

Implementation guide

BACSTEL-IP for direct submitters

BACSTEL-IP



Contents

Welcome to BACSTEL-IP	3
Using this guide	3
Useful contacts.....	4
Understanding BACSTEL-IP	5
The software	6
The website.....	6
The security.....	7
The people.....	8
Getting ready	9
Choosing your BACSTEL-IP software	9
Getting your IT infrastructure ready.....	10
Creating your workflows.....	11
Setting up your security procedures.....	12
Planning for contingency.....	13
Filling in your application form.....	14
What happens next?.....	14
Installation	15
Preparing for installation.....	15
Installation day	16
After installation.....	16
More information	17
Contact ID and password – ASM.....	17
Smartcards – PKI security.....	18
Notification emails.....	19
From BACSTEL to BACSTEL-IP.....	20
Glossary	21

This is version 1.10 of this guide.

Our reference: PN6200

BACS Payment Schemes Limited © 2005.
All rights reserved.

The copyright in this document is owned by BACS Payment Schemes Limited. All material, concepts and ideas detailed in this document are confidential to BACS Payment Schemes Limited. This document shall not be used, disclosed or copied in whole or in part for any purposes unless specifically approved by BACS Payment Schemes Limited.

BACS, BACSTEL-IP, BACSTEL and BACSAFE are registered trademarks of BACS Payment Schemes Limited.

Welcome to BACSTEL-IP

BACSTEL-IP[®] is the new access channel for the BACS[®] service. It has new security measures and new functionality to benefit all BACS users. This guide takes you through some of the basics of BACSTEL-IP and helps you plan and implement your move to this new service.

This guide is for organisations that send payment information directly to BACS (these organisations are called “**direct submitters**”). It can be used by customers that are new to the BACS service as well as customers that are upgrading their systems from BACSTEL.

 **Plan your implementation now!**
BACSTEL-IP is replacing the BACSTEL service. BACSTEL will not be available after December 2005. This means if you have not started planning your move to BACSTEL-IP, you must start now.

Using this guide

This guide is divided into a number of parts. Begin by Understanding BACSTEL-IP (page 5), then start Getting ready (page 9) for your implementation. When you are ready to come onto BACSTEL-IP, Installation (page 15) explains what you need to do before the installation of your new BACSTEL-IP software and lets you know what happens on installation day. In More information (page 17) there is extra detail on some topics covered in this guide. If you need help with the terms used, turn to the Glossary (page 21).

You will find a lot more information to help you at www.bacstel-ip.com

Symbols used in this guide



Take note, this is background information, especially for people new to the BACS service.



Important information you must be aware of.



Directs you to more information.

Useful contacts

Here is a list of contacts you may find useful during your implementation of BACSTEL-IP. Make sure you also have the contact details of your software supplier and your bank.

Before and during your implementation

Contact your bank or the BACSTEL-IP Customer Information Centre:

Telephone 0870 240 8138

Website www.bacstel-ip.com

Email bacstel-ip@BacsServices.co.uk

BACSTEL-IP training courses

Telephone 01202 318520

Website www.voca.com/product/training.php

Email bacstraining@unitrain.com

Some solution suppliers can also provide additional training.

Connectivity

Telephone 0870 920 8072

Website www.voca.com/connectivity/index.php

Installation questions

Please contact the supplier of your BACS approved software.

After you have implemented BACSTEL-IP

Contact your bank, solution supplier or the BACS service desk:

Service desk telephone 0870 165 0018 or 0870 010 0698

Email servicedesk@BacsServices.co.uk

Telephone calls to the BACS service desk may be recorded for security or monitoring purposes.

Other useful contacts

Charteris Consultancy Services

A consultancy service for customers migrating to BACSTEL-IP

Telephone 020 7600 9199

Email bacsteam@charteris.co.uk

HSM implementation and customer take-on training

Provided by Voca. For information and to book by telephone, call 0870 920 8072.



In December 2003, BACS separated into two companies to best meet the needs of its customers.

Voca Limited (formerly BACS Limited) is the company that physically processes payments for the BACS service and maintains the payments network. As part of this, Voca provides connectivity solutions and training for BACSTEL-IP.

BACS Payment Schemes Limited is a membership based organisation that enhances the integrity of the payment schemes.

This does not impact your use of the BACS service. For more information, go to www.bacs.co.uk

Understanding BACSTEL-IP

BACSTEL-IP is used to send payment information to the BACS service and to get your BACS reports electronically. BACSTEL-IP also allows you to manage some aspects of your organisation's set up for the BACS service.

You can connect to BACSTEL-IP using the internet, the dial-up extranet or an "always on" fixed extranet, DSL or broadband solution. The internet and dial-up extranet mean you can re-use existing infrastructure to connect to BACSTEL-IP.

There are two ways you access BACSTEL-IP: using software that BACS has approved for BACSTEL-IP; and using a secure website called BACS payment services.



To access BACS services, you are sponsored by your bank. You are set up as a "service user" and given a unique service user number. Some organisations may be set up with more than one service user; for example, your payroll and finance sections may be set up separately.

Users may be familiar with the terms, BACS user number and originator identification number (OIN); these are the same as your service user number in BACSTEL-IP.



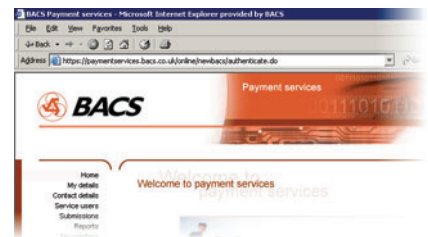
Use **BACS Approved Software for BACSTEL-IP** to...

- Send payment information
- Get your BACS reports

Your software checks your payment information before you send it; this helps to reduce processing problems.

Use the **BACS payment services website** to...

- Get your BACS reports
- View information about your recent submissions
 - Maintain your user details
- Set up people to act for your service user
- View information about your service user.



With BACSTEL-IP, you get your reports electronically as web pages that you can print or save, and/or in XML (extensible markup language). XML lets you upload your reports into other programs, so the information can be integrated into your business applications or systems. Using BACSTEL-IP, you will get your reports faster than the current paper-based system.

The software

The only software you can use to access BACSTEL-IP, is software that has been approved under the BACS Approved Software Service for BACSTEL-IP. This service makes sure that software meets set standards and provides you with core functionality. In this guide, BACS Approved Software for BACSTEL-IP is referred to as BACSTEL-IP software.

The core functionality that all software provides, includes:

- **Payment file creation**, BACSTEL-IP software can create payment files and submissions for you
- **File and submission signing**, all submissions must be digitally signed, you can also sign payment files within submissions. Your software takes you through the signing process
- **Checks before you send a submission**, before sending a submission for processing, your software carries out certain checks on it. If there are problems, you have the opportunity to address them before you send the submission. This helps to reduce problems later
- **Updates to ISCD and modulus check routines**, software suppliers will give you updates to the ISCD (industry sorting code directory, to validate sorting codes before you send payment information) and modulus check routines (to validate account numbers)
- **Accessing reports**, all BACSTEL-IP software lets you get your BACS reports, as web pages or in XML.

Your software will be linked to your service user by your bank. Your software must also be tested before you can use it; your software supplier helps you with this. Once the testing is complete, your bank needs to update your service user profile so you can use your software for live submissions. If you need to, your service user can have up to three BACSTEL-IP software packages linked to it.

↳ For more information, see Getting ready – Choosing your BACSTEL-IP software, page 9.

The website

BACS payment services is a secure website for BACSTEL-IP. On this site, you can...

- View information about your BACS submissions, including errors identified when they were sent
- Get your reports as web pages or in XML
- Maintain some details of your service user and the people that act for your service user
- Maintain your own details.

↳ To preview the website, go to www.bacstel-ip.com and follow the navigation to the interactive tour.

Note: You get the web address for the payment services website in a “welcome” email when you are set up for BACSTEL-IP. www.bacstel-ip.com provides you with general information on BACSTEL-IP and an interactive tour of the payment services website.



When you send payment information for BACS processing, you send it as a “**submission**”. The submission is like an envelope; it contains a “**payment file**” that has details of each payment you want to make or collect.

If you are a bureau, your submission can have more than one payment file in it; for other service users, your submission can only contain one payment file.

The security

BACSTEL-IP offers heightened security to use the BACS service. It uses the latest public key infrastructure (PKI) technology. PKI uses digital keys and digital certificates to provide authenticity and data integrity for electronic communications and data transfers.

There are two ways you can use PKI security with BACSTEL-IP:

- With a **smartcard** – a smartcard is the size of a credit card and contains a chip that holds your PKI credentials (digital keys and digital certificates). You use it by inserting the card into a smartcard reader and using a PIN to digitally “sign” information that is displayed to you
- With a **hardware security module (HSM)** – an HSM is a piece of hardware that is installed into your computer systems and is used to hold PKI credentials. HSMs allow you to automate your submission and report access process. Using an HSM means you do not need someone present to enter their smartcard and PIN. HSMs will mainly be used by organisations that make frequent submissions or need to automate the process. (You will still use smartcards if you need PKI access to the payment services website.)

When using BACSTEL-IP software, you use a smartcard or an HSM to log on to BACSTEL-IP; this creates a secure session so you can send submissions and get reports. Smartcards can also be used to access the payment services website and to confirm changes to data on the website.

All submissions sent to BACSTEL-IP must be digitally signed using PKI (your software helps you do this). Payment files within submissions can also be signed.

Unlike BACSAFE[®] devices used on BACSTEL[®], people must have their own smartcards; smartcards cannot be shared between people. This improves the audit trail as you can find out who, for example, sent a submission.

➡ For more information on smartcards, see page 18; for more information on HSMs go to www.bacstel-ip.com or speak to your software supplier or bank.

The alternative security method – ASM

As well as using PKI, you can access the payment services website using a username (called a contact ID) and password. This is called the alternative security method (ASM). You cannot use ASM with your BACSTEL-IP software. ASM cannot be used for submissions.

When you are logged on with ASM you can get reports and maintain some information about your service user. Using ASM means you can log on to the website using most computers with a web browser and access to the internet. (You do not need a smartcard or reader to use ASM.)

➡ For more information on ASM, see page 17.

Note: You can use a combination of PKI and ASM to suit your business needs. You may want some people to use PKI, some to use ASM and some to use both security methods.

The people

To use BACSTEL-IP, you are set up as a “**contact**”. Contacts are linked to service users. They are given “**privileges**” to do certain things for that service user. For example, a contact may have the privilege to sign submissions. If you do not have the right privileges, you will be stopped from carrying out that activity.

Contacts are given PKI and/or ASM security. The choice of security depends on what privileges the person needs (there are some privileges that can only be given to contacts using PKI).

If your organisation has more than one service user, and the service users are sponsored by the same bank, then contacts can sometimes be linked to more than one service user. The contact only needs one set of security credentials; so if you have a smartcard, you use that smartcard and PIN for all service users you are linked to. If you do have more than one service user and want to be able to do this, speak to your bank about your set up on BACSTEL-IP.

If you have service users sponsored by different banks, you need different smartcards for each bank.

There are two types of contacts:

- **Primary security contacts** – called PSCs; and
- **Additional contacts.**

Each service user must have at least two PSCs linked to it. There is no minimum requirement for additional contacts. You can have as many contacts of either type as you need.

The role of the PSC

PSCs are your bank's first point of contact with your service user. PSCs can be given a wider range of privileges than additional contacts. In particular, PSCs can be given privileges to add and maintain additional contacts. If, for example, an additional contact forgets their ASM password, a PSC (with the right privilege) can reset the password. But, if a PSC forgets their ASM password, they need to speak to their bank to have it reset. PSCs can also be given privileges to maintain some details about your service user.

PSCs receive email alerts when certain things happen on BACSTEL-IP. These emails relate to your:

- **Service user**, you get emails when your service user is set up and then when any changes are made to it by another PSC or by your bank
- **Additional contacts**, you get emails when they are added or deleted and when their details are changed by another PSC or by your bank. You also get emails if their access to BACSTEL-IP gets locked for any reason
- **Submissions**, you get emails when a submission is rejected.

 For details of the emails a PSC gets during the registration process, see page 19.

Getting ready

This part helps you start planning for BACSTEL-IP. You need to coordinate the implementation of BACSTEL-IP within your organisation. This may mean involving different departments such as payroll and finance and other users of the BACS service. You also need to involve your IT department.

Before you start getting ready, you should speak to your bank to tell them you want to start using BACSTEL-IP. Here is a checklist summary of what you need to do to get ready for BACSTEL-IP:

- Choose your BACSTEL-IP software
- Get your IT infrastructure ready:
 - Computer hardware
 - Connection method
 - Web browser
 - Email addresses
- Create your workflows
- Set up your security procedures
- Plan for contingency
- Fill in and send your application form(s)



If you do not already use the BACS service, speak to your bank or building society. They will tell you what you do to start using the BACS service and provide advice on the best set up for your organisation. You still need to start planning your implementation of BACSTEL-IP.

Choosing your BACSTEL-IP software

You must get new software to use the BACSTEL-IP service. This software must be approved for BACSTEL-IP (see page 6). If you are a BACSTEL user, your software supplier may have similar products to your BACSTEL software that have been designed and approved for BACSTEL-IP. For a list of suppliers with approved software available, go to www.bacstel-ip.com

While all software provides core functionality (see page 6), some software may have extra functionality or add-on modules. When choosing your BACSTEL-IP software, consider your needs and then look at the solutions available. It is your responsibility to check with the supplier that the software performs all the functions you need. Here are some things to consider:

- Will it work on the operating system and platform you use?
- What are the computer specifications needed, for example hard drive space, memory?
- Does it integrate with other software you already have?
- Does it support Direct Debits and Direct Credits, or do you only need it to support one?
- Does it support multiple service user numbers?
- Does it support the use of HSMs (if you need them now or in the future)?
- What are the licensing and support arrangements?
- Does it support your workflows, see Creating your workflows, page 11?
- Does the supplier offer any form of contingency service?

Getting your IT infrastructure ready

At its most simple, your IT set up for BACSTEL-IP could be one computer with:

- A modem (and phone line)
- A smartcard reader attached and signing software installed
- A web browser
- BACSTEL-IP software.

While you could use this set up, remember, you should also plan for contingency, see page 13.

Computer hardware

If you have existing computers you want to use for BACSTEL-IP, get the specifications together when you speak to software suppliers to ensure that they are suitable. The information you need is:

- The operating system used
- Hard disk space and processor speed
- Details of the modem or other connection.

If you are going to get new computers, make sure their specifications are suitable for your software.

You also need to be able to attach a smartcard reader to any computer you want to use a smartcard on. A reader is normally attached using a USB connection; however, you may be able to get readers that connect over a serial port or PCMCIA. Check with whoever is supplying your readers.

↳ See Smartcards – PKI security, page 18 for more information on the smartcard readers.

Connection methods

You need to be able to connect to BACSTEL-IP. You can connect using:

- The internet
- The dial-up extranet, using a modem and a phone or ISDN line you can connect to the dial-up extranet
- DSL Connect, Fixed Extranet Connect and Broadband Direct: these offer “always on”, high-speed connections.

Over any of these connections you can access the website or connect using your BACSTEL-IP software. You can have more than one connection type; for example, some users may want to use the internet to connect to the payment services website and a fixed extranet connection for using their BACSTEL-IP software.

Not all connection methods are suitable for all users. It depends on your existing infrastructure set up and your requirements for BACSTEL-IP. Speak to your IT department and your software supplier.

↳ Go to www.bacstel-ip.com for details about connection methods including submission speeds and the level of service you can expect. The site also contains links to order a DSL Connect, Fixed Extranet Connect or Broadband Direct solution.

Web browser

To access the payment services website, we recommend you upgrade your web browser to the latest version of Netscape Navigator (available from www.netscape.co.uk/netscape) or Internet Explorer (www.microsoft.com).

Email addresses

Contacts need email addresses. It is best if each contact has their own email address, but a group address can sometimes be used; your bank's application form should say if a group email address is acceptable. If you want more than three people to receive email notifications when reports are available, you could set up a group email address to use as your service user's default email.

Creating your workflows

BACSTEL-IP lets you define workflows and set up strong audit trails for your payment submissions. By giving people different “privileges”, you can make sure that sending payment submissions involves more than one person. Because activities use PKI, you can find out who signed a payment file or submission and who sent a submission.

Some of the privileges that you can give to contacts include:

- Signing payment submissions
- Sending submissions
- Accessing processing reports.

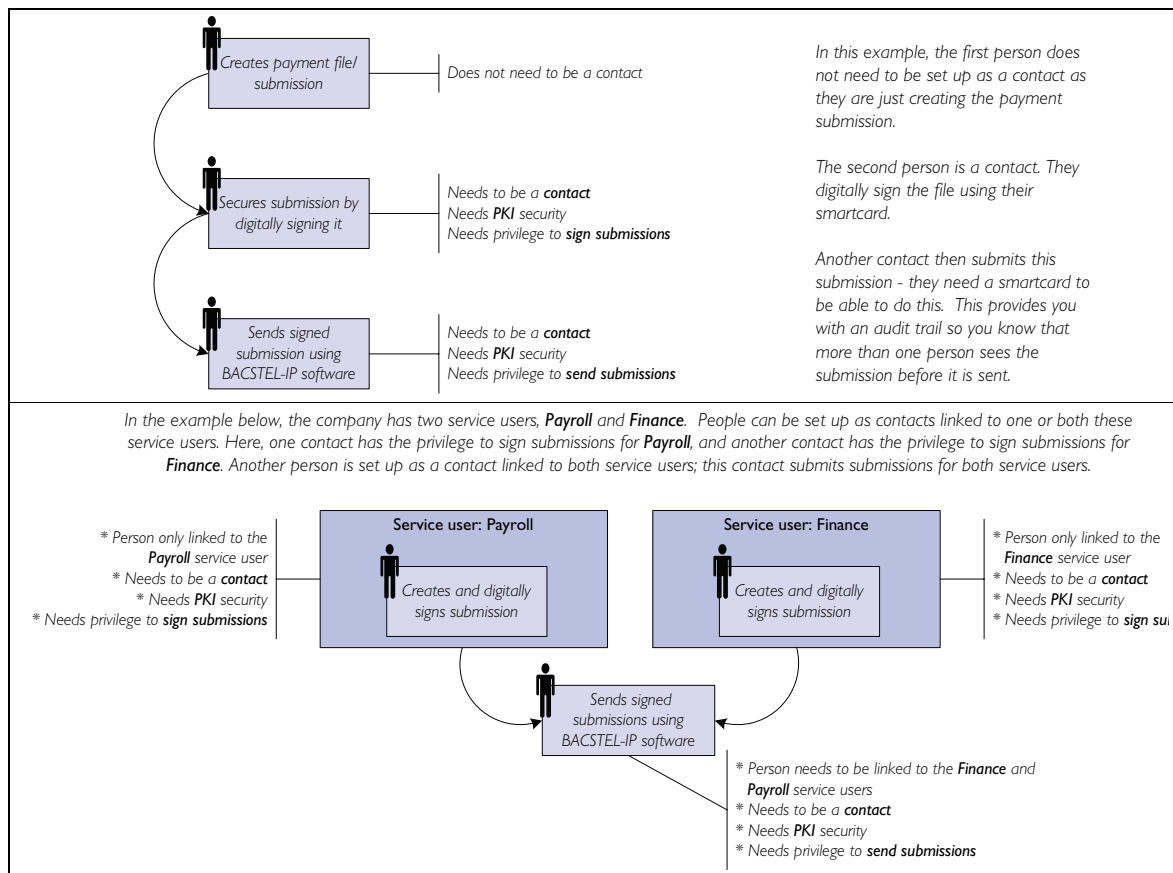
↳ For a detailed list of privileges, see the “BACSTEL-IP – Service user guide”; download it from www.bacstel-ip.com

You may want one group of people to be able to sign submissions and another group to be able to send submissions. (Not all software will allow different people to sign and send submissions, check with your supplier.) For example, in your payroll section, you may want a payroll administrator to create and send payment submissions, but the payroll manager to secure the payment by digitally signing the submission. You may also want everyone to be able to access processing reports.

Remember, when planning your workflows, you must make sure there are no single points of failure in your organisation. This means you need more than one person that can do a given role.

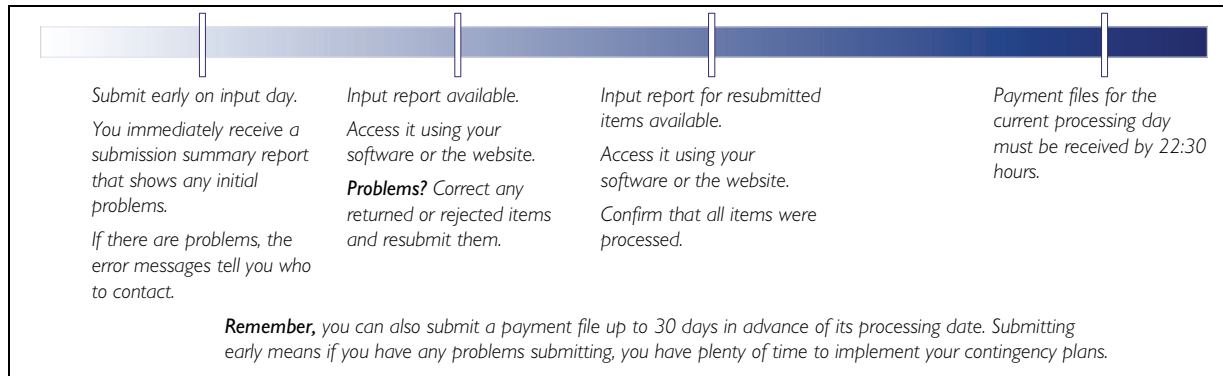
As well as these privileges, BACSTEL-IP software may also have permission settings to support your workflows; speak to your supplier.

The following diagrams are some examples of workflows to give you an idea of what you can do using privileges.



When you put together these workflows, consider the times that different activities are done to take full advantage of the capabilities of BACSTEL-IP. Your input report is normally ready within 4 hours of your payments being processed on input day – this means if you submit early in the day (or even before input day), you can fix errors and resubmit for the same processing cycle. (If you submit before input day, you still only get your input report on input day, but you will get it early in the day.)

The diagram below shows how submitting early means you can fix problems the same day.



➡ See the “BACSTEL-IP – Service user guide” for information on the processing cycle and the opening times of BACSTEL-IP. You can download the guide from www.bacstel-ip.com

Setting up your security procedures

As well as these workflows, you must set up policies and procedures for using PKI and ASM security with BACSTEL-IP. You should also make sure your processes in relation to cancelling smartcards meet your bank’s requirements. Some things to consider are:

- Where smartcards are stored when not in use, eg locked in a person’s drawer
- Smartcard use during office hours, eg they should not be left in the reader when not in use
- Who to contact if a smartcard is lost or becomes compromised; you should contact your bank immediately. If it is an additional contact, a PSC should also suspend the contact using the payment services website
- Procedures if a person leaves your organisation to have their access to BACSTEL-IP revoked
- Protection of a contact’s PIN and ASM password; they must not be given to anyone else. If the PIN or password does become compromised (meaning someone else could have used it, or someone else knows it) you must contact your bank immediately.

Planning for contingency

Part of your planning for BACSTEL-IP must consider your contingency needs. It is essential you have no single points of failure that could stop you from sending payment information.


When assessing your needs, consider the impact if you could not submit a file. The business implications and the associated costs of such a problem need to be considered when deciding on contingency solutions.

We recommend you have a relationship set up with a bureau that can submit on your behalf if needed. Your bank or software supplier may offer bureau services or you can go to another organisation that offers a bureau service. Any organisation that provides bureau services to third parties must be a BACS Approved Bureau, so you know they meet set standards. You must inform your bank of the details of any bureau you may use to submit, before a file is submitted.

You should also consider the following:

- Connection problems – you should have other ways to connect, for example a spare telephone line to connect using a dial-up connection
- A contact's smartcard does not work or a contact is off sick or on holiday – you should always have multiple contacts with smartcards and the necessary privileges
- The computer with your BACSTEL-IP software fails – under your licensing arrangements you may be able to have backup installations of your software.

If you have multiple sites, you may consider having people at different sites that are set up as contacts for your service user. If you use an HSM, you may also consider having the ability to submit using a smartcard as a backup (not all software will support this) or having a second HSM. You should speak to your supplier or your bank for advice when considering contingency for HSMs.

 There is no equivalent in BACSTEL-IP to the “emergency password” that you could get for the BACSTEL service. This means if a smartcard (or HSM) fails, for example, when you are trying to sign a submission, another contact at your service user will have to sign the submission using their smartcard or another HSM needs to be used. If you do not have any other contacts with PKI available, your only choice would be to submit using a bureau.

Filling in your application form

Your bank will ask you to fill in an application form for BACSTEL-IP. For details of where to get the forms for your bank, speak to your bank or go to www.bacstel-ip.com

(You may also complete application forms for your software supplier or if you get a DSL Connect, Fixed Extranet Connect or Broadband Direct product.)

The exact contents of the form depends on your bank, but here are things that you will need to fill in.

Details of two PSCs. You have to select two people that will be PSCs. You need to provide their name, email address and telephone numbers. If they will have ASM, you also need to provide security information and a hint for this information; see Contact ID and password – ASM, page 17.

↳ For information on the role of a PSC, see Understanding BACSTEL-IP, The people, page 8.

Software supplier, package name and installation date. You need to include details of your supplier and package. Ideally, you should have agreed the installation date with your supplier. You should also discuss it with your bank to ensure that smartcards and PINs can be issued in time.

Connection method. You are normally asked about how you plan on connecting to BACSTEL-IP. If you tick dial-up extranet, then your bank will set you up to receive an extranet ID and password. If you need DSL Connect, Fixed Extranet Connect or Broadband Direct solution, you need to arrange these separately; go to www.bacstel-ip.com for information on the connection types, including links to order them.

A default or generic email address. This can belong to an individual or could be a group email address. It is used to send email notifications to alert you when new reports are available (these notifications can be configured after your registration; you can choose to have up to three named contacts notified instead of the notification going to the default email, but, you still must specify a default email).

What happens next?

When your bank registers your service user for BACSTEL-IP, your PSCs will get a series of emails – these need to be kept for your installation. Check to make sure you have these emails...

- An email confirming that your service user has been registered for BACSTEL-IP. If you have been set up for the dial-up extranet, this has your extranet ID and password
- An email to allow each PSC to register their smartcards
- An email to allow any PSC with ASM to get their contact ID and password.

If you do not have any of these emails the day before your installation, speak to your bank.

Your bank will issue smartcards and PINs and, in some cases, smartcard readers and signing software. Your bank may also send the PSCs emails about the registration process or when your smartcards have been issued.

↳ For details of the emails, see page 19.

Installation

Preparing for installation

Your software supplier will install your BACSTEL-IP software. The time taken for the installation depends on a number of factors; speak to your supplier for an estimate. An HSM installation will take more time than a smartcard installation.

To make sure the installation goes smoothly, you must make sure you have everything ready before they arrive. Here is a checklist of things to consider (some suppliers may also provide a preinstallation checklist).


- Have the contact details for your bank and your software supplier
- Make sure you have returned any licensing agreement to your software supplier
- Confirm the installation date with your software supplier and your bank
- Have your service user number(s) and details of all bank accounts you have set up for this service user
- Your supplier will help you make a test submission during the installation. Make sure you have test data available; your supplier will give you more details of what is needed
- Check with your supplier to see if there are any other special requirements they may have.

Computer hardware and software...

- Your computer equipment must be ready
- If you have IT staff, make sure they will be available on installation day to resolve any internal IT issues you may have
- Your supplier will need to have sufficient administrator access to your systems to be able to install the BACSTEL-IP software, smartcard readers and signing software. Software will normally be installed from a CD. Make sure you have a CD-drive available and make sure it can be accessed (they are sometimes disabled)
- Smartcard readers and signing software must be available and ready to be installed (in some cases, your software supplier may provide these; confirm this with them). Make sure you have the right connection types available to attach the reader
- You need a connection method available, if you will use..
 - The internet, make sure your internet connection is working and that your firewall settings allow access to BACSTEL-IP and emails from info@bacs.co.uk
 - The dial-up extranet, make sure you have a modem installed and have a telephone or ISDN line available and that it is working. Your bank must have set you up to receive a dial-up extranet ID and password. This is emailed to the PSCs
 - A Fixed Extranet Connect, DSL Connect or Broadband Direct solution, if this is not ready when your software is installed, make sure you have one of the connection methods above available.

Your PSCs must be available for the duration of the installation. They must each have...

- Their smartcard, PIN and "Registering your smartcard" email
- If PSCs have ASM, they need their "Your contact ID and password" email
- If you will use the dial-up extranet, you must have the email containing the extranet ID and password.

 If after you have arranged the installation date, one PSC cannot be there for the installation, the other PSC must take full responsibility for training others in your organisation. We recommend you do not reschedule your installation wherever possible.

Installation day

On the day of installation, your software supplier will...

- Install your new BACSTEL-IP software
- Install your smartcard readers and the signing software
- Help the PSCs register their smartcards. If you have ASM they will also help you get your contact ID and password
- Complete a series of tests including sending in a test submission; see Testing your software below
- Provide training on your software and the payment services website.

When contacts register their smartcard and when they get their contact ID and password for ASM access, they get a "Welcome" email; this contains the web address for the payment services website.

Testing your software

Before using your BACSTEL-IP software for live submissions, your supplier will help you perform a few tests. If you will use your BACSTEL-IP software for more than one service user number, then you need to complete the tests for each service user.

The tests are recorded in a "service qualification plan" that is linked to your software.

Your software supplier helps you complete these tests as part of the installation; the tests will also form part of your training. Here are the tests:

Log on to BACSTEL-IP using your software

After the PSCs have registered their smartcards, your supplier will show you how to connect and then log on to BACSTEL-IP using your software. When you have logged on successfully, the test is complete.

Access generic test reports

BACSTEL-IP has a "generic test report"; this is a sample report, used to make sure you can access reports. Once you have successfully accessed the report, then the test is complete.

Make a test submission that undergoes online validation

When you send a submission, BACSTEL-IP performs certain checks on it while you are still online. When these checks are done, BACSTEL-IP sends you a submission summary report confirming that the submission has been received and whether it was accepted for further processing. When a submission is accepted, the test is complete.

Make a test submission that undergoes full live simulation testing


Your bank may not require you to perform this test; they will let you know if you need to. For this test, you send a test submission that goes through full test processing. This produces a test input report. Your bank will check this report to see if there were any issues during processing. After sending the submission, it may take one or two days before your bank can confirm if the test is OK.

Once testing is complete, your supplier contacts your bank to notify them. When your bank is satisfied things are working, they update your service qualification plan so your BACSTEL-IP software is ready for live submissions. (If you performed the live simulation test, this may take one or two days.) Your PSCs will receive an email when this is done.


After installation

Once the installation is completed and your software is live, you are ready to start using BACSTEL-IP. Issues with your software should still be directed to your software supplier. Other issues should be directed to your bank (although if your bank has a dedicated implementation team, you may need to speak to a different section) or the BACS service desk.

If you do not already have them, make sure you get your...

- BACSTEL-IP – Service user guide
- Getting started guide – BACSTEL-IP for direct submitters
-  You can download these guides from www.bacstel-ip.com

If you are migrating from BACSTEL to BACSTEL-IP, see page 20 for more information.

 If you try to send a live submission using a software package that has not been set to live, the submission will be rejected.

More information

Your key sources for more information are:


- **www.bacstel-ip.com**
This site contains wide ranging information on BACSTEL-IP, including downloads of the guides below. It also contains a list of software suppliers that have BACS approved software available.
- **BACSTEL-IP – Service user guide**
The “Service user guide” contains more detail on using BACSTEL-IP and explains the security. It also includes detailed procedures for using the payment services website. This includes your “Contact’s guide” for BACS payment services.
- **Getting started guide – BACSTEL-IP for direct submitters**
The “Getting started guide” helps you with initial tasks and day to day activities on BACSTEL-IP.

This part has more information on some topics mentioned in this guide.

Contact ID and password – ASM

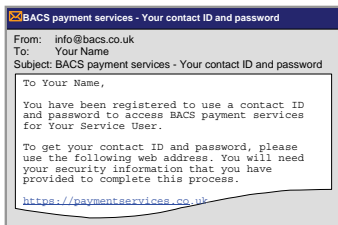
ASM allows you to get onto the BACS payment services website using a username (called a contact ID) and password. You get your contact ID and a temporary password by following a process of authenticating yourself using “security information”. (The first time you use the password, you have to change it.)

To be set up for ASM...

 You must never give your password to anyone else. Your bank and the BACS services desk will never ask you for your password.

<p>Security information <input type="text"/></p> <p><i>This will be used to retrieve your password.</i></p> <p>Security information hint <input type="text"/></p> <p><i>This will be emailed to you if you forget your security information.</i></p>	<p>...on your application form, each contact that needs ASM provides “security information” and a “security information hint”. (Some banks may set your security information hint.)</p> <p>For example, the hint could be a question, such as “Mother’s maiden name?” with the security information being the answer.</p> <p>You have to enter your security information to be issued with your contact ID and password. The security information is not case sensitive.</p>
--	--

After you are set up as a contact with ASM, you get..

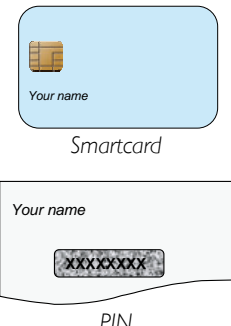
 <p>Issue of access codes email</p>	<p>...an email with the subject “BACS payment services – Your contact ID and password”. This email contains a unique web address that allows you to get your contact ID and password.</p> <p>You will be asked to enter your security information as part of this process. If you do not remember your security information, you can have the hint emailed to you.</p>
--	--

Smartcards – PKI security

PKI security is the only security method you can use with your BACSTEL-IP software; you can also use it to access the payment services website. You use PKI security to digitally sign information. This digital signature is checked by the BACS service to authenticate that it is you that has signed the information and that the information has not been changed since you signed it. The “BACSTEL-IP – Service user guide” has more information on how PKI security works. For information on HSMs see www.bacstel-ip.com or speak to your bank or software supplier.

! You must never tell anyone your PIN. Your bank and the BACS services desk will never ask you for your PIN.

When you are set up as a contact with PKI security, you get...



The illustration shows two items: a blue smartcard with a gold chip and the text 'Your name' below it, labeled 'Smartcard'; and a white card with a black chip and the text 'XXXXXXXX' below it, labeled 'PIN'.

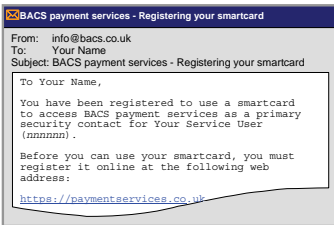
... a **smartcard** and **PIN** from your bank for each person that is set up as a contact with PKI. These will be sent separately.

You will often have to change your PIN the first time you use it.

What you do? Keep your smartcard and PIN separate and secure until the installation of your software.

You cannot use your smartcard until it has been registered on BACSTEL-IP, and your smartcard reader and signing software have been installed.

Your software supplier will help the first two PSCs register their smartcards when they install your BACSTEL-IP software.



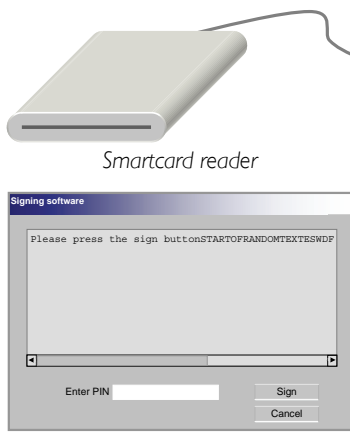
The screenshot shows an email from info@bacs.co.uk to 'Your Name' with the subject 'BACS payment services - Registering your smartcard'. The body text says: 'To Your Name, You have been registered to use a smartcard to access BACS payment services as a primary security contact for Your Service User (nnnnnn). Before you can use your smartcard, you must register it online at the following web address: https://paymentservices.co.uk'.

When you are set up as a contact with PKI security, you are sent an email with the subject “BACS payment services – Registering your smartcard” from info@bacs.co.uk. This email contains a unique web address for you to use to register the digital certificate that forms part of your PKI credentials.

What you do? Keep this email until your smartcard has been registered. Your software supplier will help the first two PSCs register their smartcards. (If you delete the email, speak to your bank to have it resent.)

Registration of digital certificate email

On each computer that you want to use your smartcard, you need...



The illustration shows a white smartcard reader with a cable, labeled 'Smartcard reader'. Below it is a screenshot of a 'Signing software' window with the text 'Please press the sign button STARTOFRANDOMTEXTESWDF' and an 'Enter PIN' field with 'Sign' and 'Cancel' buttons, labeled 'Signing software'.

... a smartcard reader attached to a computer that has signing software installed. This signing software “runs” your card reader.

Some banks provide you with a reader and the software, some only provide the software, and others do not provide either.

If your bank does not provide these, speak to your software supplier who should be able to provide them. (The signing software needed depends on your bank, your software supplier should have the details or your bank will let you know what you need.)

Whenever you need to digitally sign something using your software or the website, the signing software automatically opens. You must insert your smartcard in the reader (the chip must be inside the reader), and enter your PIN to sign the information.

What you do? Your software supplier will install the reader and signing software when they install your BACSTEL-IP software.

Notification emails

When your organisation is registered to use BACSTEL-IP, your PSCs get a series of emails from info@bacs.co.uk notifying them of certain things. Some of these emails are just for information purposes and others need to be actioned.

PSCs should check to make sure they get the following emails related to their service user. If a PSC is linked to more than one service user, then they will get these emails for each service user.

Email subject: BACS payment services – Service user registered

- You get this when your service user is registered to use BACSTEL-IP
- If you have been set up to access the dial-up extranet, then this has your extranet ID and password
- Keep this email so you have a record of your extranet ID and password (your supplier needs it for the installation).

Email subject: BACS payment services – Service user details update

- PSCs receive this email whenever there are changes made to their service user
- These emails are for information; however, you should read the emails, and if necessary check the updated details on the payment services website. If you have any concerns, speak to your bank
- After the installation and testing of your BACSTEL-IP software, you receive an email with this subject telling you that your software qualification plan has been set to live. This means that you can start using your software for live submissions.

Email subject: BACS payment services – New contact added/Contact linked to service user

- When an additional contact is added to your service user you receive a notification email. If the contact is already linked to another service user, and has just been linked to your service user, then you get a “Contact registration extended” email
- This email is for information.

The following emails go to all contacts (depending on their security methods)...

Email subject: BACS payment services – Registering your smartcard

- Each contact with a smartcard receives an email unique to them. This contains a web link so you can register your smartcard online
- **You must keep this email** until your smartcard has been registered. Your supplier will help the PSCs do this as part of the registration process. PSCs should then help any additional contacts with this process.

Email subject: BACS payment services – Your contact ID and password

- Each contact with ASM receives an email unique to them. This contains a web link so you can get your contact ID and password online
- **You must keep this email** until you have followed the process to get your contact ID and password. Your supplier will help the PSCs do this as part of the registration process. PSCs should then help any additional contacts with this process.

Email subject: Welcome to BACS payment services

- After a contact registers their smartcard and/or gets their contact ID and password, they get a welcome email
- This contains the web address for the payment services website. If you have both security methods, you will get two copies of this email.

From BACSTEL to BACSTEL-IP

If you are migrating from BACSTEL to BACSTEL-IP, you may want to keep your BACSTEL infrastructure in place until you have made one or two live submissions using BACSTEL-IP. After this, check that you...

■ Return any BACSAFE devices that you still have. Speak to your bank to arrange when these should be returned. When you do return them, send them to the Freepost address below:

Voca Limited
Customer Delivery
Freepost LOL 1954
Unit 17, Humphrys Road
Woodside Estate, Dunstable
Bedfordshire LU5 4TB

■ If you use a BT Dialplus connection for BACSTEL (and you do not use it for anything else), you should cancel this. More details and a cancellation form are available on www.bacstel-ip.com

What has changed?

Here are some things you may be familiar with in BACSTEL that have now changed.

Control points are no longer needed. The closest things in BACSTEL-IP are contacts. See Understanding BACSTEL-IP, The people, page 8.

Online acceptance/rejection advices have now been replaced with a more detailed submission summary report. After you have sent your submission using your BACSTEL-IP software, you get this report automatically. You can print it or save it. You can also check the payment services website to see if your submission was accepted and any errors that were found.

BACSAFE devices are no longer used. Security for submissions is handled using smartcards and HSMs. So you no longer need to generate a password or a transaction authentication number when you make a submission. See Understanding BACSTEL-IP, The security, page 7.

Emergency passwords can no longer be issued. Because security for submissions is provided using smartcards and HSMs digitally signing information, you can no longer contact your bank or the BACS service desk to get an emergency password. This means you must have at least two contacts with PKI credentials as well as other contingency measures. See Planning for contingency, page 13.

Printed reports are being replaced by electronic reports. You can now access your reports online using the payment services website or your BACSTEL-IP software and save them or print them. This means you get them faster. You can also access them in XML which means they can be uploaded into your own systems.

Glossary

<i>additional contact</i>	<i>A type of contact able to act for a service user on BACSTEL-IP. Additional contacts cannot be given any privileges to maintain their service user or other contacts.</i>
<i>alternative security method (ASM)</i>	<i>An access method using a contact ID and password to provide secure access to the BACS payment services website. (To do certain things on the website, you need to use PKI.)</i>
<i>BACS Approved Software Service for BACSTEL-IP</i>	<i>An approval service to make sure that all software used with BACSTEL-IP meets set requirements. You can only use software to access BACSTEL-IP that is approved under this service.</i>
<i>BACS payment services website</i>	<i>A secure website used by service users to get their reports, view their submission information and manage their contacts.</i>
<i>BACSTEL-IP</i>	<i>A service providing a secure access for the BACS service. It uses internet technologies and PKI security. You access BACSTEL-IP either using the BACS payment services website or BACS approved software for BACSTEL-IP.</i>
<i>BACSTEL-IP software</i>	<i>In this guide, BACSTEL-IP software refers to software that has been approved under the BACS Approved Software Service.</i>
<i>bureau</i>	<i>A bureau submits payment files to the BACS service for other service users. Bureaux that submit for third parties must be certified as a BACS Approved Bureau. A bureau is a type of direct submitter.</i>
<i>contact</i>	<i>A person that can act for a service user. There are two types of contacts: primary security contacts (PSCs) and additional contacts.</i>
<i>contact ID</i>	<i>This is used to identify a contact when they are logging on with the alternative security method (ASM). It is generated automatically and cannot be changed.</i>
<i>digitally sign</i>	<i>You digitally sign information using a smartcard or an HSM. This produces a digital signature that is attached to the file or message before it is sent. This digital signature allows the receiver to identify the sender and tell if the contents of the file or message have been altered after it was signed.</i>
<i>direct submitter</i>	<i>A service user that sends payment information directly to the BACS service. A direct submitter (that is not a bureau) also originates payment information.</i>
<i>hardware security module (HSM)</i>	<i>A piece of hardware installed into your computer systems that holds PKI credentials. HSMs allow you to automate the submission and report collection process.</i>
<i>indirect submitter</i>	<i>A service user that can originate payment information, but does not send it to BACS itself. It uses a bureau to send the payment information.</i>
<i>input report</i>	<i>A report that the BACS service produces following the processing of payment information for a particular service user for a particular day. Any payments that have been amended, rejected or returned are highlighted on the report. Using BACSTEL-IP, you can access input reports within 4 hours of processing.</i>
<i>modulus check</i>	<i>A process to check if a particular account number could exist at a given sorting code. BACSTEL-IP software modulus checks payment information before it sends it for processing.</i>
<i>payment file</i>	<i>A set of payment instructions that are submitted to the BACS service for processing. A payment file is sent as part of a submission. You can optionally digitally sign payment files.</i>

<i>primary security contact (PSC)</i>	<i>A type of contact linked to a service user. Service users must have at least two PSCs. A PSC can be given a wider range of privileges than an additional contact. Including the privilege to be able to add and maintain additional contacts.</i>
<i>public key infrastructure (PKI)</i>	<i>A system to verify the validity of parties involved in electronic communications and to secure electronic data transmissions. PKI uses two "keys": a public and a private key. A message encrypted with a private key can only be decrypted with the associated public key (and vice versa).</i>
<i>public key infrastructure (PKI) credentials</i>	<i>The collective term for the public and private keys issued to an individual in the form of a digital certificate. PKI credentials are used for authentication and encryption. They are issued by a trusted certificate authority.</i>
<i>service user</i>	<i>A company, group of companies, charity etc that is sponsored to use the BACS service.</i>
<i>service user number</i>	<i>A number allocated to a service user to uniquely identify it. A service user number is six numerals (or for a bureau, a B followed by five numerals).</i>
<i>smartcard</i>	<i>A card with an embedded microchip that is used to store a contact's PKI credentials. The smartcard is used to authenticate the holder and digitally sign data.</i>
<i>software suppliers</i>	<i>In this guide, software suppliers refers to companies that provide software approved under the BACS approved software service for BACSTEL-IP.</i>
<i>sponsoring bank</i>	<i>A bank or building society that can authorise service users to use the BACS service.</i>
<i>submission</i>	<i>A payment file or files transmitted to the BACS service for processing. All submissions sent to BACSTEL-IP must be digitally signed using PKI credentials.</i>
<i>XML (extensible markup language)</i>	<i>A computer language allowing data to be associated with instructions for processing the data. Reports on BACSTEL-IP can be accessed in XML format. This allows you to upload the reports into other applications.</i>