CODE AUTHENTICATOR

User guide

LLOYDS BANK

Contents

Introduction

With our Code Authenticator service you can securely authorise the requests you send to us. You'll use the Smart Card and reader to generate a unique authentication code, protected by the latest encryption technology.

Benefits

- You choose who can authorise instructions for your business.
- Payment details cannot be altered as they are embedded into the code.
- A full audit trail is available.

In this guide

- Definition of the two roles available, service administrator and user.
- Introduction to the Smart Card and reader.
- Instructions on generating the two types of code, payment and non-payment, to allow you to securely send instructions to us.
- Explanation of what types of instructions are accepted under which code.

Please note: the code verifies the originator of the request only and does not replace your bank mandate. All requests must still be signed in accordance with this mandate to enable us to act upon that request.

Service administrator

Role and responsibilities

The service administrator(s) will be the main point of contact within your business on matters connected with this service. We recommend that there are at least two people in this role to allow for cover should one be unavailable. Depending on the size of your business more may be required.

Service administrators are responsible for:

- Issuing cards to any individual registered with the service, including themselves.
- Completing and returning the card receipts so that the cards can be activated.
- Holding any additional cards securely until they are required.

They can:

- Generate authentication codes in the same way as any other user.
- Deal with queries we may have regarding the instructions we receive.
- Suspend or delete the card of another service administrator or user.
- Apply for additional user roles and maintain users within that role.
- Request replacement cards and readers.

Adding a new service administrator

If your business needs a new service administrator, including upgrading an existing user to that role, please ask for an application form from your service centre or business manager. This must be completed and signed, in accordance with your bank mandate, and returned to your usual point of contact within the bank (refer to page 13 for details).

Deleting and suspending service administrators

To delete a service administrator from this service, temporarily suspend their card or reinstate a suspended card, please telephone E-Operations.

Please note: your request will only affect the Code Authenticator service. If changes are required to your signing mandate, please contact your service centre or business manager.

User

Role

Users can generate authentication codes, which will confirm who sent the instruction to us.

Adding users

If a new user role is required, please ask for an application form from your service centre or business manager. Once completed by your service administrator, it should be sent back to E-Operations at the address shown on the form. A Smart Card should be issued to the new user from the stock held by the service administrator and the signed receipt returned with the application form.

We will send confirmation to the requesting service administrator once the user and card have been activated.

Deleting and suspending users

To delete a user from this service, temporarily suspend their card or reinstate a suspended card, a service administrator should telephone E-Operations.

Please note: your request will only affect the Code Authenticator service. If changes are required to your signing mandate, please contact your service centre or business manager.

Smart Cards

Issuing Smart Cards

A Smart Card should be issued to each person authorised by your organisation to authenticate instructions. The code generated enables us to identify which individual has authenticated the request.

A card will only be activated once the card receipt is authorised by a service administrator and returned to us for activation by E-Operations.

Ordering replacements

The service administrator(s) should maintain the stock of spare, unassigned cards. Depending on your organisation's usage and turnover of cards, a request for new cards should be made before the last card is issued. To do this, a service administrator must obtain an order form from your service centre or business manager.

Reader

The reader can be shared between users who are authorised to generate codes. They have been designed to work with several of the services provided by us and so there are certain functions the reader can perform which are not applicable for the Code Authenticator service.

Checking battery life

In normal use, the battery life will be between three and five years, after which time the reader will need replacing. It is possible to obtain a reading of the remaining power of the battery, which is shown as a percentage. Periodically, please carry out the following:

- Turn on the reader by either inserting your card or pressing the blue button in the bottom left-hand corner.
- When prompted, press the Menu button twice. Test Battery will be displayed on the screen. Press OK.
- The percentage of remaining battery power will be displayed in the bottom right-hand corner.
- If the reading is shown as 7% or less please order a replacement reader.

The reader is a sealed unit and no attempt should be made to disassemble it. Readers and Smart Cards are the property of Lloyds Banking Group and should not be used other than in accordance with this user guide.

Ordering a replacement

To request a new or replacement reader, your service administrator should obtain an order form from your service centre or business manager.

PIN

The first time you enter your card into a reader, you will be prompted to choose a PIN. This must be between six and 12 digits long and something easily remembered by you but not easily guessed by others.

Please note: after choosing your PIN, if it is entered incorrectly three times in a row, the card will become invalid and need replacing from the stock held.

Setting your PIN

- Insert your card into the reader in the direction indicated on the card.
- New PIN will be displayed on the screen. Enter your chosen PIN (between six and 12 digits) and press OK.
- Confirm PIN will be displayed on the screen. Re-enter your chosen PIN and press OK.
- The reader will now confirm that your PIN has been accepted and will display a PIN accepted message.

If you enter a wrong digit, you can simply press the C button to delete it. Wrong PIN will be displayed if an invalid PIN has been entered.

Changing your PIN

You may change your PIN at any time. To do this:

- Insert your card into the reader in the direction indicated on the card.
- When prompted, press the Menu button four times. Change PIN will be displayed on the screen. Press OK.
- Old PIN will be displayed on the screen. Enter your current PIN and press OK.
- New PIN will be displayed on the screen. Enter your new PIN (between six and 12 digits) and press OK.
- Confirm PIN will be displayed on the screen. Re-enter your new PIN and press OK.
- The reader will now confirm that your new PIN has been accepted and will display a PIN Accepted message.

If you enter a wrong digit, you can simply press the C button to delete it.

Please note: your new PIN cannot be the same as the one it is replacing. Weak PIN will be displayed if the same PIN has been entered.

Security and risks

Please be aware that fax is not a secure method of contacting us. A fax may be intercepted, giving someone outside your organisation access to confidential information. It is not possible for us to know whether a signature on a fax is genuine. Please see section two of the original application form for further details.

Please choose your PIN carefully and never write it down. If you think someone else knows your PIN, change it immediately as described in the previous section.

It is the cardholder's responsibility to keep their card safe and secure. Any lost or stolen cards should be reported immediately, via a service administrator, to E-Operations.

Generating codes

There are two types of code that can be generated using the Smart Card and reader: payment and non-payment. The code confirms that the individual creating that particular code can authorise instructions on behalf of your organisation.

Please note: all requests must be signed in accordance with your bank mandate.

Payment codes

Payment codes must be used when requesting a transfer to other accounts (e.g. CHAPS or international payments to a third party) or a Sterling or international draft.

Before generating your code, first complete our standard request form, as you will require information from it to produce the code.

- Insert your card into the reader in the direction indicated on the card.
- When prompted, press the Menu button once. Press OK.
- 1 Payment will be displayed on the screen. Press OK.
- The screen will display Currency. Enter the two-digit currency code relevant to your request (as shown in the Currency code section) and press OK.
- On the Amount screen, enter the amount in whole units only, e.g. 46,859.65 should be entered as 46,859. Do not round the figure up. Press OK.
- Your A/C will be displayed on the screen. Enter a minimum of eight digits from the account number to be debited. Please include any leading zeros. Press OK.

- Payee A/C is then displayed. Enter the first 12 digits (or less if applicable) of the receiving customer account number or international bank account number (IBAN)*. Starting from the left, you should leave out any letters and enter numbers only. For example, the IBAN IE29 AIBK 9311 5212 H 3456 78 should be entered as 299311521234. Press OK.
- Enter your PIN and press OK.
- Your unique eight-digit authentication code will be displayed. This code is valid for seven days.

Please note: your request must include your user name, the code itself and the date the code was generated. Please clearly print this information on your instruction to us.

* Where a payment is to be sent via a forwarding account and two (or more) beneficiary accounts are used, please use the account number of the ultimate beneficiary when generating the code. For drafts and certain international payments a payee account number may not be applicable. In these cases leave this field blank and press OK. Remember, if a payee account appears on your request to us, it must be included as part of the code.

Non-payment codes

Non-payment codes must be used when requesting us to carry out certain instructions on your organisation's behalf. A list of the types of instructions that require a non-payment code are listed below.

- Insert your card into the reader in the direction indicated on the card.
- When prompted, press the Menu button once. Press OK.
- 1 Payment will be displayed on the screen. Press the Menu button again and 2 Non-payment will appear. Press OK.
- Enter your PIN and press OK.
- Your unique eight-digit authentication code will be displayed. This code is valid for seven days.

Please note: your request must include your user name, the code itself and the date the code was generated. Please clearly print this information on all instructions sent to us.

The following instructions require a non-payment code:

- Application for or amendment to guarantees.
- New or increased standing order instruction.
- New card request (e.g. Visa debit card, Business Charge Card).
- Remove stop cheque(s).
- Application for or amendments to Trade Finance guarantees.
- Application for or amendment to import letter of credit.
- Application for or amendment to standby letter of credit.
- Instructions in connection with a Trade Finance transaction.
- Requests for account information to be sent to any other address.
- Statement request to be sent to another address.
- Cheque book request to be sent to another address.
- Purchase and sale of investments.
- Instructions to buy and sell currency.
- Certain requests relating to the Code Authenticator service.

Currency codes

—— 🪙 ——

Part of the information you need to enter into the reader to generate a payment code is a currency code. This forms an integral part of the code and enhances the security of your request. The 12 most commonly used currencies have each been allocated a two-digit code as listed below. If the currency you are sending does not appear here, please use 99 for Other when producing your code.

Currency codes		
Full currency name	**Currency**	**Two-digit code**
Sterling	GBP	05
Euro	EUR	10
US Dollars	USD	15
Swiss Francs	CHF	20
Swedish Kronor	SEK	25
South African Rand	ZAR	30
Japanese Yen	JPY	35
Australian Dollars	AUD	40
Danish Kroner	DKK	45
Hong Kong Dollars	HKD	50
Canadian Dollars	CAD	55
New Zealand Dollars	NZD	60
All other currencies	OTHER	99

Please note: when requesting a payment in currency equivalent of Sterling, please use the currency code for Sterling.

Contact points

For any queries concerning your instruction or if you have any questions about this service please speak to your usual point of contact within the bank.

This should be your service centre or business manager for Commercial Banking and business customers. If known, your service centre should be the primary contact point for this service.

The E-Operations helpdesk should only be telephoned to report a lost or stolen card or in the event of you requiring the suspension, reinstating or deletion of a service administrator or user from the service. They will be unable to assist you in any other queries relating to the Code Authenticator service or your account(s).

Get in touch

Go to lloydsbank.com/commercialbanking

Contact your relationship manager

Call E-Operations on 0870 900 2070
9am–5pm, Monday to Friday. If you have an urgent administration request outside these hours, please fax your instruction supported by a non-payment code to +44 (0) 870 0 100 261 where it will be actioned the following working day.

Please contact us if you would like this information in an alternative format such as Braille, large print or audio.

If you have a hearing or speech impairment you can use Text Relay (previously Typetalk).

Important information
Calls may be monitored or recorded in case we need to check we have carried out your instructions correctly and to help improve our quality of service.

Lloyds Bank plc. Registered Office: 25 Gresham Street, London EC2V 7HN. Registered in England and Wales No. 2065. Telephone: 020 7626 1500. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority

The Lloyds Banking Group includes companies using brands including Lloyds Bank, Halifax and Bank of Scotland and their associated companies. More information on the Lloyds Banking Group can be found at lloydsbankinggroup.com

LLOYDS BANK