Lombard Internet Banking Software Token Operating Instructions

Software Token Activation

1

2

3

4

A software token is for use on an Android or iOS mobile phone and is used to generate Security Codes to login and to authenticate transactions executed from the Lombard Internet Banking Service. It can also be used to authorise on-line card transactions using biometrics.

Application for a software token may be made in person at any one of our branches— if you are not a subscriber to the Lombard Internet Banking Service you will need to submit an application and a Login ID will be issued once the application has been processed.

Download and install the *Lombard Mobile Token* from the Google Play Store or iOS App Store.

Please enter the SMS password you received

Continue

SMS Password *

Back to login

Using a PC or laptop, visit the Bank's website at: https://www.lombardmalta.com/ and click on 'Internet Banking Login' > 'Software Token Activation'. The Mobile token activation window will be displayed. Proceed to enter the details required and click on 'Activate mobile token'

lobile token activation

India	Please fill the below fields
	Login ID *
	would phone (starting with +) *
	ID Card or Passport *
	Back to login
	Activate mobile token
_	

- You will receive an 8-digit password via SMS on your mobile phone.
- Enter this 8-digit password in the 'SMS Password' text box on your PC/laptop.
- Click on the '*Continue*' button.

Please scan OR code or enter the below activation data manually for offline activation using your mobile token Serial Number FDU Activation Code:28136847760426250771368241008521397346833 IMPORTANT: Please enter the mobile token generated number below
Mobile token generated number * Back to login Continue



		-
15:17 +	ali 46 💼	
Serial number	OK	
FDU!	Ма	nual
Enter your activation code.		
Authorisation Code		
Confirmation Authorisation Code)	
Confirm your Authorisation Code		

From the Lombard Mobile Token app select an activation method:

- either by entering details manually
- or by scanning QR code



7

5

You will next be required to CREATE an Authorisation Code – a personal password/PIN. This must be memorised for future use.

Should your device support biometric protection you may enable this on the Lombard Mobile Token app.

As displayed below, the Mobile token generates a number, 'Your Mobile Token generated number is:





This number is to be entered on your PC/laptop in the field – 'Mobile token generated number' 'Your token has been successfully activated' will be

displayed on your PC/laptop. At this point, your Lombard Mobile Token app is activated

and ready to use.



Generated One Time Password

782374

Serial number

Cone Time Password/A

Challenge Signature/A

Touch ID for "Lombard Mobile Token"

authenticate using fingerp rition to protect your DIGIP/ Cancel

Logging in & Signing APPLI 1 Transactions

8

Using your mobile app, follow the below steps:-

0

ture/APPLI 2

tion Data Signing

- 1. Select the One Time Password / APPL 1
- 2. Enter Authorisation Code

One Time Password/APPLI 1

3. Mobile will generate a 6-digit One-time password (OTP).

On your PC/laptop, input the Login ID and the generated password on the Lombard Internet Banking login window > 'Security Code' field, to access the Lombard Internet Banking portal.

Lombard Internet Banking Service

Login ID: * xxxxxx Security Code: *

se enter your Login ID and Security Code

Signing A	APPLI	2 T	ransa	ction	S

C

The second option on the screen 'Challenge Signature/APPLI 2 is used to authorise financial transactions. Please enter this number to your Token in APPLI 2 mode:	App App One Time Challenge	1234 The second	all genetike Uts test and tes
 Once transaction details have been inserted, click on 'Continue' A 6-digit number (challenge) will be displayed on your screen. On your mobile app, select 'Challenge Signature/APPLL2' and 	,		Generated Security CODE:
 enter this 6-digit number. A security code (challenge response) will be generated and displayed on your mobile screen. 3. Enter this code in the relevant field on your PC/laptop to authorise your transaction. 		1 2 3 4 5 6 7 - / : ; () £ #** - , ? ! ABC & space	032000
		L	Remaining time

Authorising Card Transactions using Biometrics.

10

The final option on the screen is '*Transaction Data Signing*' This option is used to authorise on-line card transactions using biometrics (e.g. fingerprint, face recognition).

Once you reach the online checkout and input your card details, the following pop-up window may be presented.

	Cancel
LOMBARD	ID Check.
Payment S	Security
For added security use you for transaction authentication	r Lombard Mobile Token on
Open the Lombard Mobile Select "Transaction Data S	e Token application. igning"
Authenticate by using you biometric	r authorisation code or
Select the transaction from approve it; you will be promyourself again	n the list. Press OK to pted to authenticate
press CONTINUE	
CONTI	NUE
	•

If so, follow the instructions on the pop-up window and open the Lombard Mobile Token and selecting "*Transaction Data Signing*".



This process will trigger the Mobile Token to list the transactions to be authorised. '*Retrieving transactions please wait*' will appear on your mobile. Once the system retrieves the transactions, select the one to be authorised (if more than one transaction requires authorisation), the '*Transaction Data Signing*' screen will be displayed.

Should you wish to proceed with authorising the transaction, tap on '*Proceed to Authorise*'. A screen will be displayed to enable either 'Fingerprint Recognition' or 'Face Detection'.

	47.78 4
0803 0 0 17 • 5 4 1 0	07.50
Transaction Data Signing	
#53+++++2553	
marchant	Good morning,
Purchase Amount	
Reject transaction Proceed to authorise	
Please authenticate using fingerprint recognition	(2)
Fallback Cancel	Face ID
and the second se	1000.00
	Forgot your passcode?
III O <	



Once the above is finalised, go back to the payment page and Press CONTINUE to complete the process.



You may also opt to Cancel the transaction from the top righthand corner of the payment page or reject the transaction from your mobile. Once you select '*Reject Transaction*' from your mobile, '*Transaction Rejected Successfully*' will appear. You need to press 'OK' to continue. In both cases, the payment shall not be effected.

If the above procedure is not followed, the payment page will expire. You may either follow the procedure again or opt to enter the Static Password and One Time Password (OTP).

12