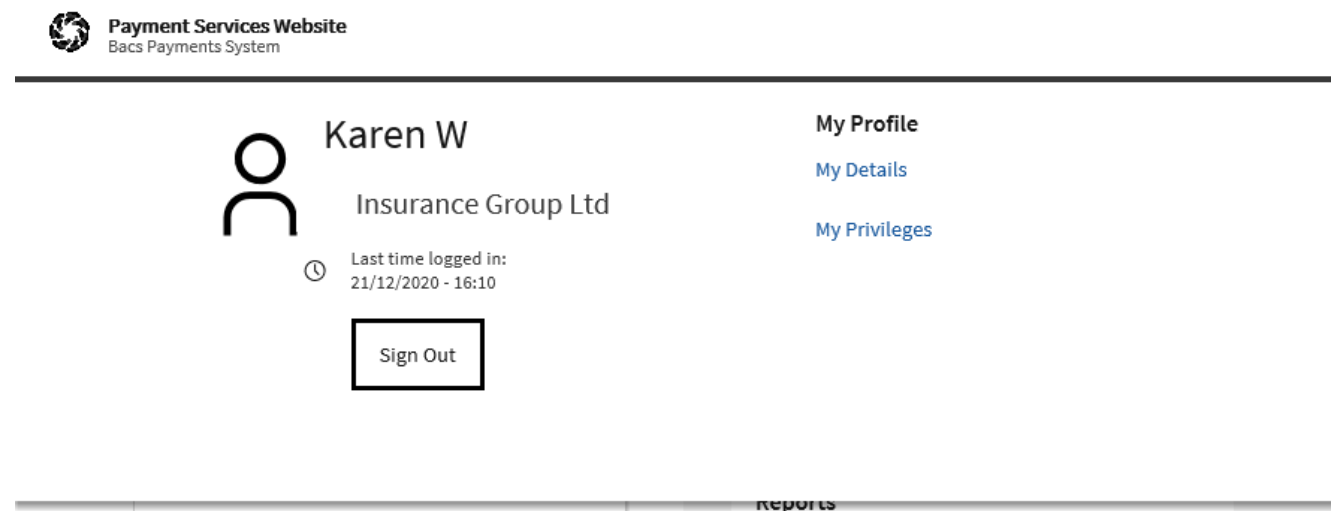


2.  Click **Sign Out**.

    When prompted "Are you sure you want to sign out?", click **Sign Out**.

    STEP RESULT

    Note that any unsaved changes will be lost when you sign out and cannot be recovered.

    The *Signed out* screen displays with a *Sign out successful* message at the top, and you are signed out of the payment services website.

# 2 PKI security information and procedures

## 2.1 Security information: PKI

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 on the payment services website for all registered PKI credentials. |

### 2.1.1    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 2.   A stylised diagram of a smartcard and PKI credentials
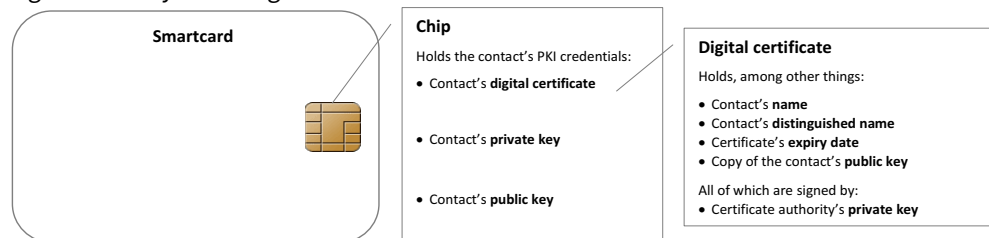


PKI credentials can also be held on a hardware security module (HSM). An HSM is used by companies who require a high volume of automated digital signing and verification.

### 2.1.2    Using PKI with the payment services website

**What PKI is used for**

You can use your PKI credentials to do the following:

- Log in to the payment services website.

- Confirm actions you have carried out on the payment services website.

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 website.

**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) – some software refers to a PIN as a passphrase

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.

**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 payment services website. The following describes how PKI security works with payment services.

**Logging in**

To authenticate you as a contact, when you log in to the payment services website with your PKI credentials, the payment services website 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 payment services website along with a copy of your digital certificate.

If the payment services website 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 payment services website was not able to verify with the certification authority that your digital certificate is still valid (that is, 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).

**Confirming an action**

To confirm an action on the payment services website using your PKI credentials, you will have to carry out a similar process as that described for logging on. However, instead of the payment services website 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.

## 2.2    Security procedures: PKI

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 website and perform activities and functions on the payment services website.

### 2.2.1    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 with 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.

### 2.2.2    Smartcard activation

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 3.  Overview of the smartcard activation process

```
                    ┌─────────────┐
                    │Initialisation│─────┐
                    └─────────────┘      │  If you have to initialise it
                                         │  (your card issuer will advise you)
                                         │
        If your smartcard is already     │
        initialised when you receive it  │      ┌──────────────┐
                                         │      │  Follow the   │
                                         │      │ instructions from│
                                         │      │ your card issuer│
                                         │      └──────────────┘
                    ┌─────────────┐
                    │DN Registration│
                    └─────────────┘
                                         ┌──────────────┐
                                         │ You receive a │
                                         │registration email.│
                                         │Follow registration│
                                         │  procedure    │
                                         └──────────────┘

                                         ┌──────────────┐
                                         │ System checks │
                                         │ performed. If │
                                         │ successful, your│
                                         │contact is set to PKI│
                                         │   Active      │
                                         └──────────────┘

        ┌──────────────┐                 ┌──────────────┐
        │ You receive a │                 │ You receive a │
        │ Welcome Email │                 │ Welcome Email │
        │(with the URL to log│            │(with the URL to log│
        │     on)       │                 │     on)       │
        └──────────────┘                 └──────────────┘

        ┌──────────────┐                 ┌──────────────┐
        │First log on. If│                │Follow first log on│
        │ successful, your│               │  procedure    │
        │contact is set to PKI│           └──────────────┘
        │   Active      │
        └──────────────┘

                    ┌─────────────┐
                    │  Smartcard   │
                    │activation complete│
                    └─────────────┘
```

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.

### 2.2.3 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.

### 2.2.4 DN registration

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

Your DN can be registered manually on the system or by an automatic process.

**Manual registration**

When a contact is set up, the DN associated to your digital certificate can be entered as part of the contact details. This means that you do not have to carry out the automated registration process. If your card supplier does register your DN manually, you will have a PKI status of "manual". For more information on statuses see "PKI statuses" on page 27.

If your DN is manually registered, then you receive a welcome email when your contact is registered.

Note: Manual registration is usually not used when you have a smartcard. Where PKI credentials are held on HSMs, this is the only DN registration process that is used.

**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 a smartcard registration email from the payment services website you must carry out this automated registration process.

Your smartcard registration email contains a unique URL (web address). These instructions should be used in conjunction with the following procedure.

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.

PREREQUISITE

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

STEPS

1. Go to your registration URL.

   Open the smartcard registration email and click on the URL (web address). Your web browser opens and the *Digital certificate registration* screen loads. (Alternatively, copy the registration URL from the email, open a web browser and paste the URL into the address bar and press **Return**.)

2. 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 payment services website.

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

   Your signing software automatically opens. 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.

4. A screen displays 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.

### 2.2.5    System checks

When your DN is registered on the system, additional system checks are carried out. When these checks are complete, and successful, your contact status will become "active". You will also receive a welcome email from the payment services website.

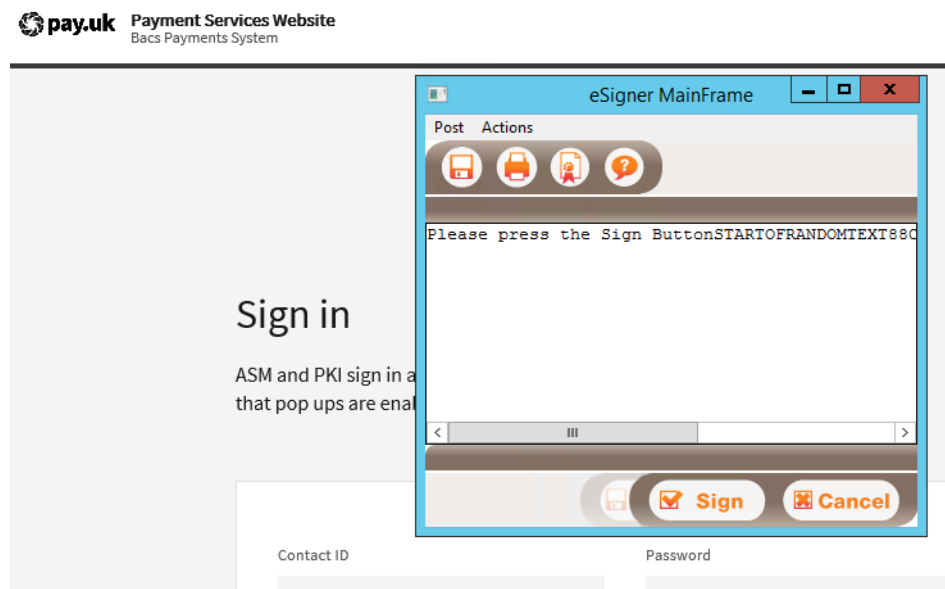### 2.2.6    Log in to the payment services website using PKI

PREREQUISITE

- You must have received your welcome email, and your PKI status must be 'Active' or 'Manual'.

STEPS

1. In a web browser go to paymentservices.bacs.co.uk

   STEP RESULT

   The payment services website displays and your signing software opens.



**NOTE:**  You signing software may look different. Note that Thales Gemalto eSigner PKI signing solution only runs on Internet Explorer. Thales Gemalto Websigner PKI signing solution should be used for all non-Internet Explorer browsers.

2. Sign the random text.

   Your signing software displays a random string of text to sign to enable authentication of you to the payment services website. Sign the text by doing the following:

   a)  Insert your smartcard into your reader (if it is not already inserted).
   b)  Click the **Sign** or **Sign and submit** button on your signing software.
   c)  Enter your PIN and click **OK.**

RESULT

The payment services website *Dashboard* displays.

If your PKI status was 'Manual', then it is updated to be 'Active' after you successfully log on using PKI.

> **NOTE:**
>
> - For security purposes, when you are logged in to the payment services website and are inactive for eight minutes, a timeout countdown displays. If after a further two minutes no activity is detected, the session times out, any unsaved work is lost, and you are logged out. You must log in again before you can perform any more activities on the payment services website. For further details, see "Timeouts" on page 11.
>
> - If you have saved a draft of your session (**Save as Draft**) before your session times out or you log out, you can retrieve the draft when you log in again under **My tasks** on the *Dashboard*.
>
>   ***Save as Draft*** is available for:
>
>   – Contact maintenance (all contact profile types)
>
>   – Service user registration
>
>   – Manual entry submissions for 'A' services (ARUDD, ARUCS, AWACS, ADDACS, AUDDIS returns) and DDIC, provided they are then submitted and approved by 22:25 the same day
>
>   – CASS (for example, accepting a switch with many Direct Debits and Credits)

### 2.2.7    Action changes using PKI

When you change or add or delete information on the payment services website, you are prompted to confirm the changes. You must confirm the changes using the security method you logged in to the payment services website with. The following procedure details how to confirm changes using your PKI credentials.

PREREQUISITE

You must have logged in using your PKI credentials and made changes on the payment services website.

STEPS

1. Review a summary of your changes and accept them.

   A *Summary* screen displays detailing the changes you are making.

   Home / My Profile / Summary

   ## Maintain contact summary
   Summary

   **Changes made**

   | | |
   |---|---|
   | Changes being made by | Karen West |
   | Acting on behalf of | |
   | First name | Karen |
   | Last name | West |
   | Date | 2021-11-15 |
   | Effective Date | 2021-11-16 |

   **Telephone details**

   | Field | Before | After | Change type |
   |---|---|---|---|
   | Telephone type | Mobile | | For Info |
   | Extra information | 99999999999999999999 | 999999999999999 | updated |

   Confirm

pay.uk

For each change:

- *Field* column: displays the field name
- *Before* column: displays each field before the change
- *After* column: displays the changes made
- *Change type* column: displays created, updated, or deleted, as appropriate

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 displays where you authorise the changes by entering your security credentials. If you logged in to the payment services website with your PKI credentials, and are therefore authorising the changes with your PKI credentials, your signing software loads, displaying text detailing the changes you are going to make.

3. Click **Sign**, enter your PIN and then click **OK** (or press **Enter**) to sign the text.

   You will "digitally sign" the text displayed, and hence sign the changes you are making.

   If before signing the text, you decide you do not want to make the changes click **Cancel** or the **x** button on your signing software to close it. The summary screen redisplays.

   You can return to a previous screen using the breadcrumb menu at the top. You can use the global menu on the left to return to the **Dashboard** or another screen, but you will lose any changes that have not been confirmed.

   STEP RESULT

   If the changes were made successfully, a *Success* screen displays.

   In some circumstances, for example, if your browser crashes, you may not see the success screen. If this happens, confirm that the changes you made have been applied.

   To make another change, like the one you just made click **Another** on the success banner.

   **NOTE:** *After several changes are actioned on the payment services website, email notifications are sent by the payment services website to the PSCs associated with the contact making the changes. The email notifications detail what was changed, who made the changes and so on.*

## 2.3    Protecting your smartcard and PIN

As your PIN is not known to anyone other that yourself, if you forget your PIN you must 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, and others will not allow you to change it at all. If you would like to change your PIN you should refer to the documentation that accompanied your signing software.

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.

## 2.4    PKI statuses

If you have been set up for PKI security, you have a PKI security 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 "DN registration" on page 21. |
| Suspended | You cannot log on or perform any action using your PKI credentials.<br><br>The status of "Suspended" may have been automatically generated by the payment services website following an incident (for example, you have logged in to the payment services website but your digital certificate has been revoked).<br><br>The status of "Suspended" may have been set by your card issuer, your sponsor (if you have one), Vocalink or a PSC who can amend your details, through the process of suspending a contact.<br><br>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.<br><br>If you only have PKI security, or if you ASM status is also "Suspended", you will no longer receive any notification emails. |

| Status | What it means |
|---|---|
| Suspended - Pending | As for "Suspended", you cannot log on or perform any action using your PKI credentials.<br><br>You were in a state of "PKI pending" before you were suspended, and, if you are reinstated, your status will revert to "Pending".<br><br>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.<br><br>If you only have PKI security, or if your ASM status is also "Suspended", you will no longer receive any notification emails. |
| Manual | Your DN has been manually registered on the system. Your status will automatically change to "Active" the first time you log in the payment services website 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". |

## 2.5   Issues with your PKI security

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

### 2.5.1   DN registration issues

| Issue and description | Action |
|---|---|
| **Email deleted/cannot be accessed**<br>You have deleted/cannot access your email with your unique URL for DN registration, and have not registered your DN. | 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. |
| **URL does not work**<br>You web browser returns an error saying the page cannot be found when you try use your unique URL for registering your DN. | You should ensure that you are properly connected to the internet (or Vocalink 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 Vocalink service desk. |
| **Name displayed is not correct**<br>After going to your unique URL, the name displayed on the first page is not yours. | 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 payment services website. If they are, they should contact the service desk. |
| **Technical error**<br>During DN registration, the payment services website returns a "technical error". | You should reattempt the action using the same URL. |

| Issue and description | Action |
|---|---|
| "Try again later" message<br>During DN registration, the payment services website returns a "try again later" message. | You should reattempt the action using the same URL. |
| Failure message<br>You attempt to register your DN. The payment services website returns a "Digital certificate – registration failure" message. | You must re-attempt the action using the same URL. If it still does not work, 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. |

### 2.5.2    First login issues

| Issue and description | Action |
|---|---|
| Failure message<br>You attempt to log on for the first time and the payment services website returns a failure message. | You must re-attempt the action. If it still does not work, 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. |
| No welcome email<br>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. |

### 2.5.3    Smartcard or PIN issues

| Issue and description | Action |
|---|---|
| PIN forgotten<br>You have forgotten your PIN. | You must inform your card issuer immediately. |
| Incorrect PIN entered<br>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<br>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 payment services website (your PKI status may be "Suspended" or "Suspended – pending") before you can use your new smartcard/PIN.<br>**NOTE:**  *The number of times the PIN must be entered incorrectly before the card is locked depends on the card issuer.* |
| Card lost<br>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. |

| Issue and description | Action |
|---|---|
| Card cannot be read<br>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. |

### 2.5.4  Other smartcard issues

| Issue and description | Action |
|---|---|
| New smartcard with new DN<br>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<br>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, your 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<br>You attempt to log on and the payment services website 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 must initialise your smartcard, and whether your new smartcard has a new DN. |
| Suspended for PKI security<br>You have been suspended automatically for PKI. This can occur for several reasons; for example, digital certificate invalid, digital certificate expired and so on. | You must 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 in 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. |

# 3   ASM security information and procedures

## 3.1   Security information: ASM

The 'alternative security method' (ASM) means that a contact can use a contact ID and password to access the payment services website.

A contact ID is generated when a contact is first registered; the contact ID cannot be changed.

The contact ID and a password is issued by the payment services website as part of a 'retrieval' process that a contact performs. The retrieved password is a temporary password that must be changed the first time a contact logs in.

When a contact is logged in to the payment services website using a contact ID and password, they can perform activities that they have the privilege to perform, provided the activity does not specifically require you to be logged on with a smartcard (PKI).

### 3.1.1   Password management

Contacts can reset their own password if they forget it. Contacts can also change their password at any time when they are logged onto the payment services website.

### 3.1.2   Password expiry

Passwords expire after a configured period of 90 days. If a contact logs in with an expired password, then they are made to change it before they are logged in.

Note that the password criteria are available on the following areas of the payment services website:

- ASM login password change screen (click link **Password Rules**)

- ASM first time login (click link **Password Rules**)

- ASM login following a password reset (click link **Password Rules**)

- My details screen when the change password option is selected (click **Help** at the top of the screen)

### 3.1.3   Security information and hint

Security information is used by contacts to retrieve their contact ID and password and to reset their password. A security hint provides a prompt to a contact as to what their security information is.

For example, if the security hint is "Mother's maiden name", then the security information is the answer (for example, "Smith").

Security information and the hint is added when a contact is registered with ASM security. The security information and hint can be changed by a contact that is able to maintain your details. You cannot change your own security information and hint.

NOTE: ASM contacts that were set up before August 2016, are prompted to complete the security information and security hint details, the first time they login to the payment services website following a password reset or change. This is not required for subsequent password changes.

In tasks that require you to enter your security information, you can request that the hint is emailed to you. Security information is not case sensitive.

### 3.1.4  Password requirements

Your password must meet a number of requirements. Ensure it is not something that people can easily guess. Your password is case sensitive.

When you select a password, it must:

- Be at least eight characters.

- Contain at least two numeric characters; these must not all be at the start and/or end of the password (correct: dec3ember1; incorrect: december31).

- Not contain two consecutive identical characters (correct: log3ing1; incorrect: logg1ng7).

- Not be the same as any of the past 12 passwords used.

- Not be the same as your contact ID.

### 3.1.5  Retrieving a contact ID and password

The first time a contact is set up to use ASM, their security information and hint are set up. The payment services website sends an email to the contact that enables the contact to retrieve their contact ID and password. The contact must then login and change that password.

Figure 4.   Process to get contact ID and password
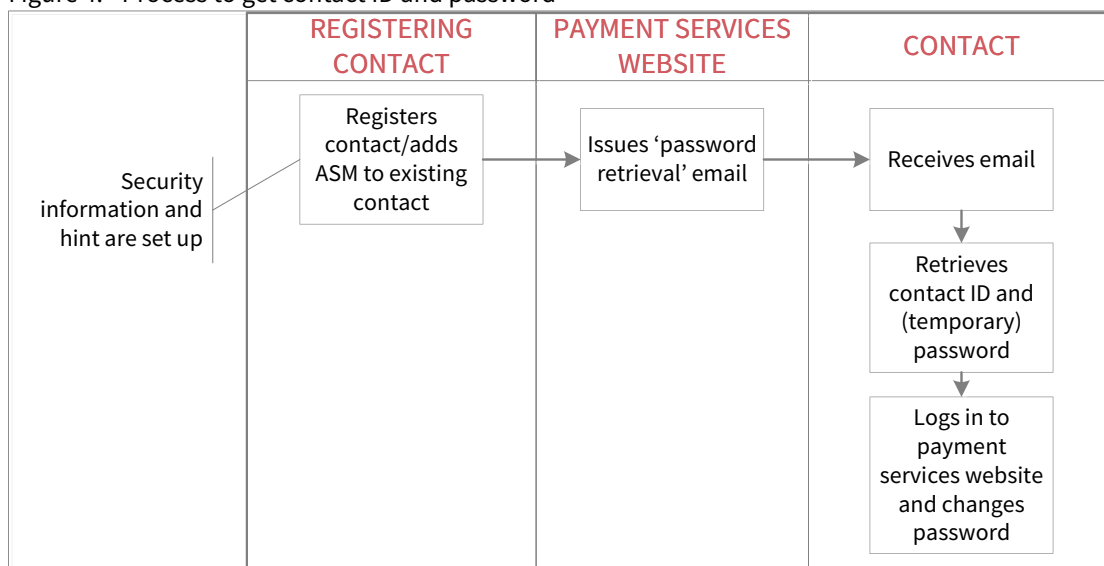
## 3.2 Retrieve your contact ID and password

The first time you are set up to use ASM and any time that your password is reset, you must retrieve your new password. To do this follow the link in the 'password retrieval' email that you receive, then enter your security information.

PREREQUISITE

- You must have your password retrieval email that contains a unique link to get your password.

  **NOTE:** If you have lost or deleted the email, then a PSC or the PSP that maintains your registration can resend it to you.

STEPS

1. Click the URL in the email.

   STEP RESULT

   The payment services website launches in your web browser displaying a *Confirmation* screen with your name.

   **NOTE:** If the *Contact ID and password registration* screen does not display, then copy the complete URL from the email and paste it into a browser address bar. Ensure you copy the full URL (it is usually on multiple lines).

2. Check your name and, if it is correct, click **Confirm**.

3. Enter your security information and click **Confirm**.

   This is not case sensitive.

   **NOTE:** If you have forgotten your security information, click the ***I've forgotten my security information*** link, and when prompted enter your contact ID. An email is then sent to you with the hint for your security information.

RESULT

Your contact ID and a temporary password display on screen and you receive a 'welcome' email. Your ASM status is set to 'Active'.

AFTER COMPLETING THIS TASK

You should change your password immediately.

Log in with your temporary password which you will be prompted to change.

## 3.3    Log in using a contact ID and password

PREREQUISITE

- Your ASM status must be 'Active' otherwise you cannot successfully log in.

This section describes how to log in to the payment services website with your contact ID and password.

If you forget your password, you must get it reset. It can be reset by a PSC (if you are an additional contact) or by your sponsor. Refer to section "Reset your password" on page 37.

STEPS

1.  In a web browser go to https://paymentservices.bacs.co.uk/online/newbacs/loginBrowser.do

    STEP RESULT



   **NOTE:**  If you have signing software installed, then it opens automatically. Close the signing software to log in using your contact ID and password.

2.  Enter your **Contact ID** and **Password**.

    Your password is case sensitive.

3.  Click **Sign in**.

    **NOTE:**  *If you repeatedly get your password wrong, then your ASM access becomes suspended. You must be re-instated before you can access the payment services website again using your contact ID and password.*

If your password has expired, or this is the first time you have logged in using a temporary password, then you are prompted to change your password.

Click **Password Rules** to view the password criteria and ensure your new password meets the requirements listed in section "Password requirements" on page 32.

4.  Enter your existing (temporary) password, then enter your new password twice.

5.  Click **OK**.

RESULT

The payment services website welcome screen displays.

AFTER COMPLETING THIS TASK

Log out after you have finished using the payment services website.

If you remain logged in to the payment services website, but are inactive for 10 minutes or more, then the website times out and you are prompted to enter your login details again when you try to perform an action. Note that a timeout reminder will display for the last 2 minutes.

SEE ALSO

## 3.4  Action changes using ASM

When you change, add or delete information on the payment services website, you are prompted to confirm those actions. You must confirm the actions using the security method you logged on to the payment services website with. The following procedure details how to confirm changes using your ASM credentials.

PREREQUISITE

You must have logged in using your ASM credentials and made changes on the payment services website.

STEPS

1.  Review the summary of your changes and accept them.

    A *Summary* screen displays detailing the changes you are making.

    For each change:

    • *Field* column: displays the field name
    • *Before* column: displays each field before the change
    • *After* column: displays the changes made
    • *Change type* column: displays created, updated, or deleted, as appropriate

    If the summary is correct, click **Confirm** to start the process of actioning the changes.

2. Authorise the changes by signing the text that displays.

   If the changes were made successfully, the *Confirmation* screen displays with a success banner at the top.

   In some circumstances, for example, if your browser crashes, you may not see the success screen. If this happens, confirm that the changes you made have been applied.

   To make another change like the one you just made, click **Another** on the success banner.

   ***NOTE:*** *Following many changes actioned on the payment services website, email notifications are sent by the payment services website to the PSCs associated with the contact making the changes. The email notifications detail what was changed, who made the changes and so on.*

## 3.5   Change your password

You can change your password when you are logged in to the payment services website.

PREREQUISITE

- You must be logged in to the payment services website using your password

  **IMPORTANT:**  If you think that someone else knows your password or may have used your password, contact the service desk or your sponsor immediately.

STEPS

1. From the top right-hand corner of any screen, click the down arrow to open the *My Profile* menu.

   STEP RESULT

   *My Profile* menu displays.

2. Click **My details**.

   STEP RESULT

   *My Profile* screen displays.

3. Click **Change password**.

   The *Update password* screen displays.

4. Enter your current password.

   When you enter your password, it is masked. To check that you have entered it correctly, click the **View** icon to reveal it.

5. Enter your new password, and then enter it again to confirm it.

   Ensure your password complies with the requirements listed in section "Password requirements" on page 32.

6. Click **Update password**.

   STEP RESULT

   If successful, a success banner displays at the top of the screen, and the *My Profile* screen reloads.

RESULT

pay.uk

Your password is changed.

> **NOTE:** ASM contacts that were set up before August 2016, are prompted to complete the security information and security hint details when they log in to the payment services website for the first time following a password reset or change. This is not required for subsequent password changes.

SEE ALSO

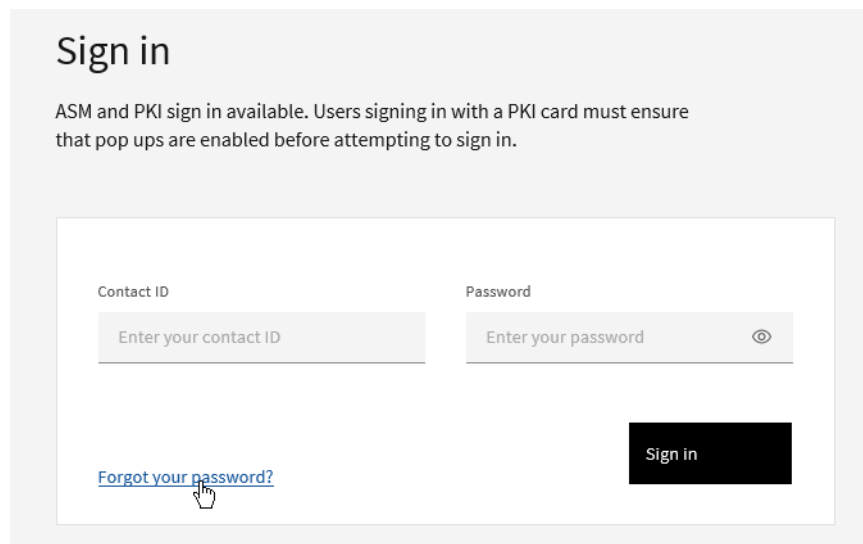[“Password requirements” on page 32](#)

## 3.6 Reset your password

If you have forgotten your password, you can reset it from the payment services website login screen. This removes your existing password and initiates the process for you to retrieve a new password.

PREREQUISITE

- Your ASM status must be 'Active' (if you are suspended, for example, because you have repeatedly mis-entered your password, then a PSC or the PSP that maintains your registration must first reinstate you before you can reset your password).

STEPS

1. From the payment services website login screen, click **Forgot your password?**

🌀 pay.uk

STEP RESULT

The *Forgotten password* screen displays.



2. Enter your **Contact ID** and the **Answer to your security information** (this is not case sensitive).

   **NOTE:** *If you have forgotten the answer to your security information, click* **I've forgotten my security information***. On the Forgotten security information screen enter your Contact ID and click* **Remind me***. An email is sent to you with the hint for your security information. If you still cannot remember your security information, then contact your sponsor or the Bacs service desk.*

3. Click **Reset password**.

   STEP RESULT

   If you successfully entered your security information, a 'Success' message displays at the top of the *Sign in* screen.

   **NOTE:** The password criteria display on the payment services website following a password reset.

RESULT

Your password is reset. You receive an email to enable you to retrieve your new password. Your ASM status is changed to 'Pending'.

   **NOTE:** Emails are sent immediately, but please allow one hour for the email to be received. If you do not receive it, then check that it is not in your email 'junk' folder.

   The first time you change your password, you are prompted to complete the security information and security hint details. This is not required for subsequent password changes.

## 3.7    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.

### 3.7.1    Contact ID and password retrieval issues

| Issue and description | Action |
|---|---|
| You have deleted the 'password retrieval' email. | Ask a contact that can maintain your details to resend the email to you. |
| URL to retrieve your password does not work | Ensure you are properly connected to the internet (or extranet). If the URL has been copied and pasted into the browser, ensure that the complete URL has been copied. |
| Name displayed is not correct | Ensure that you are using the correct email. Ask a contact that can maintain your details to check your name on the payment services website. |
| Technical error or 'try again later' message displayed in browser | Try the action again (using the same URL). |
| Security information is not accepted | If you have forgotten your security information, then have the hint emailed to you (you can do this as part of the steps to retrieve your password). If your security information is still not accepted, ask a contact that can maintain your details to change it. |

### 3.7.2    Password issues

| Issue and description | Action |
|---|---|
| Forgotten password | Follow the steps to reset your password. |
| Your repeatedly mistype your password and your account is locked | You need to ask someone that can maintain your details to reinstate you. |
| Password has been compromised (you think that someone else may know your password) | Contact the PSP that maintains your details, or the service desk. |

## 3.8   ASM statuses

All contacts have an ASM status; to log on using contact ID and password your ASM status must be 'Active'.

| Status | What it means |
|---|---|
| Not set | The contact has not been set up to use ASM. |
| Active | The contact can use their contact ID and password to access the payment services website. |
| ASM pending | The contact has not retrieved their contact ID and password. |
| Suspended | The contact cannot access the payment services website using their contact ID and password. The suspension may have been automatically done by the system, for example, if a contact repeatedly mis-enters their password, or another contact may have manually suspended the contact. The contact must be re-instated before they can use their contact ID and password. When the contact is re-instated, their ASM status returns to 'Active'. |
| Suspended - Pending | A contact has been suspended. Before the contact was suspended, their ASM status was 'ASM pending'. After the contact is re-instated, their status returns to ASM pending. |

SEE ALSO

# 4   Update your details

You can update your email address and telephone numbers. Other information can only be maintained by a PSC or the PSP that maintains your registration. No privilege is required for this activity.

PREREQUISITE

- You must be logged in to the payment services website with PKI or ASM.

STEPS

1. From the top right-hand corner of any screen, click the down arrow to open the **My profile** menu.

2. Under *My profile*, click **My details**.

   STEP RESULT

   The M*y profile* screen displays.

3. Scroll down until you can see the **Update details** check box and select it.



   STEP RESULT

   The *My profile* screen redisplays, and the fields can now be edited.

4. Make the required changes.

   You can change your email address, phone, and fax numbers, as required. You can also add extra information for your office and mobile telephone numbers.

   **NOTE:**  *You cannot change your security information and hint. Your PSC or your sponsor can change this for you.*

5.  Click **Continue**.

6.  Review the details on the summary screen.

    For each change

    *   *Field* column: displays the field name
    *   *Before* column: displays each field before the change
    *   *After* column: displays the changes made
    *   *Change type* column: displays created, updated, or deleted, as appropriate

7.  Confirm the action.

    If you are logged in with PKI, the Security check screen displays. With your smartcard in the reader, use your PIN to sign the information.

    If you logged on with ASM, enter your password and click **OK**.

    STEP RESULT

    If successful, the *Confirmation* screen displays with a success banner at the top.