User Guide

User Authentication

January 2013

Disclaimer

This document is issued by HSBC Bank plc ('HSBC'). HSBC is authorised and regulated by the Financial Services Authority and is a member of the HSBC group of companies ('HSBC Group').

This document is for information purposes only and does not constitute or form any part of (i) any invitation or inducement to engage in investment activity, or (ii) any offer, solicitation or invitation by HSBC or any of the HSBC Group for the sale or purchase of any products, services and/or any investments.

HSBC provides this document to the recipient on an 'as is' basis and except as provided herein, does not warrant that the contents of this document is accurate, sufficient or relevant for the recipient's purposes.

HSBC may have obtained information in this document from sources including from third party suppliers, it believes to be reliable but which have not been independently verified. In relation to information on products and/or services supplied by a third party supplier, the recipient should obtain further information on these products and/or services directly from the supplier.

Please note that this document may contain hypertext links to websites operated by other members of the HSBC group and third parties respectively. In relation to hypertext links to websites operated by members of the HSBC group, please read the terms and conditions of the linked website. In relation to hypertext links to websites operated by third parties, please note that: (1) the recipient should read the terms and conditions of the website; and (2) HSBC does not have any control whatsoever over these websites and shall not be liable for the recipient's use of them.

HSBC will use its reasonable endeavours to ensure that the contents of this document are current at the date of its first publication. HSBC gives no undertaking and is under no obligation to provide the recipient with access to any additional information or to update all or any part of the contents of this document or to correct any inaccuracies in it which may become apparent.

HSBC is not responsible for providing the recipient with any legal, tax or other advice regarding the contents of this document and the recipient should make its own arrangements in respect of this accordingly. This document has not been prepared to address the specific requirements or objectives of any particular client. The recipient is solely responsible for making its own independent appraisal of an investigation into the products, services and other content referred to in this document.

This document should be kept confidential and shall be used for internal business purposes only by the recipient to whom it is provided and its officers, employees and agents. This document should be read in its entirety and shall not be photocopied, reproduced, distributed or disclosed in whole or in part to any other person without the prior written consent of the relevant HSBC Group member. This document is proprietary to HSBC and the recipient agrees on request to return or, if requested, to destroy this document and all other materials received relating to the information contained herein.

Except in the case of fraudulent misrepresentation and/or breach of these terms, no liability is accepted whatsoever by HSBC and the HSBC Group for any direct, indirect or consequential loss arising from the use of this document.

Please contact your local HSBC representative for further information on the availability of products and/or services discussed herein in your region.

Contents

About User Authentication

Types of Authentication Profiles

Depending on their location/institution, all HSBC*net* customers are allowed to choose one of two authentication profiles:

- Mixed Security profile
- One-time-password/Security Device profile

Customers with **Mixed Security** profile have the option to assign one of three authentication types to their Users during the initial setup – **One Time Password** (also called Security Device), **Smart Card**, or **Password Only**. Under this profile, Users who are entitled to transactional tools must be assigned a Smart Card or Security Device. If the User is only entitled to enquiry tools (such as Balance and Transaction Reporting, Reports and Files Download etc.) they are set up as Password Only Users. They can log on to HSBC*net* only using their password and memorable answer.

Customers with **One-time-Password** (Security Device) profile must assign a Security Device to all their Users even if they are only entitled to conduct enquiries.

HSBC*net* security

HSBC*net* offers a reliable and secure online environment by adopting best-in-class technologies, proven best practice IT policies and procedures and the dedication of expert resources. HSBC*net* employs industry-standard solutions to authenticate your identity when you log on to ensure that your data is transmitted securely and reliably and that the customer data the Bank holds is protected. HSBC*net* has backup and contingency plans to ensure interruptions to the service, for whatever reason, are minimised.

Drawing on the Bank's considerable experience as providers of secure electronic banking systems, HSBC*net* also operates a control and support structure designed to ensure that the Bank addresses all aspects of the risks faced in providing transactional banking online.

Key features

- Robust authentication processes
- Two-factor authentication using one-time-password generating Security Devices or Smart Cards, ensuring identification integrity and mitigating key-logging and denial-of-service risks **on user credentials**
- Encrypted sessions between customer and the Bank (SSL v3 128 bit)
- Protection of sensitive information in transit and storage to ensure confidentiality of customer data
- Industry-standard security mechanisms to protect the infrastructure
- Regular independent reviews of system security
- Robust and regularly reviewed information security policies covering systems and installation development and management
- Comprehensive contingency and backup arrangements
- 24/7 security monitoring and centralized incident management team

- Audit trails for administrative and transactional activities

Two-factor authentication

HSBC*net* uses a two-factor authentication approach to help ensure your banking security:

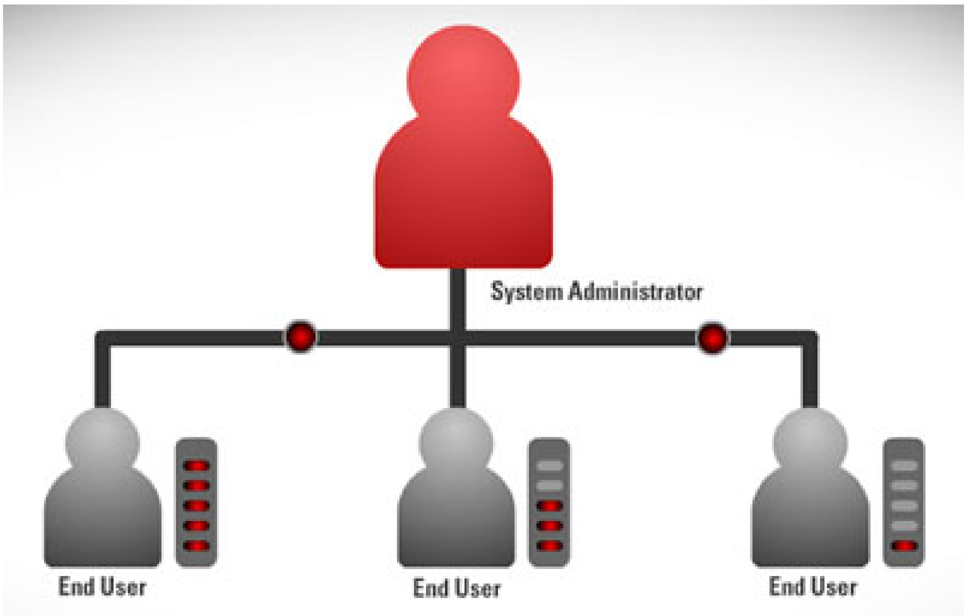
1. A username and password combination chosen by the User at Registration

2. a. Smart Card with a microchip that identifies the User when the card is inserted in a Smart Card reader, or
   b. Security Device token that generates unique passcodes as the User requires them

Access control

Most importantly, HSBC*net* puts you in control of your internal security with flexible administration tools to make your online experience efficient and secure. Whether your organisation is large or small, you have the opportunity to tailor the system to align with your corporate, compliance and audit needs.

At the heart of HSBC*net* are the actions of your designated System Administrators, who determine what each staff member is allowed to see and do on HSBC*net*. From payment clerks to senior accountants, your System Administrators decide who receives specific functionality. By managing access to tools and report options, you can streamline internal processes and improve your operational efficiency.



Adding new Users to HSBC*net* is easy. System Administrators provide them with a quick step-by-step registration process. HSBC*net* features flexible options for adding new Users, including copying specific access entitlements from existing Users.

You can also access information on who is using the system, at what time and for what activity. These details are time and date stamped to help simplify your audit process.

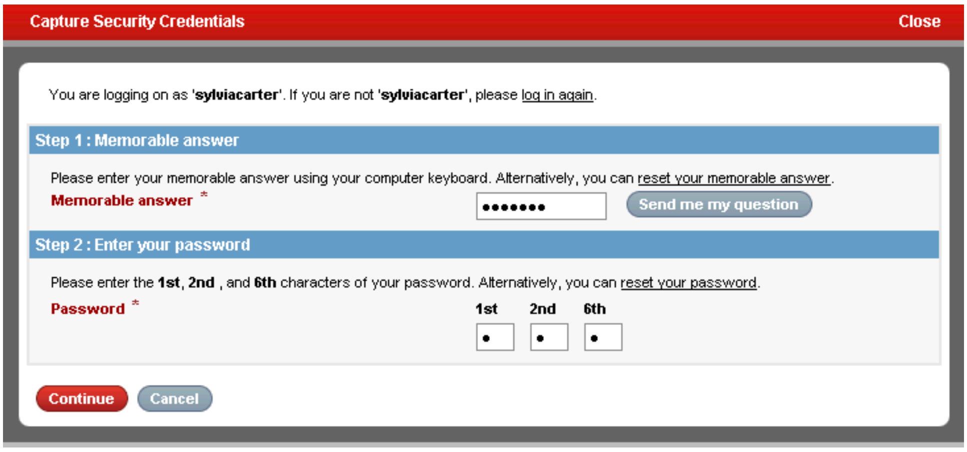
HSBC*net* security levels

In order to protect your banking information, HSBC*net* provides the following levels of security.

Initial log on: At this security level, you must enter your username on the HSBC*net* home page, including:

- Your memorable answer, and
- Three requested characters of your current password

Initial Logon Authentication page



You are logging on as '**sylviacarter**'. If you are not '**sylviacarter**', please log in again.

Step 1 : Memorable answer

Please enter your memorable answer using your computer keyboard. Alternatively, you can reset your memorable answer.

Memorable answer * ●●●●●●●

Step 2 : Enter your password

Please enter the **1st**, **2nd** , and **6th** characters of your password. Alternatively, you can reset your password.

Password * **1st** ● **2nd** ● **6th** ●

Session validation: At this level of security, you must enter the combination of:

- Your username
- Your memorable answer and the three requested characters of your current password (only for Smart Card Users or Password only Users)
- Your Security Device PIN (only for Security Device Users)

Authorise transactions and administrative changes: At this security level, you must enter your Smart Card or Security Device personal identification number (PIN) and select **OK**.

The following are some HSBC*net* User tools and services that require authentication.

- HSBC*net* log on
- Payment creation and authorisation
- Administrative setup and change approval
- File Upload
- Internet Trade Services (ITS)
- e-Securities (Transaction Entry)

User-level Security guidelines

Basic common sense and adherence to the following security guidelines can help ensure that your information remains safe and secure.

- Keep your password, memorable answer, security answers and PIN secure and secret at all times
- Never write or otherwise record these credentials or reveal them to anyone else
- Promptly destroy any PIN advice from the Bank or other parties
- Avoid passwords, PIN or memorable question and answer combinations that may be easy for others to guess

- Never record passwords, memorable answer, security answers or Smart Card/Security Device PIN on any software that can store it automatically (for example, computer screen prompts or save password features on internet browsers)
- Ensure that others are unable to read your screen or that you are not being monitored by closed circuit TV while logging on to the system
- Change your initial PIN upon receipt. Change your password and PIN on a regular basis. Do not alternate between the same pair of passwords
- Never disclose your password, memorable answer or PIN to HSBC staff. Be cautious of any correspondence or communication requesting the disclosure of your passwords or any bank account details. Report any suspicious correspondence or communication to HSBC
- Never leave your Smart Card or Security Device unattended. Always keep it securely locked up when not in use
- Never share your authentication device with other colleagues.

Organisation-level Security guidelines

At your organisational level, consider the following security guidelines.

1. Enhance the security of your computer and networks to protect against malicious software.

Minimize the number of, and restrict the functions for, computer workstations and laptops that are used for online banking and payments. A workstation used for online banking should not be used for general web browsing, e-mailing, and social networking. Conduct online banking and payments activity from at least one dedicated computer that is not used for other online activity.

2. Install and maintain real-time anti-virus and anti-spyware desktop firewall and malware detection and removal software.

Use these tools regularly to scan your computer. Allow for automatic updates and scheduled scans.

- Install security updates to operating systems and all applications, as they become available. These updates may appear as weekly, monthly, or even daily for zero-day attacks.
- Block pop-ups.
- Keep operating systems, browsers, and all other software and hardware up-to-date.
- Do not use public Internet access points (e.g., Internet cafes, public wi-fi hotspots (airports), etc.) to access accounts or personal information. If using such an access point, employ a Virtual Private Network (VPN).

3. Enhance the security of your corporate banking processes and protocols

Initiate payments under dual control using two separate computers. For example: one person authorizes the creation of the payment file and a second person authorizes the release of the file from a different computer system.

4. Monitor and reconcile accounts at least once a day

Reviewing accounts regularly enhances the ability to quickly detect unauthorized activity and allows the business

5. Note any changes in the performance of your computer such as:

- A dramatic loss of speed.
- Changes in the way things appear.
- Computer locks up so the user is unable to perform any functions.
- Unexpected rebooting or restarting of your computer.
- An unexpected request for a one time password (or token) in the middle of an online session.
- Unusual pop-up messages.
- New or unexpected toolbars and/or icons.

Smart Card Guide

About Smart Cards

Your company provides Smart Cards in order to securely set up Users and authenticate their transactions on HSBC*net*.

HSBC*net* System Administrators are responsible for ordering, setting up and managing Smart Cards for all Users in their company.

Note: Images in the Smart Card Guide may not be exactly as you see them on HSBC*net*.

Before you begin

When setting you up as a User, your HSBC*net* System Administrator must entitle you with access to tools and services, and order a Smart Card. The Smart Card is required to validate your username in certain circumstances such as initiating and authorising administrative changes, creating and authorising payments, etc. Depending on the setup at the User access level, you may be entitled to different roles as a User.

PIN-protected Smart Card

Using Smart Cards

This section is intended for Smart Card users. The following are some of the HSBC*net* tools and services requiring Smart Card authentication:

- User Management
- User Authorisation Summary
- Managing HSBC*net* Accounts
- Payment creation and authorisation
- Initiating and authorising entitlement changes
- File Upload
- Internet Trade Services (ITS)
- e-Securities (Transaction Entry)

Note: For customers with Mixed Security Profiles, if any of their Users are only entitled to enquiry tools such as Balance and Transaction Reporting, Reports and Files Download, etc. they do not need a Smart Card to log on to HSBC*net*.

Using your Smart Card

To authenticate yourself on HSBC*net*, insert your Smart Card into the reader and enter your PIN. If your Smart Card is inserted correctly, the light on the reader displays solid green (not blinking).

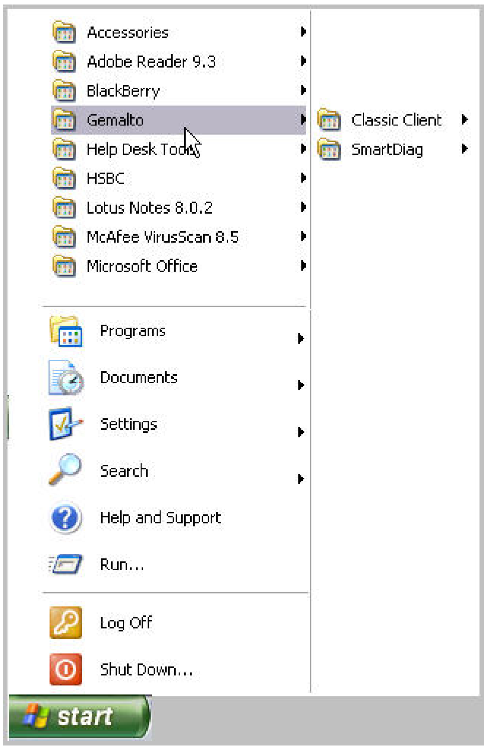
Smart Card inserted in reader

Changing your Smart Card PIN

To change your Smart Card PIN, complete the following steps:

1. Insert your Smart Card into the reader.

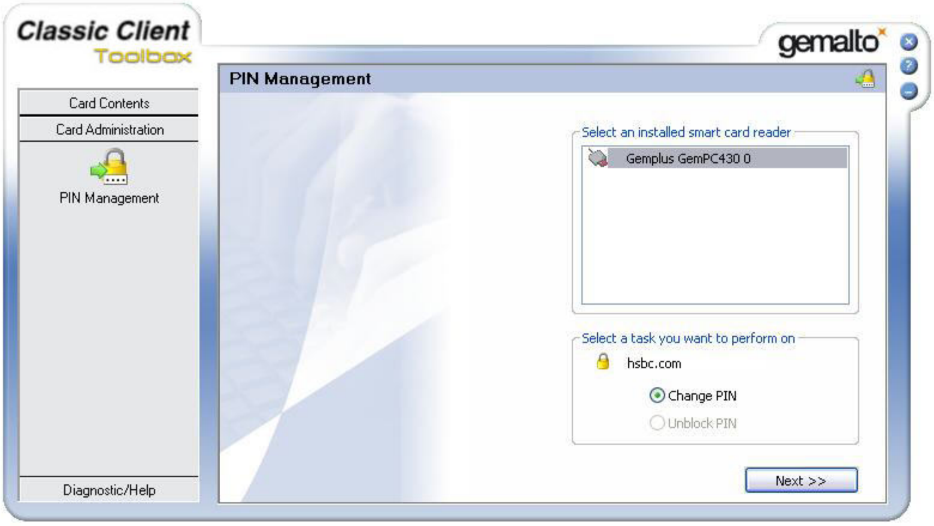
2. Open Classic Client Toolbox in your start or programs menu.



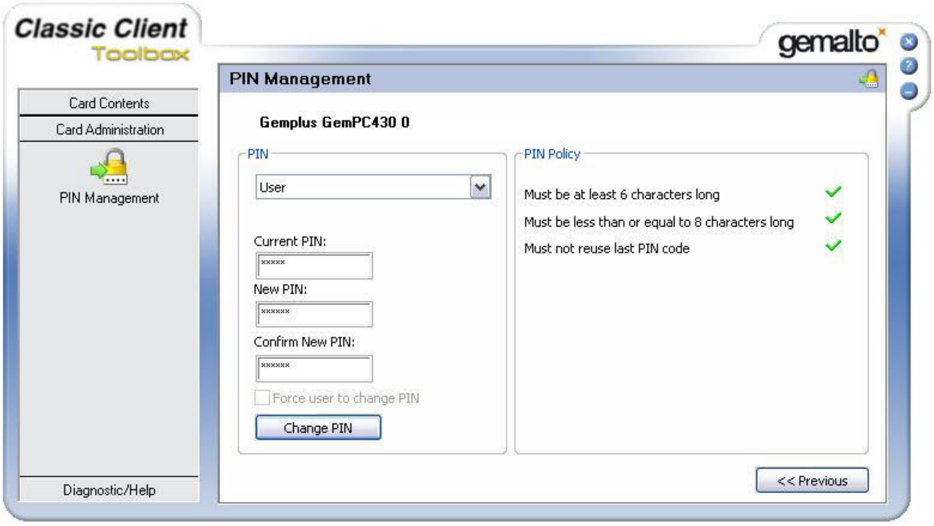
3. In the Classic Client Toolbox, under Card Administration, select **PIN Management**.

Under **Select an installed Smart Card reader**, select the name of your card reader.

Under **Select the task you want to perform on**. Select **Change PIN**. Then select **Next**.



4. Enter the old new PIN and confirm the new PIN.



PIN Management

Gemplus GemPC430 0

PIN

User

Current PIN: *****

New PIN: ******

Confirm New PIN: ******

□ Force user to change PIN

PIN Policy

Must be at least 6 characters long ✓

Must be less than or equal to 8 characters long ✓

Must not reuse last PIN code ✓

5. For the new PIN, review the PIN Policy Rules for any unchecked rules. All rules must be checked (✓) in order to proceed. Enter the new PIN as necessary.

6. Select **Change PIN**.

Important: If you lose or forget your PIN, you will need a new Smart Card.

Registering your Smart Card

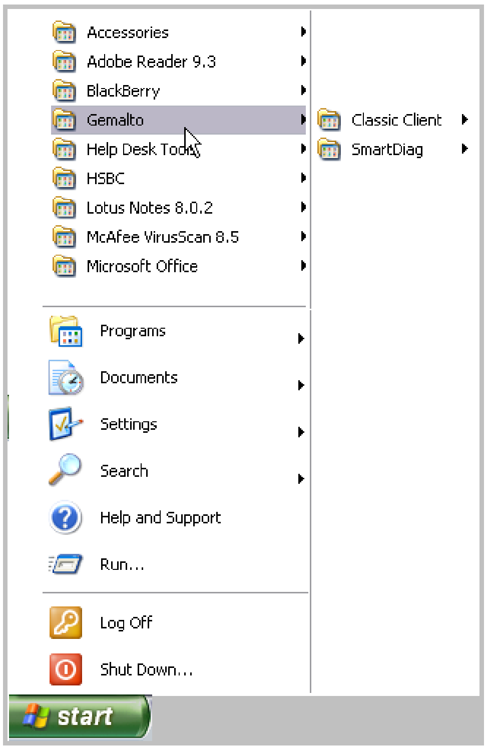
Before you can use HSBC*net*, the system requires that you register your new Smart Card. To register Smart Cards, you will need:

- Smart Card software and card reader installed on your computer (software CD and reader are shipped with the Smart Card)
- Smart Card PIN (sent separately to you by mail/courier). If you did not receive your PIN, contact your System Administrator

To register your Smart Card on your computer, complete the following steps:

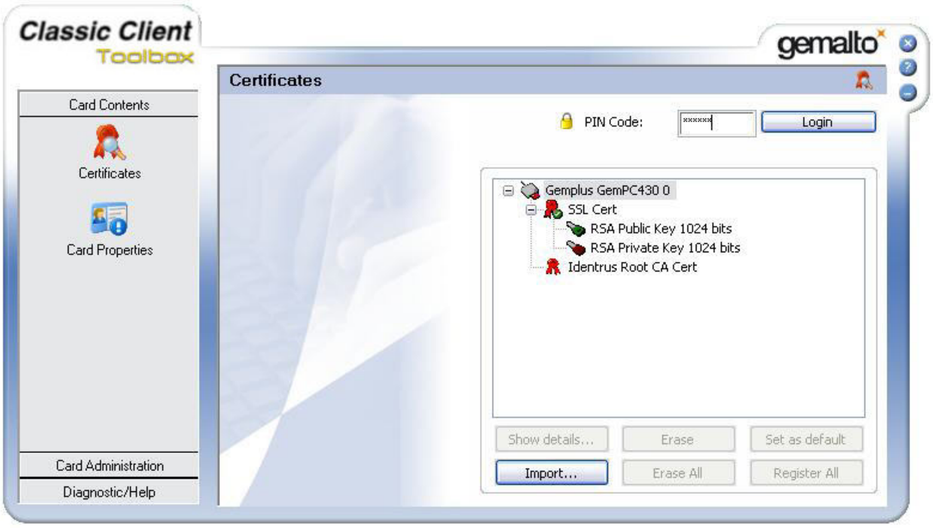
1. Insert your Smart Card into the reader.

2. Open Gemalto, Classic Client Toolbox in your start or programs menu.



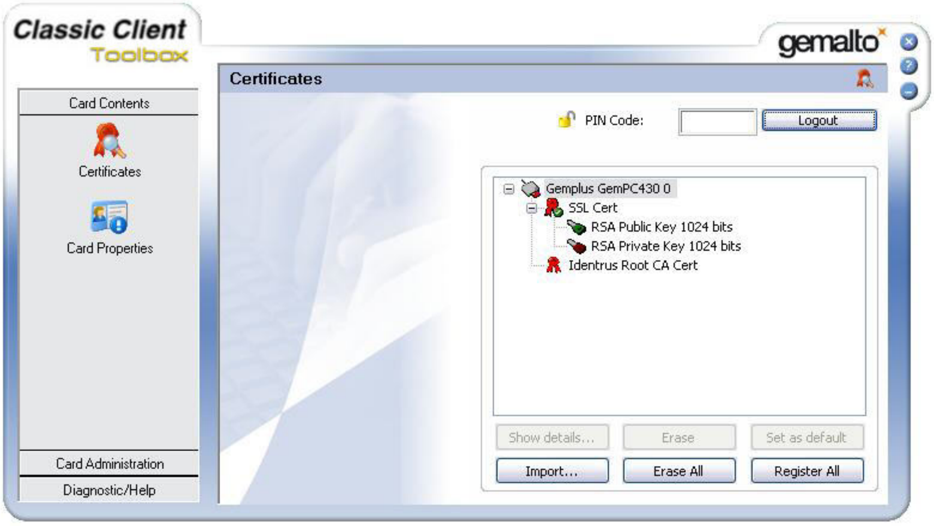
3. In Classic Client Toolbox, under Card Contents, select **Certificates**.

4. In the Card Contents - Certificates page, enter the PIN that was mailed to you and select **Login**.



.

5. When your PIN is accepted, select **Register All** (this option is not available until your PIN is accepted).



Gemplus GemPC430 0
SSL Cert
RSA Public Key 1024 bits
RSA Private Key 1024 bits
Identrus Root CA Cert

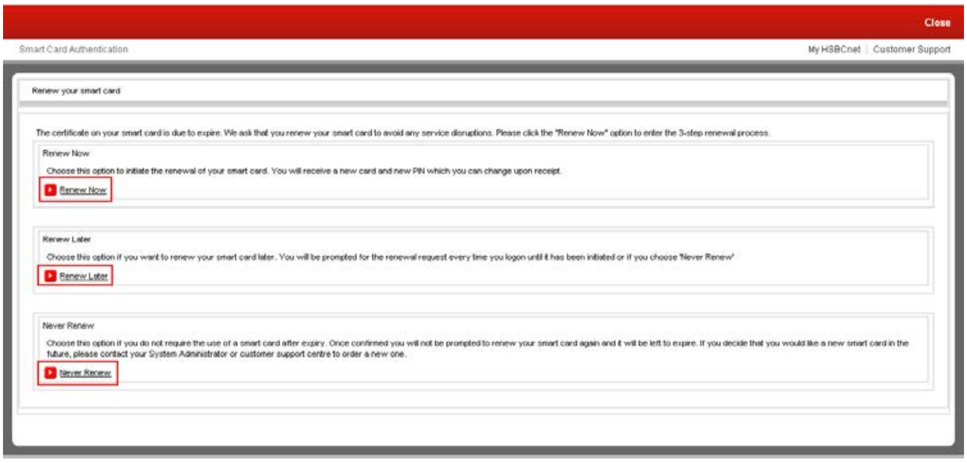
.

You have successfully registered your Smart Card.

Renewing Your Smart Card

This section applies to all types of Users. For security reasons, HSBC*net* Smart Card certificates have three-year validity. Forty-five days before your card expires, a Smart Card renewal window appears when you log on to HSBC*net*. This window offers the following options to the reader:

- **Renew now—**select to initiate the renewal process and a new Smart Card and PIN will be ordered
- **Renew later—**select to have HSBC*net* prompt you to renew your Smart Card every time you log on
- **Never renew—**select when you no longer need a Smart Card when using HSBC*net* (e.g. if you are only checking account balances and not authorising transactions or making administrative changes)



Renew your smart card

The certificate on your smart card is due to expire. We ask that you renew your smart card to avoid any service disruptions. Please click the "Renew Now" option to enter the 3-step renewal process.

Renew Now

Choose this option to initiate the renewal of your smart card. You will receive a new card and new PIN which you can change upon receipt.

Renew Now

Renew Later

Choose this option if you want to renew your smart card later. You will be prompted for the renewal request every time you logon until it has been initiated or if you choose 'Never Renew'

Renew Later

Never Renew

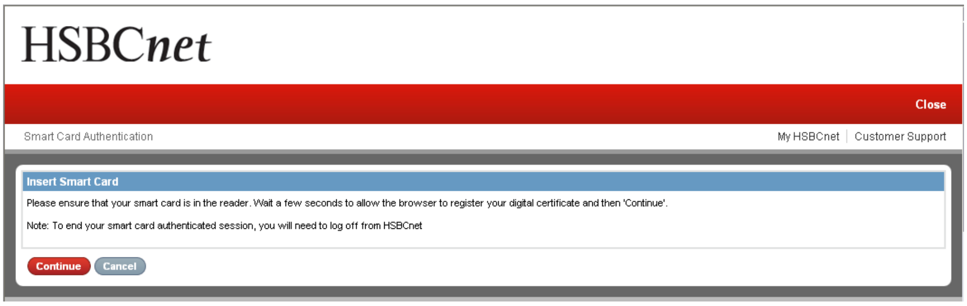
Choose this option if you do not require the use of a smart card after expiry. Once confirmed you will not be prompted to renew your smart card again and it will be left to expire. If you decide that you would like a new smart card in the future, please contact your System Administrator or customer support centre to order a new one.

Never Renew

Renew now

Select **Renew now** to initiate the renewal of your Smart Card. You will receive a new Smart Card and new PIN.

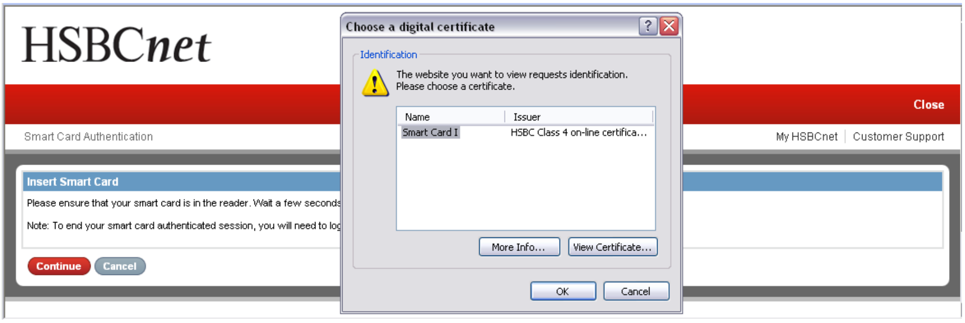
1. Insert your Smart Card and complete the authentication process.



Please ensure that your smart card is in the reader. Wait a few seconds to allow the browser to register your digital certificate and then 'Continue'.

Note: To end your smart card authenticated session, you will need to log off from HSBCnet

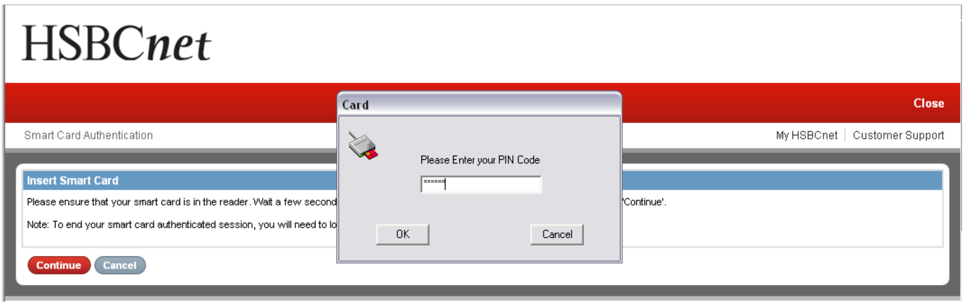
2. Select your Smart Card certificate and select **OK** to proceed.



The website you want to view requests identification. Please choose a certificate.

Name	Issuer
Smart Card I	HSBC Class 4 on-line certifica...

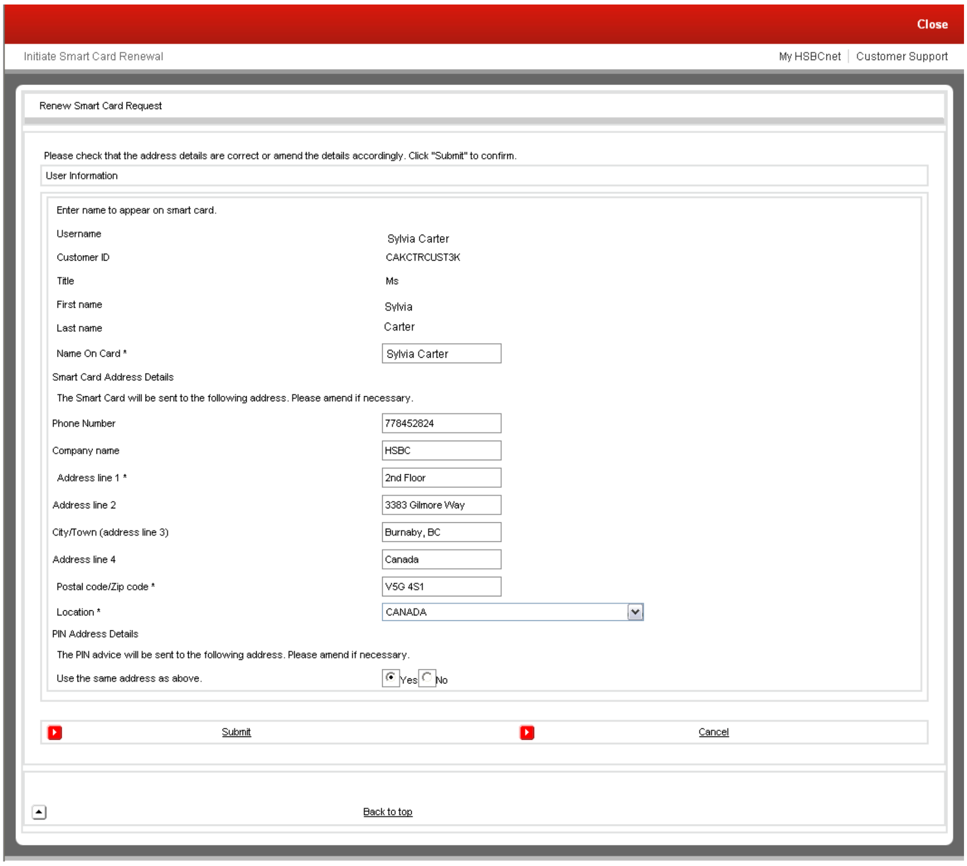
3. Enter your PIN and select **OK** to access the Renew Smart Card request page.



Please Enter your PIN Code

******

4. Complete the mandatory fields marked with an asterisk (*). Ensure that your mailing address is correct, as the new Smart Card ships to this address.



Renew Smart Card Request

Please check that the address details are correct or amend the details accordingly. Click "Submit" to confirm.

User Information

Enter name to appear on smart card.

Username	Sylvia Carter
Customer ID	CAKCTRCUST3K
Title	Ms
First name	Sylvia
Last name	Carter
Name On Card *	Sylvia Carter

Smart Card Address Details

The Smart Card will be sent to the following address. Please amend if necessary.

Phone Number	778452824
Company name	HSBC
Address line 1 *	2nd Floor
Address line 2	3383 Gilmore Way
City/Town (address line 3)	Burnaby, BC
Address line 4	Canada
Postal code/Zip code *	V5G 4S1
Location *	CANADA

PIN Address Details

The PIN advice will be sent to the following address. Please amend if necessary.

Use the same address as above. ● Yes ○ No

5. An acknowledgement confirms that the Smart Card renewal has been initiated.

Note: Your Smart Card is not renewed until you actually receive the new Smart Card in the mail and activate it. Upon activating the new Smart Card, your old Smart Card is automatically cancelled.

Renew later

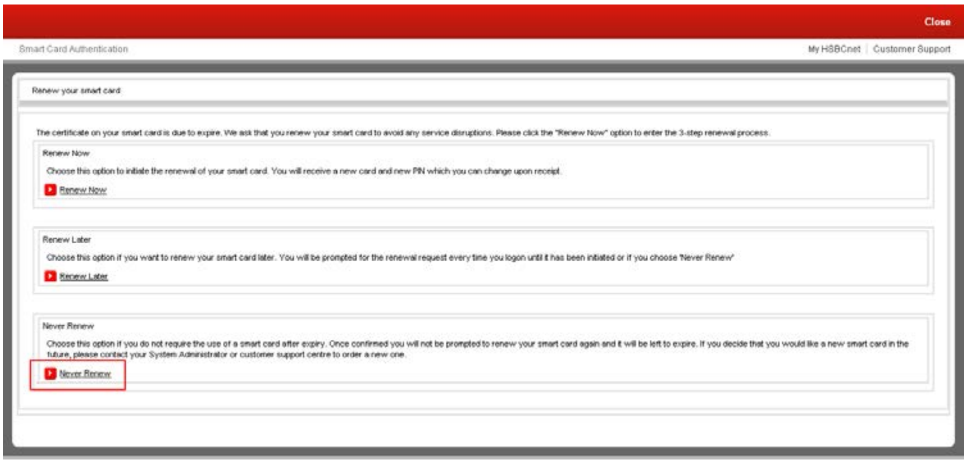
If you selected **Renew later** on the Smart Card renewal page, the system prompts you to renew your Smart Card every time you log on to HSBC*net* for up to 14 days prior to expiry. At this time, you must select either **Renew now** or **Never renew**.

Never renew

Only select **Never renew** if you no longer need your Smart Card after the expiry date. Once the Never renew process is initiated, it cannot be cancelled or reversed. Order a new Smart Card if you require a replacement in the future.

1. Select **Never renew** on the Smart Card renewal page.

Never Renew Smart Card link



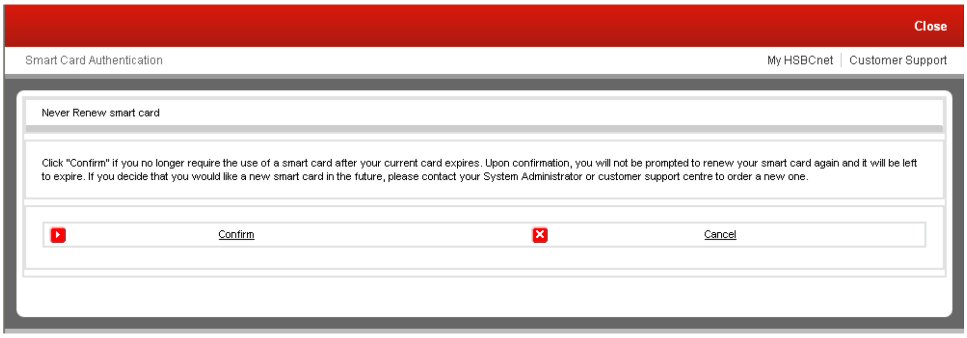
The certificate on your smart card is due to expire. We ask that you renew your smart card to avoid any service disruptions. Please click the "Renew Now" option to enter the 3-step renewal process.

Choose this option to initiate the renewal of your smart card. You will receive a new card and new PIN which you can change upon receipt.

Choose this option if you want to renew your smart card later. You will be prompted for the renewal request every time you logon until it has been initiated or if you choose 'Never Renew'

Choose this option if you do not require the use of a smart card after expiry. Once confirmed you will not be prompted to renew your smart card again and it will be left to expire. If you decide that you would like a new smart card in the future, please contact your System Administrator or customer support centre to order a new one.

2. Select **Confirm** to proceed.

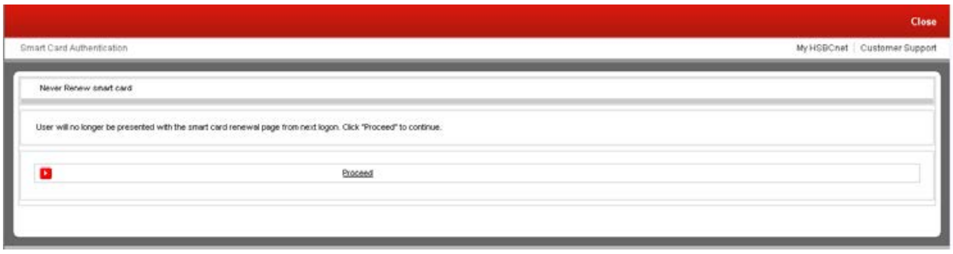


Click "Confirm" if you no longer require the use of a smart card after your current card expires. Upon confirmation, you will not be prompted to renew your smart card again and it will be left to expire. If you decide that you would like a new smart card in the future, please contact your System Administrator or customer support centre to order a new one.

3. An acknowledgement confirms your action.

4. Select **Proceed**.

Never Renew Smart Card—confirmation page



User will no longer be presented with the smart card renewal page from next logon. Click "Proceed" to continue.

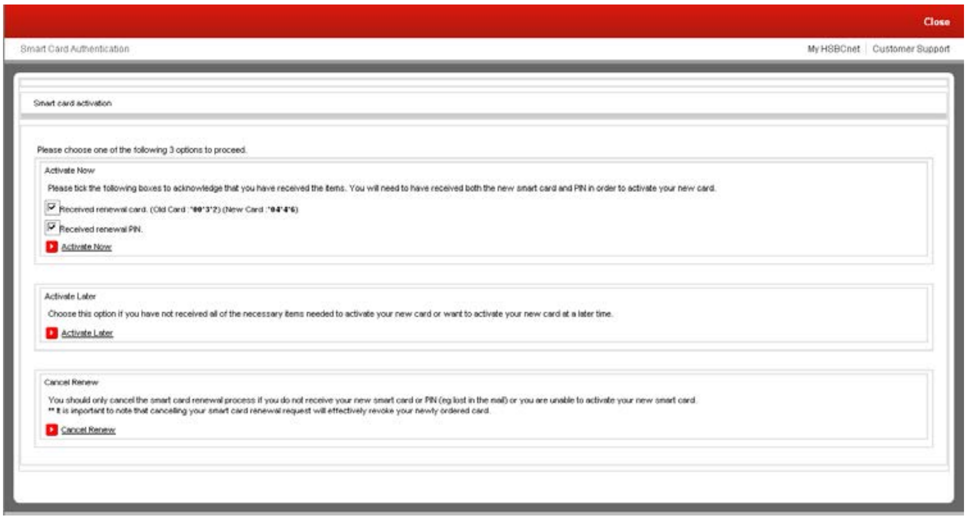
5. Select **Continue** to proceed to your personal page.

Activating renewed Smart Cards

Once you complete the Smart Card renewal process, a new Smart Card and PIN is automatically ordered and delivered to you within three to four business days. Every time you log on to *HSBCnet,* you will be presented three options on the Smart Card Activation page:

- **Activate now**—will revoke the existing card and activate the new card
- **Activate later**—to defer activation until the card and PIN are received
- **Cancel renew**—select if either the card or PIN is lost

Smart Card activation page



Smart card activation

Please choose one of the following 3 options to proceed.

Activate Now

Please tick the following boxes to acknowledge that you have received the items. You will need to have received both the new smart card and PIN in order to activate your new card.

☑ Received renewal card. (Old Card :**'00'3'2'**) (New Card :**'04'4'6'**)

☑ Received renewal PIN.

Activate Now

Activate Later

Choose this option if you have not received all of the necessary items needed to activate your new card or want to activate your new card at a later time.

Activate Later

Cancel Renew

You should only cancel the smart card renewal process if you do not receive your new smart card or PIN (eg lost in the mail) or you are unable to activate your new smart card.
** It is important to note that cancelling your smart card renewal request will effectively revoke your newly ordered card.

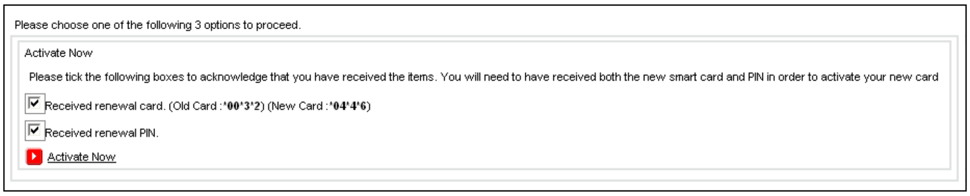
Cancel Renew

Activate now

You can activate your new Smart Card using this option.

1. Confirm receipt of the new Smart Card and PIN by selecting the relevant checkboxes. Select **Activate now** to initiate the activation process.

Smart Card—Activate now option



Please choose one of the following 3 options to proceed.

Activate Now

Please tick the following boxes to acknowledge that you have received the items. You will need to have received both the new smart card and PIN in order to activate your new card

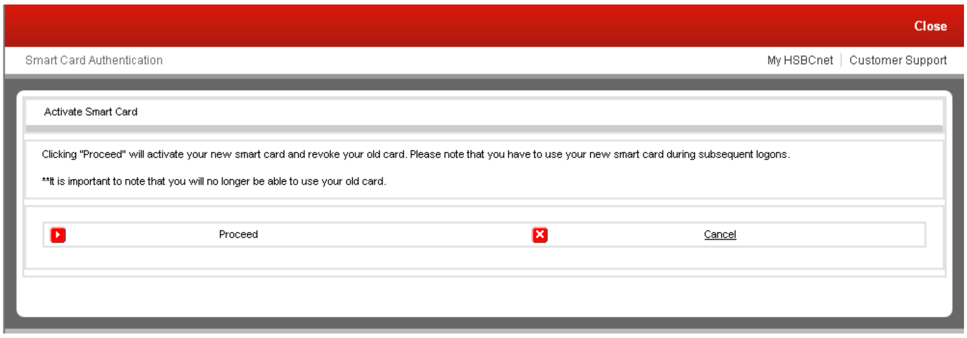
☑ Received renewal card. (Old Card :**'00'3'2'**) (New Card :**'04'4'6'**)

☑ Received renewal PIN.

Activate Now

2. In the Activate Smart Card page, select **Proceed** to activate the new card. This also irreversibly cancels the old Smart Card.

Activate Smart Card page



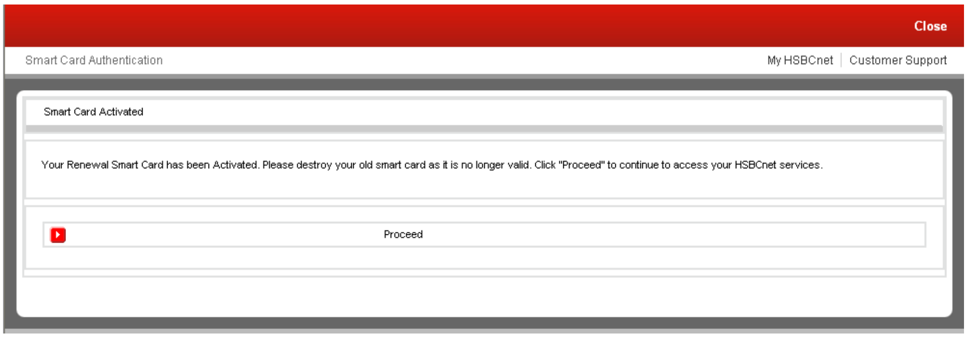
Activate Smart Card

Clicking "Proceed" will activate your new smart card and revoke your old card. Please note that you have to use your new smart card during subsequent logons.

**It is important to note that you will no longer be able to use your old card.

3. An acknowledgement confirms your action. Select **Proceed** to display your personal page.

Activate Smart Card—confirmation page



Smart Card Activated

Your Renewal Smart Card has been Activated. Please destroy your old smart card as it is no longer valid. Click "Proceed" to continue to access your HSBCnet services.

Activate later

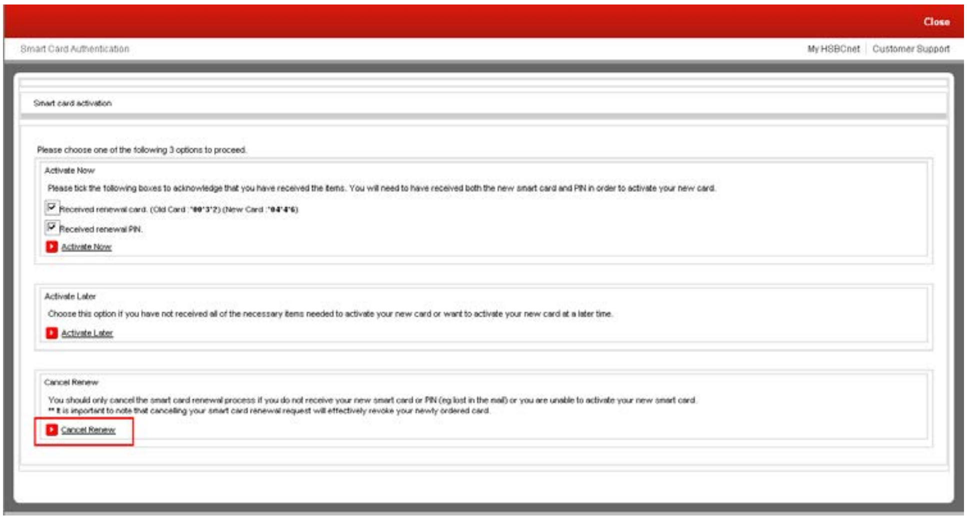
Select **Activate later** if you have not yet received your new Smart Card and PIN. You will be directed to your personal page. You can continue to use your old Smart Card and PIN until you receive and activate the new Smart Card and PIN.

Cancel renew

Cancel the Smart Card renewal process only if you do not receive your Smart Card or PIN (for example, if the package is lost in the mail) or if you are unable to activate your new Smart Card. Cancelling your Smart Card renewal effectively revokes your newly ordered card.

1. To cancel the Smart Card renewal process, select **Cancel renew**.

Cancel Smart Card renewal link



Please choose one of the following 3 options to proceed.

Activate Now

Please tick the following boxes to acknowledge that you have received the items. You will need to have received both the new smart card and PIN in order to activate your new card.

☑ Received renewal card. (Old Card : '**'3'2') (New Card : '*4'4'6')

☑ Received renewal PIN.

Activate Later

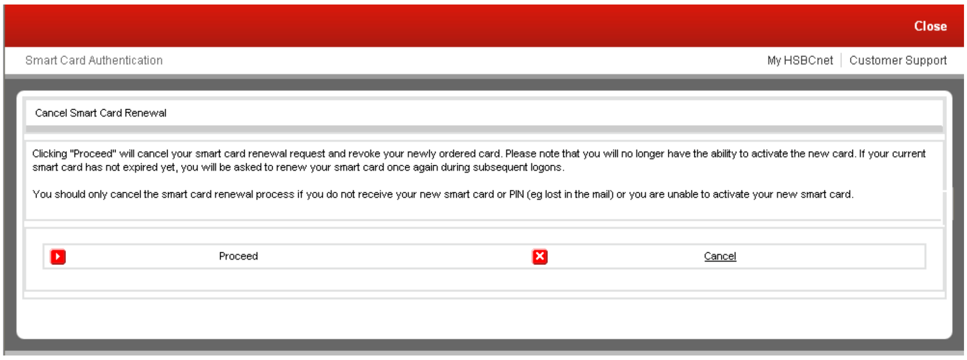
Choose this option if you have not received all of the necessary items needed to activate your new card or want to activate your new card at a later time.

Cancel Renew

You should only cancel the smart card renewal process if you do not receive your new smart card or PIN (eg lost in the mail) or you are unable to activate your new smart card.
** It is important to note that cancelling your smart card renewal request will effectively revoke your newly ordered card.

2. Select **Proceed** to confirm the cancellation.

Cancel Smart Card renewal—Proceed option

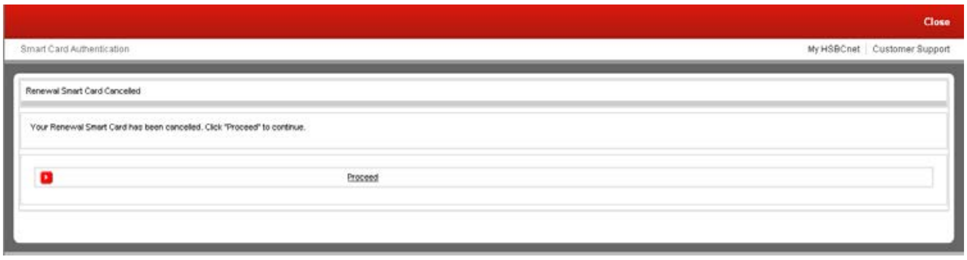


Clicking "Proceed" will cancel your smart card renewal request and revoke your newly ordered card. Please note that you will no longer have the ability to activate the new card. If your current smart card has not expired yet, you will be asked to renew your smart card once again during subsequent logons.

You should only cancel the smart card renewal process if you do not receive your new smart card or PIN (eg lost in the mail) or you are unable to activate your new smart card.

3. An acknowledgement confirms your action.

Smart Card Renewal Cancelled

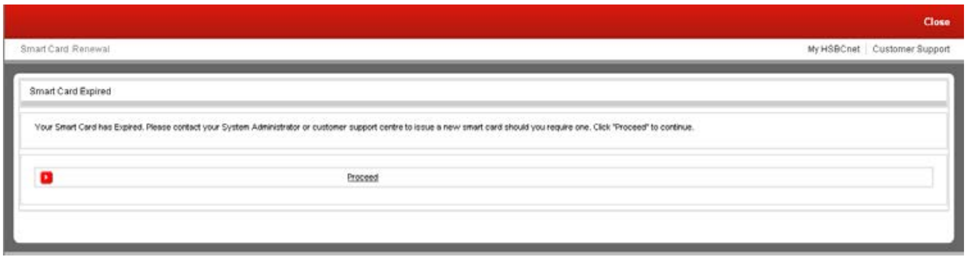


Your Renewal Smart Card has been cancelled. Click "Proceed" to continue.

If your Smart Card expires

If you have not logged on during the 45 days prior to the Smart Card expiry date, an error message appears after logging on notifying you that your Smart Card has expired. This message appears every time you log on to your account for a total of three times, after which there are no further reminders. If you try to access any of the tools requiring Smart Card authentication, the page warns you that the page cannot be displayed. You must contact your System Administrator to order a new card and PIN.

Smart Card expired notification page



Your Smart Card has Expired. Please contact your System Administrator or customer support centre to issue a new smart card should you require one. Click "Proceed" to continue.

Troubleshooting Smart Cards

Problems with Smart Cards typically fall into one of the following categories.

SYMPTOM	PROBABLE CAUSES	ACTION REQUIRED
PC does not detect Smart Card reader	Wrong Smart Card reader selected for installation	Order correct Smart Card reader
No Smart Card icon shown in the system tray	Computer was not restarted after installation	Close all programs and restart computer
'You did not present a valid certificate' error message	Smart Card not inserted properly (upside down, or not all the way in)	Insert Smart Card face up with red arrow facing forward. If inserted correctly, the blinking green light will turn solid green
'The page cannot be displayed' error message	Wrong PIN input or did not allow five seconds before selecting **Continue**	Log off, close browser and log on again to HSBC*net*
'No Smart Card reader found. CertReg will not work' error message	Installation problem	Uninstall the software and reinstall again
Smart card locked	Smart card has been revoked/replaced Incorrect PIN entered more than three times when using GemSafe utility	Request System Administrator to replace Smart Card
PIN not received	Courier problems	Traceable with a tracking number through the DHL website
Lost PIN	Courier problems	Request a new Smart Card

Security Device Guide

About Security Devices

Your company provides Security Devices in order to securely set up Users and authenticate Users' transactions on HSBC*net*.

HSBC*net* System Administrators are responsible for ordering, setting up and managing Security Devices for all Users in their company.

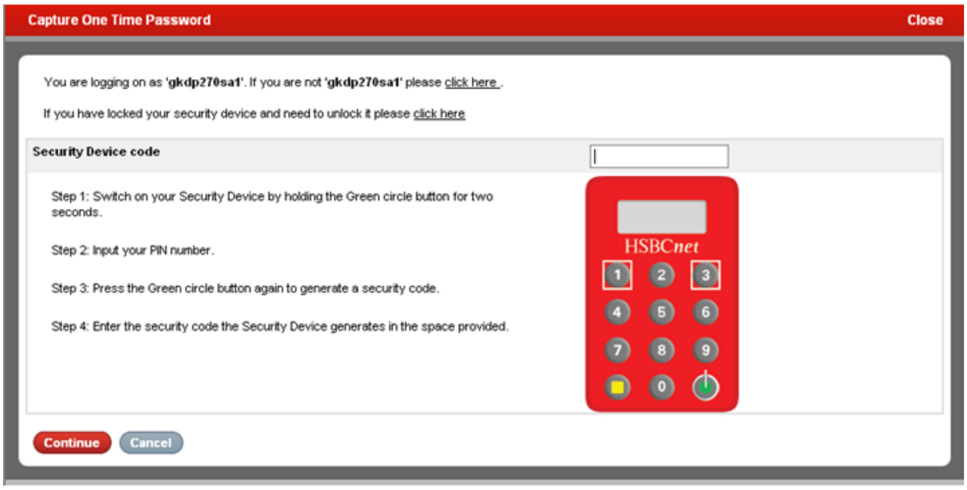
Before you begin

While setting you up as a User, your HSBC*net* System Administrator must entitle you with access to tools and services, and allocate a Security Device. The security device is required to validate your username in the following circumstances:

- Logging on to the system
- Initiating and authorising administrative changes
- Creating and authorising payments

Depending on the setup at the User access level, you may be entitled to different roles as a User.

Security Device log on authentication page



You are logging on as '**gkdp270sa1**'. If you are not '**gkdp270sa1**' please click here .

If you have locked your security device and need to unlock it please click here

Security Device code

Step 1: Switch on your Security Device by holding the Green circle button for two seconds.

Step 2: Input your PIN number.

Step 3: Press the Green circle button again to generate a security code.

Step 4: Enter the security code the Security Device generates in the space provided.

The following are some HSBC*net* User tools and services requiring authentication:

- HSBC*net* log on
- Payment creation and authorisation
- Administrative setup and change approval
- File Upload
- Internet Trade Services (ITS)
- e-Securities (Transaction Entry)

Using Security Devices

You can use your Security Device to do the following operations:

- Activating your Security Device
- Changing your Security Device PIN
- Resetting your Security Device PIN
- Security Device authentication

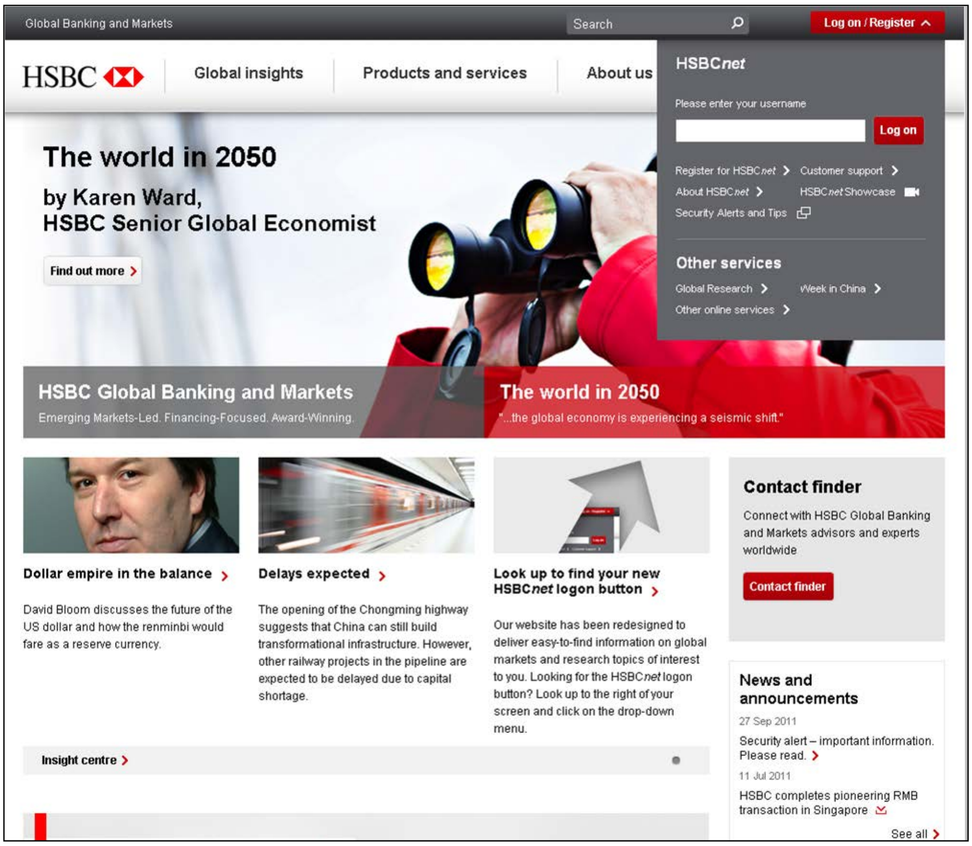
Activating your Security Device

If you are a System Administrator or End User and are logging on to HSBC*net* to activate your new Security Device, you must complete the following steps:

1. On the top right corner of the HSBC*net* home page, select **Log on/Register**. A drop-down window appears.

2. Enter your username and select **Log on**.

HSBCnet home page



The world in 2050
by Karen Ward,
HSBC Senior Global Economist

HSBC Global Banking and Markets
Emerging Markets-Led. Financing-Focused. Award-Winning.

The world in 2050
"...the global economy is experiencing a seismic shift."

Dollar empire in the balance

David Bloom discusses the future of the US dollar and how the renminbi would fare as a reserve currency.

Delays expected

The opening of the Chongming highway suggests that China can still build transformational infrastructure. However, other railway projects in the pipeline are expected to be delayed due to capital shortage.

Look up to find your new HSBC*net* logon button

Our website has been redesigned to deliver easy-to-find information on global markets and research topics of interest to you. Looking for the HSBC*net* logon button? Look up to the right of your screen and click on the drop-down menu.

Contact finder

Connect with HSBC Global Banking and Markets advisors and experts worldwide

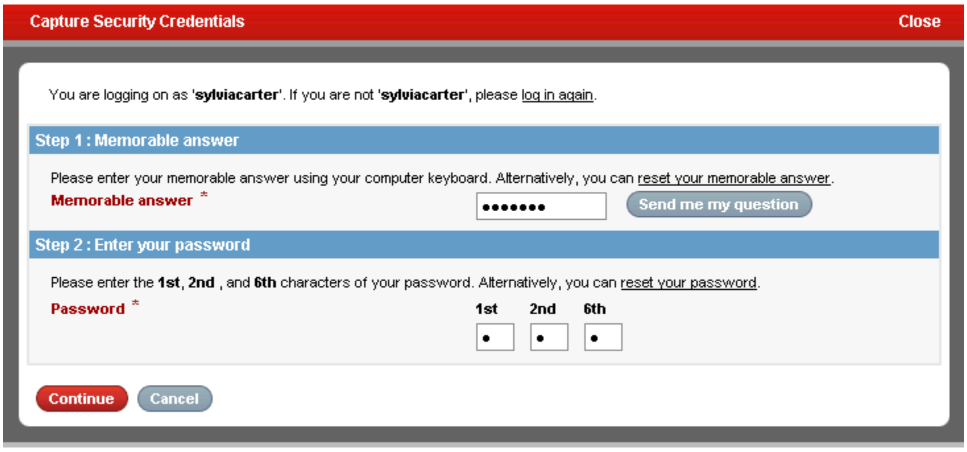
News and announcements

27 Sep 2011
Security alert – important information. Please read.

11 Jul 2011
HSBC completes pioneering RMB transaction in Singapore

3. The Capture Security Credentials page appears. Enter your memorable answer. Next, enter the three requested characters of your current password (Follow the on-screen instructions).

Capture Security Credentials page



Capture Security Credentials

Close

You are logging on as '**sylviacarter**'. If you are not '**sylviacarter**', please log in again.

Step 1 : Memorable answer

Please enter your memorable answer using your computer keyboard. Alternatively, you can reset your memorable answer.

Memorable answer * •••••••

Step 2 : Enter your password

Please enter the **1st**, **2nd** , and **6th** characters of your password. Alternatively, you can reset your password.

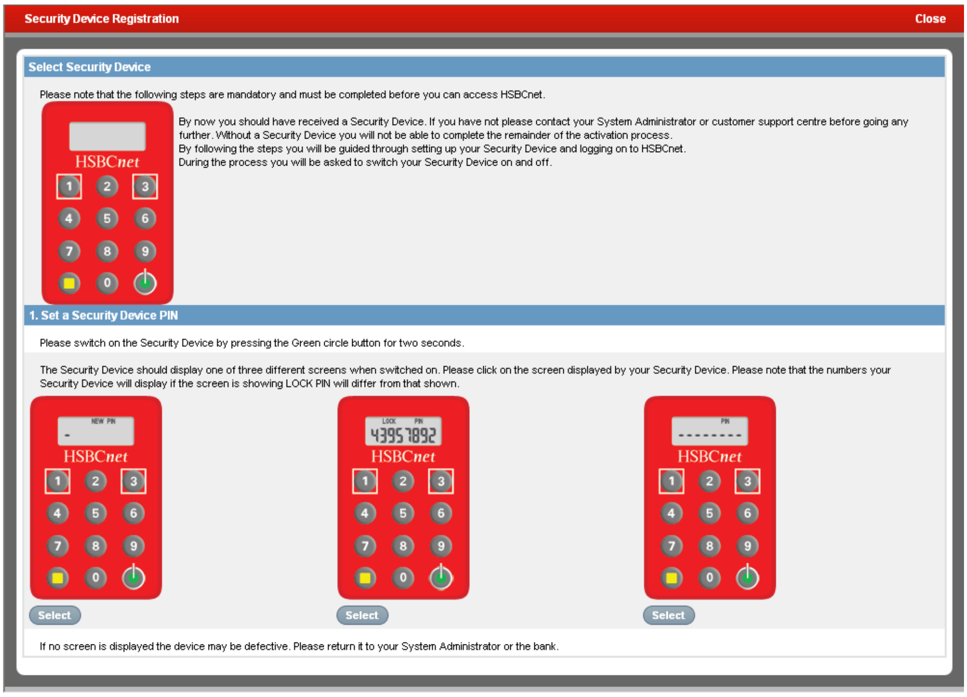
Password *

1st	2nd	6th
•	•	•

Select **Continue** to proceed.

4. The Security Device Registration page appears. Choose **Select** under the image that displays **New PIN** message to proceed. The Security Device Activation page appears.

Security Device Registration page



Security Device Registration

Close

Select Security Device

Please note that the following steps are mandatory and must be completed before you can access HSBCnet.

By now you should have received a Security Device. If you have not please contact your System Administrator or customer support centre before going any further. Without a Security Device you will not be able to complete the remainder of the activation process.

By following the steps you will be guided through setting up your Security Device and logging on to HSBCnet.

During the process you will be asked to switch your Security Device on and off.

1. Set a Security Device PIN

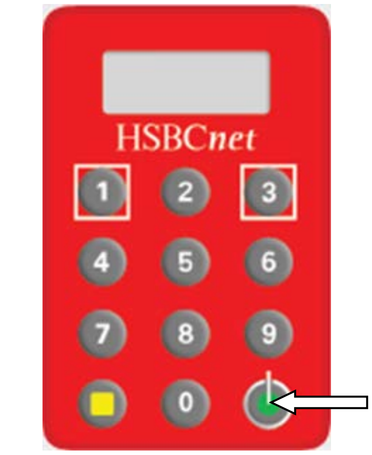
Please switch on the Security Device by pressing the Green circle button for two seconds.

The Security Device should display one of three different screens when switched on. Please click on the screen displayed by your Security Device. Please note that the numbers your Security Device will display if the screen is showing LOCK PIN will differ from that shown.

If no screen is displayed the device may be defective. Please return it to your System Administrator or the bank.

5. **Setting your PIN:** Complete the following steps to select and set a new PIN for your Device.

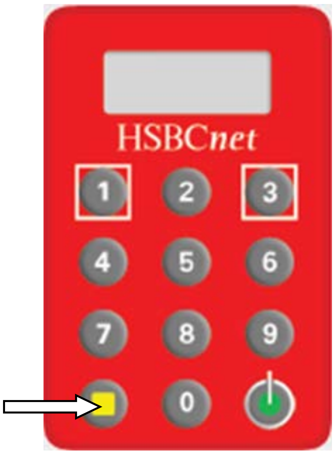
   a. To power on your device, press and hold the Green circle button on your device for **two seconds**.



b. The **New PIN** message appears in the device window. Select and enter a new 4 to 8 digit PIN using the device key pad.

NEW PIN
HSBCnet

c. To submit your PIN, press the Yellow square button on the bottom row of the device key pad.



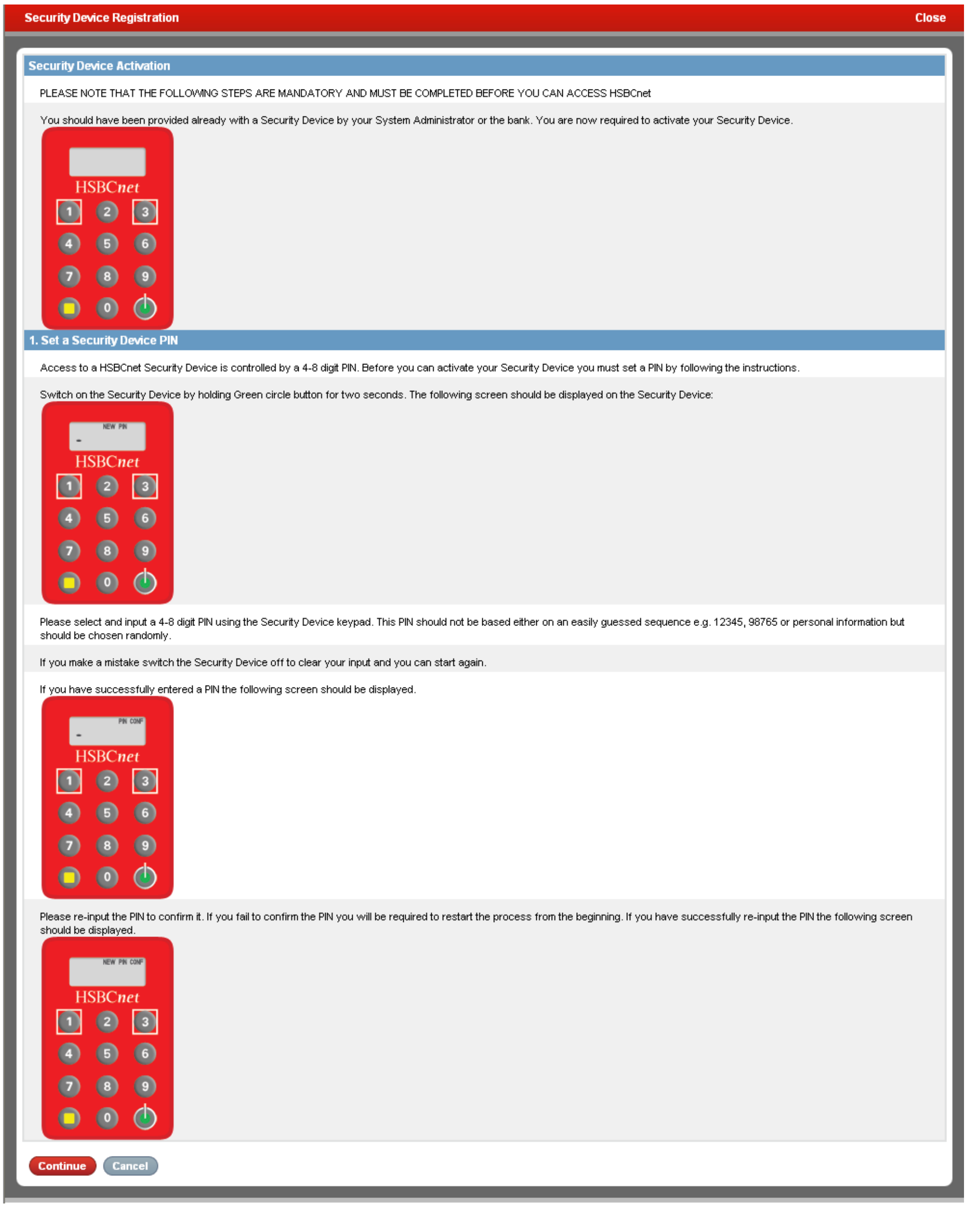
d. If your PIN is accepted, a **PIN CONF** message appears in the device window.

PIN CONF
HSBCnet

e. Key in the same 4 to 8 digit PIN again using the device key pad to confirm your PIN.

f. The **NEW PIN CONF** message appears briefly in the device window before displaying two dashes. You have successfully set your PIN.

g. Next select **Continue** to proceed.



Security Device Activation

PLEASE NOTE THAT THE FOLLOWING STEPS ARE MANDATORY AND MUST BE COMPLETED BEFORE YOU CAN ACCESS HSBCnet

You should have been provided already with a Security Device by your System Administrator or the bank. You are now required to activate your Security Device.

1. Set a Security Device PIN

Access to a HSBCnet Security Device is controlled by a 4-8 digit PIN. Before you can activate your Security Device you must set a PIN by following the instructions.

Switch on the Security Device by holding Green circle button for two seconds. The following screen should be displayed on the Security Device:

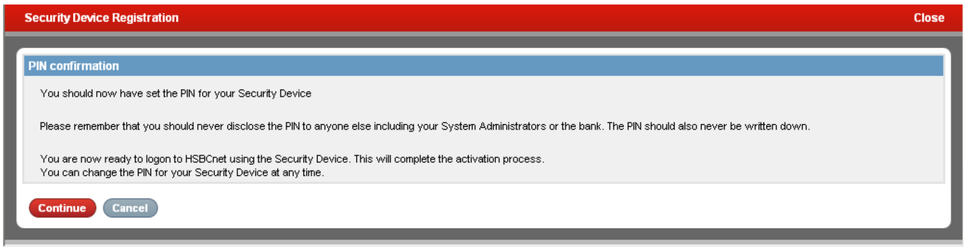
Please select and input a 4-8 digit PIN using the Security Device keypad. This PIN should not be based either on an easily guessed sequence e.g. 12345, 98765 or personal information but should be chosen randomly.

If you make a mistake switch the Security Device off to clear your input and you can start again.

If you have successfully entered a PIN the following screen should be displayed.

Please re-input the PIN to confirm it. If you fail to confirm the PIN you will be required to restart the process from the beginning. If you have successfully re-input the PIN the following screen should be displayed.

6. On the PIN Confirmation page, select **Continue**. The Security Device authentication page appears.



PIN confirmation

You should now have set the PIN for your Security Device

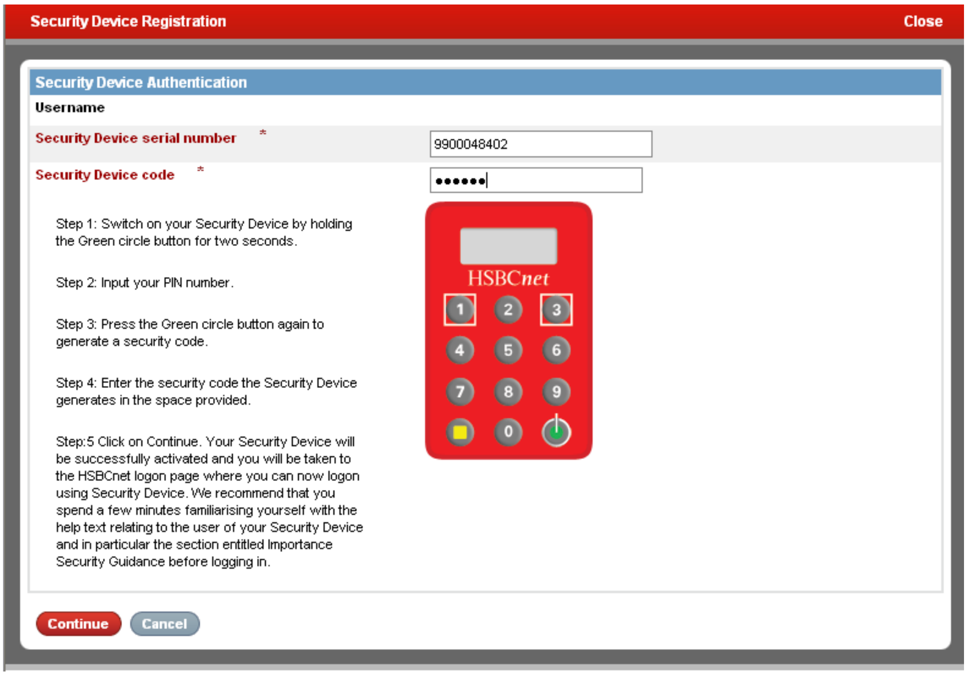
Please remember that you should never disclose the PIN to anyone else including your System Administrators or the bank. The PIN should also never be written down.

You are now ready to logon to HSBCnet using the Security Device. This will complete the activation process.
You can change the PIN for your Security Device at any time.

7. On the Security Device Authentication page, the Security Device serial number field is already populated with the number of the device assigned to you. Ensure that this on-screen serial number matches with the serial number on the back of your device.

   Press and hold the Green circle button on your Security Device for two seconds. Enter the PIN number you selected earlier. Next, enter the six-digit security code that appears in the Security Device window into the Security code field on your computer screen. Select **Continue** to proceed and you will be directed to the HSBC*net* home page. You can confirm the Security Device has been successfully activated by logging on to HSBC*net.*

Security Device Authentication



Security Device Authentication

Username

Security Device serial number * 9900048402

Security Device code * ••••••

Step 1: Switch on your Security Device by holding the Green circle button for two seconds.

Step 2: Input your PIN number.

Step 3: Press the Green circle button again to generate a security code.

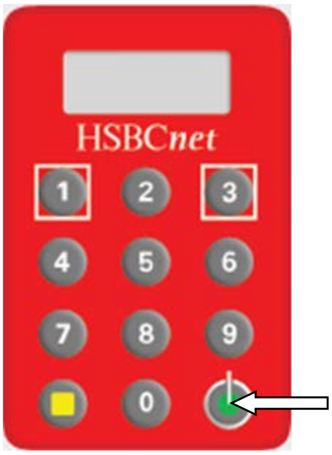
Step 4: Enter the security code the Security Device generates in the space provided.

Step:5 Click on Continue. Your Security Device will be successfully activated and you will be taken to the HSBCnet logon page where you can now logon using Security Device. We recommend that you spend a few minutes familiarising yourself with the help text relating to the user of your Security Device and in particular the section entitled Importance Security Guidance before logging in.

Changing your Security Device PIN

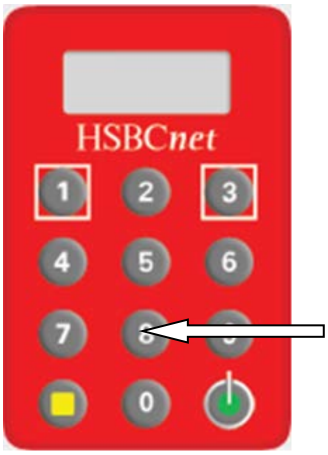
If for any reason you wish to change your PIN on the (already activated) new Security Device, complete the following steps:

1. Power on your device by pressing and holding the Green circle button on your device for **two seconds**.



2. Key in your existing 4 to 8 digit PIN using the device key pad. The device window displays two dashes.

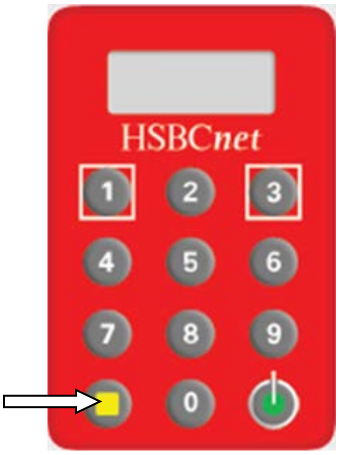
3. To change your PIN, press and hold the **number 8 button** on the device key pad for **two seconds**.



4. The **NEW PIN** message appears in the device window. Select and enter a new 4 to 8 digit PIN using the device key pad.

NEW PIN
HSBCnet

5. To submit your PIN, press the Yellow square button on the bottom row of the key pad.



6. The **PIN CONF** message appears in the device window.

7. Confirm your PIN by keying in your new 4 to 8 digit PIN again using the device key pad.

8. The **NEW PIN CONF** message appears briefly in the device window before displaying two dashes. You have successfully changed your PIN.

Note: The device will require you to select a strong PIN. A weak PIN (example 11111 or 12345) will be rejected by the device and will display a **not SAFE** message briefly before reverting to the NEW PIN message. Resume selecting a strong PIN until accepted.

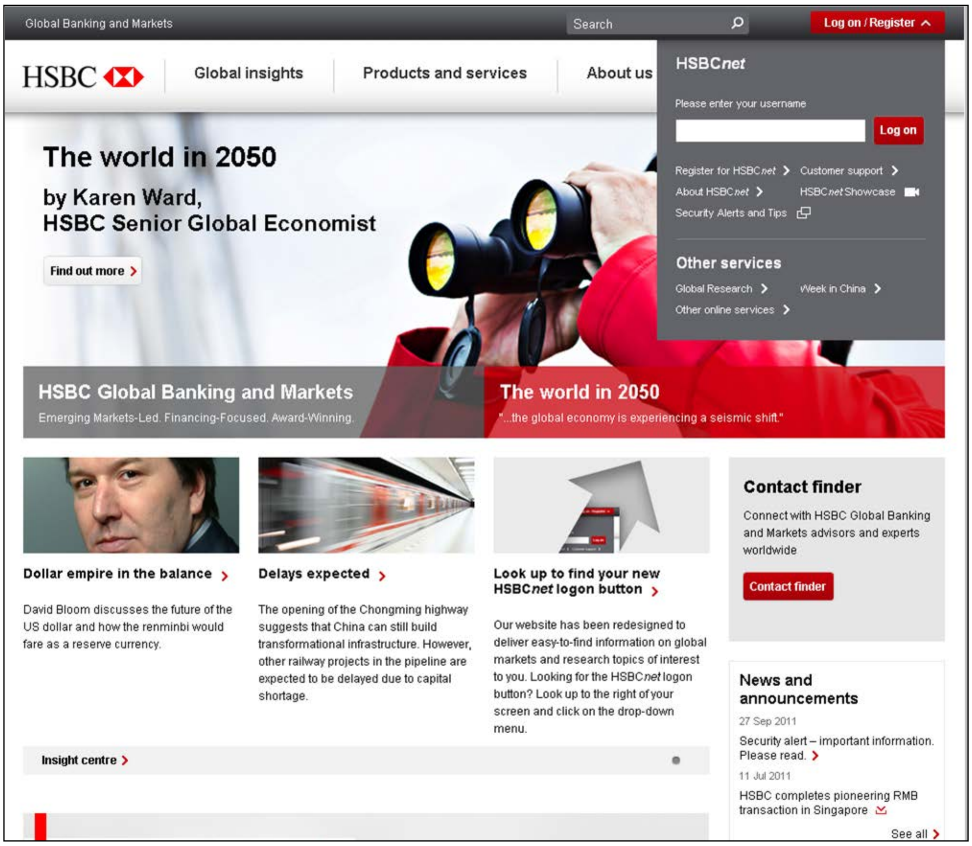
Resetting your Security Device PIN

If after a number of unsuccessful attempts to enter your PIN into the device and your Security Device is locked, you can reset the PIN using the online PIN reset function. To do so, complete the following steps:

1. On the top right corner of the HSBC*net* home page, select **Log on/Register**. A drop-down window appears.

2. Enter your username and select **Log on**.

HSBCnet Home Page



The world in 2050

by Karen Ward,
HSBC Senior Global Economist

HSBC Global Banking and Markets

Emerging Markets-Led. Financing-Focused. Award-Winning.

The world in 2050

"...the global economy is experiencing a seismic shift."

David Bloom discusses the future of the US dollar and how the renminbi would fare as a reserve currency.

The opening of the Chongming highway suggests that China can still build transformational infrastructure. However, other railway projects in the pipeline are expected to be delayed due to capital shortage.

Our website has been redesigned to deliver easy-to-find information on global markets and research topics of interest to you. Looking for the HSBCnet logon button? Look up to the right of your screen and click on the drop-down menu.

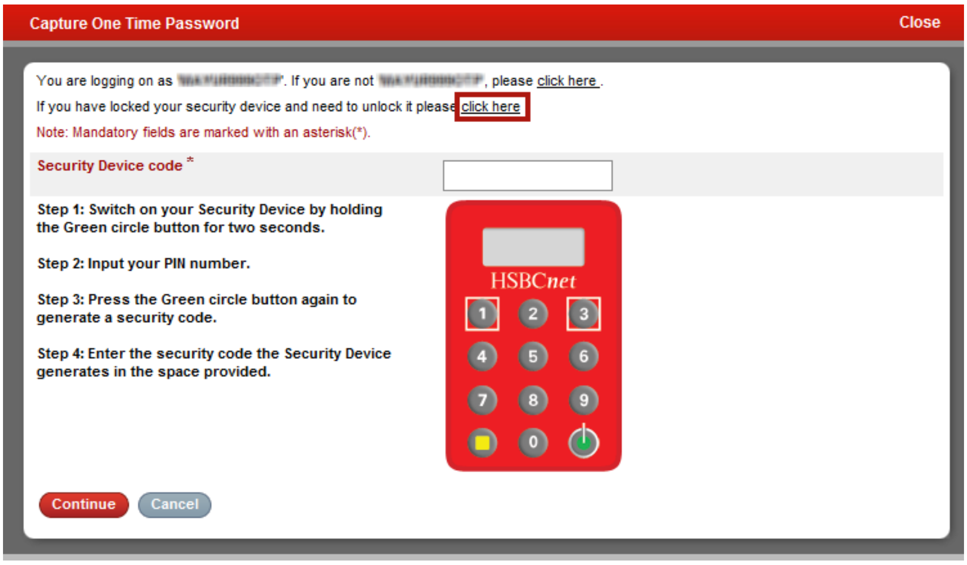
Connect with HSBC Global Banking and Markets advisors and experts worldwide

27 Sep 2011
Security alert – important information. Please read.

11 Jul 2011
HSBC completes pioneering RMB transaction in Singapore

3. On the Capture One Time Password page that appears, choose the **click here** link as shown in the image below.

Capture One Time Password



Capture One Time Password

You are logging on as [redacted]. If you are not [redacted], please click here .

If you have locked your security device and need to unlock it please click here

Note: Mandatory fields are marked with an asterisk(*).

Security Device code *

Step 1: Switch on your Security Device by holding the Green circle button for two seconds.

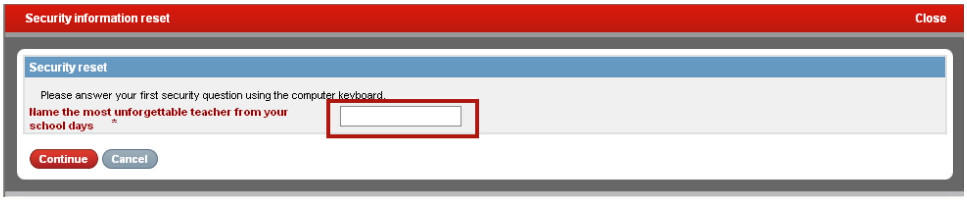
Step 2: Input your PIN number.

Step 3: Press the Green circle button again to generate a security code.

Step 4: Enter the security code the Security Device generates in the space provided.

4. A window appears requiring you to answer the first of two security questions selected by you during your registration process. Answer the first question correctly and select **Continue** to proceed to the second question.

First Security Question



Security information reset

Security reset

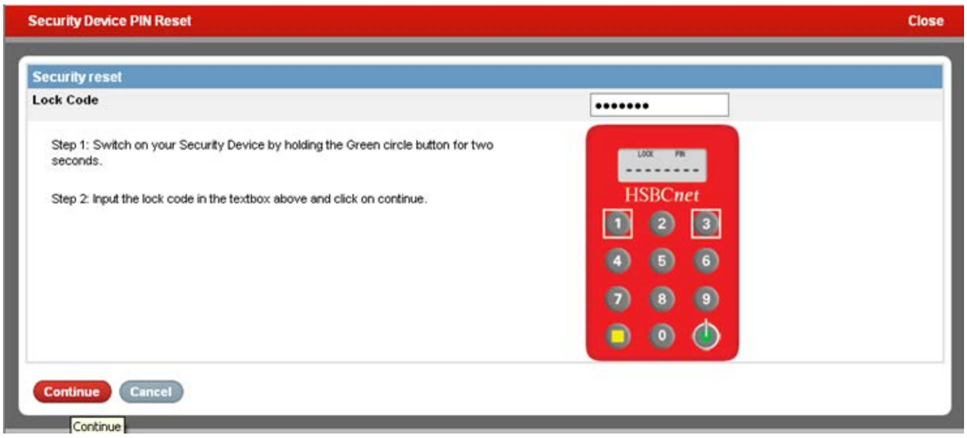
Please answer your first security question using the computer keyboard.

Name the most unforgettable teacher from your school days *

5. Answer the second security question correctly and select **Continue** to complete the verification process

Note: If you have forgotten either of your security questions, and have entered the incorrect answer three times, you will be directed to the Security Information Reset process. For more information on how to complete a Security Information Reset (SIR) refer to the section on Resetting Security Information.

6. After correctly answering both security questions, enter the LOCK PIN code from your Security Device into the Lock Code field on-screen. Select **Continue** again to proceed.



Security Device PIN Reset

Security reset

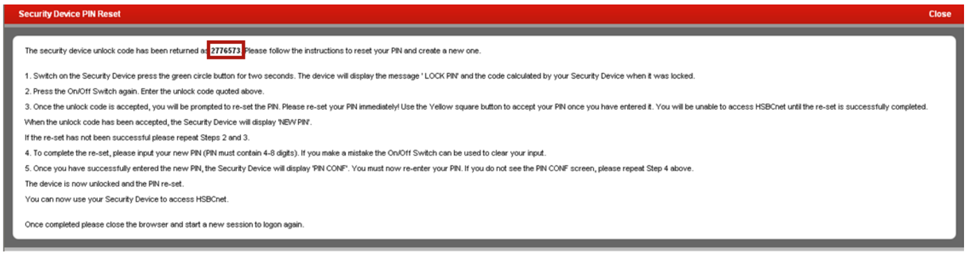
Lock Code •••••••

Step 1: Switch on your Security Device by holding the Green circle button for two seconds.

Step 2: Input the lock code in the textbox above and click on continue.

7. The Security Device PIN Reset page that appears displays the Security Device unlock code.

Security Device PIN Reset page



The security device unlock code has been returned as 2776573. Please follow the instructions to reset your PIN and create a new one.

1. Switch on the Security Device press the green circle button for two seconds. The device will display the message ' LOCK PIN' and the code calculated by your Security Device when it was locked.

2. Press the On/Off Switch again. Enter the unlock code quoted above.

3. Once the unlock code is accepted, you will be prompted to re-set the PIN. Please re-set your PIN immediately! Use the Yellow square button to accept your PIN once you have entered it. You will be unable to access HSBCnet until the re-set is successfully completed.

When the unlock code has been accepted, the Security Device will display 'NEW PIN'.

If the re-set has not been successful please repeat Steps 2 and 3.

4. To complete the re-set, please input your new PIN (PIN must contain 4-8 digits). If you make a mistake the On/Off Switch can be used to clear your input.

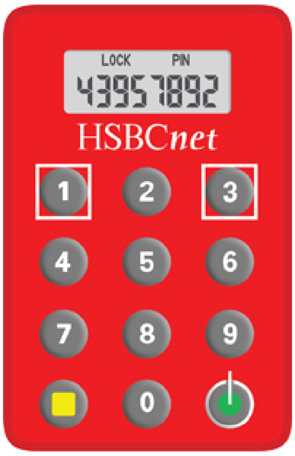
5. Once you have successfully entered the new PIN, the Security Device will display 'PIN CONF'. You must now re-enter your PIN. If you do not see the PIN CONF screen, please repeat Step 4 above.

The device is now unlocked and the PIN re-set.

You can now use your Security Device to access HSBCnet.

Once completed please close the browser and start a new session to logon again.

8. Turn on your Security Device by pressing the Green circle button for two seconds. The LOCK PIN message appears displaying the 8-digit lock pin in the device window.

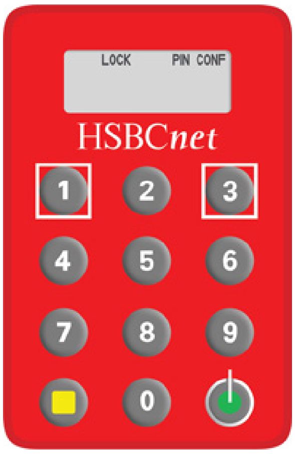


9. Press the Green circle button again. The device window displays a series of dashes. Key in the on-screen unlock code (see step 6) into your Security Device and press the Yellow square button. The LOCK NEW PIN message appears in the device window.

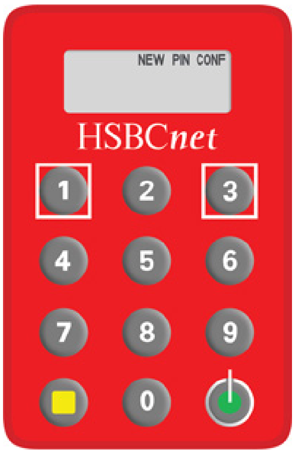
Note: If you enter the unlock code incorrectly three times your device will display a FAIL 3 message for an hour preventing any further input. For more information, refer to the Troubleshooting Security Devices section in this User Guide.

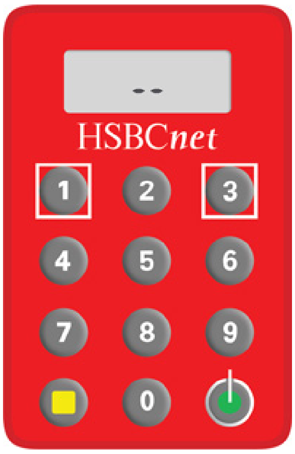
LOCK NEW PIN
HSBCnet
1 2 3
4 5 6
7 8 9
0

10. Key in a new 4 to 8 digit PIN using the device key pad and press the Yellow square button again. The LOCK PIN CONF message appears.



11. Key in the same 4 to 8 digit PIN again. The NEW PIN CONF message appears in the device window briefly before displaying two dashes. You have successfully unlocked your Security Device and reset the PIN.





Security Device authentication

You authenticate yourself on HSBC*net* by entering a dynamically generated security code (one-time password) whenever a Security Device authentication page appears. The procedure to authenticate yourself depends on your role in the company in one of the following stages:

- Initial log on by Initial System Administrators
- Initial log on by new System Administrators and new End Users
- Subsequent log on by all Users
- Authorising transactions and administrative changes

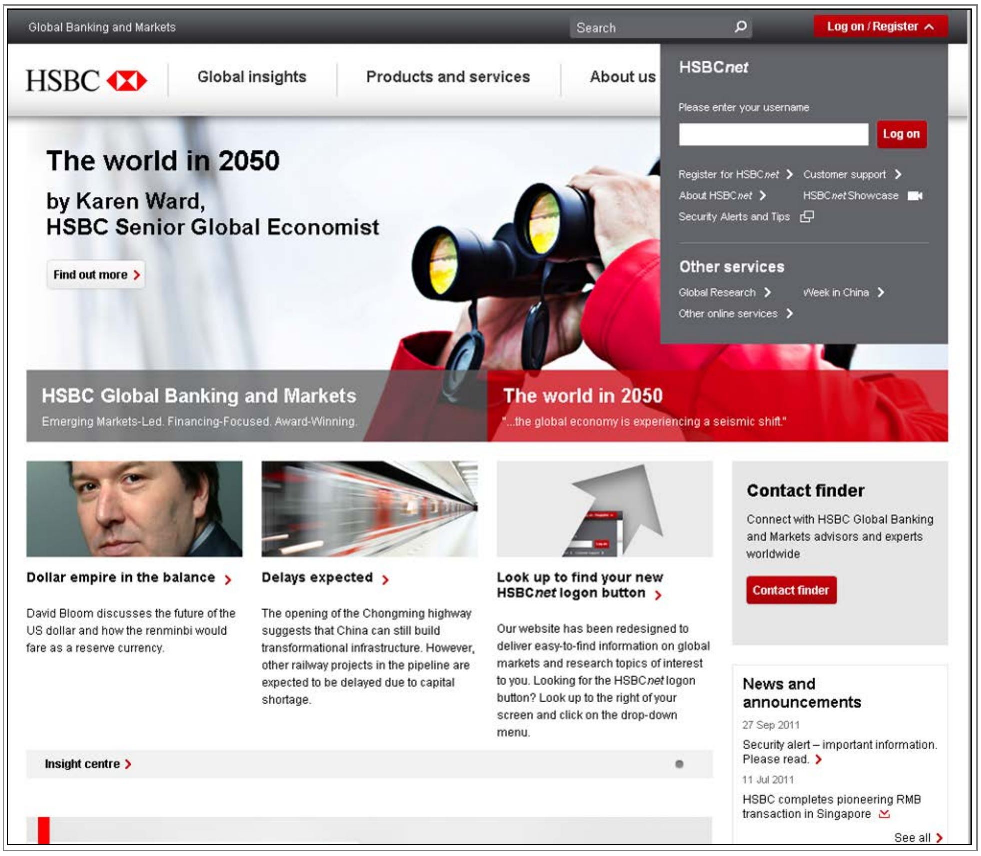
Initial log on by Initial System Administrator

If you are an Initial System Administrator (usually a signatory to your company's documentation filed with the Bank), you need to complete the following steps during your initial log on to activate your Security Device.

1. On the top right corner of the HSBC*net* home page, select **Log on/Register**. A drop-down window appears.

2. Enter your username and select **Log on**.

HSBCnet Home page



The world in 2050

by Karen Ward, HSBC Senior Global Economist

HSBC Global Banking and Markets

Emerging Markets-Led. Financing-Focused. Award-Winning.

The world in 2050

"...the global economy is experiencing a seismic shift."

Dollar empire in the balance

David Bloom discusses the future of the US dollar and how the renminbi would fare as a reserve currency.

Delays expected

The opening of the Chongming highway suggests that China can still build transformational infrastructure. However, other railway projects in the pipeline are expected to be delayed due to capital shortage.

Look up to find your new HSBCnet logon button

Our website has been redesigned to deliver easy-to-find information on global markets and research topics of interest to you. Looking for the HSBCnet logon button? Look up to the right of your screen and click on the drop-down menu.

Contact finder

Connect with HSBC Global Banking and Markets advisors and experts worldwide

News and announcements

27 Sep 2011

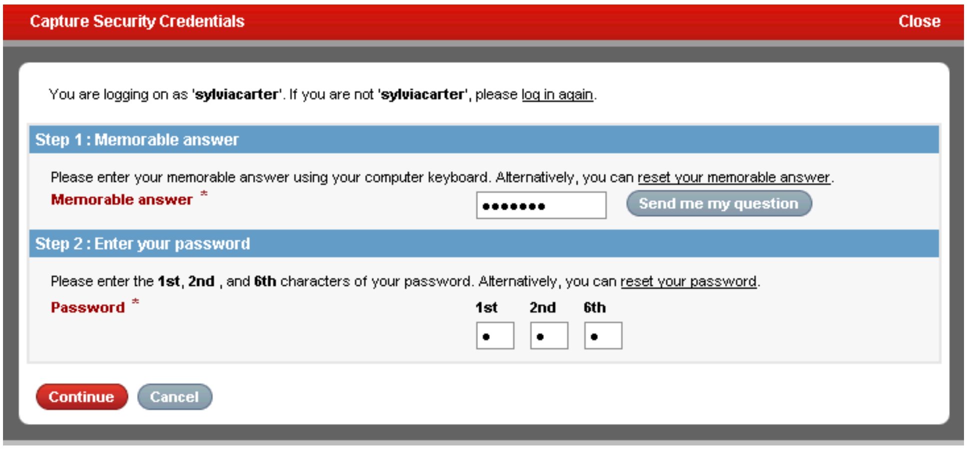
Security alert – important information. Please read.

11 Jul 2011

HSBC completes pioneering RMB transaction in Singapore

3. The Capture Security Credentials page appears. Enter your memorable answer. Enter the three requested characters of your current password. Select **Continue** to proceed.

Capture Security Credentials page



You are logging on as '**sylviacarter**'. If you are not '**sylviacarter**', please log in again.

Step 1 : Memorable answer

Please enter your memorable answer using your computer keyboard. Alternatively, you can reset your memorable answer.

Memorable answer * ●●●●●●●

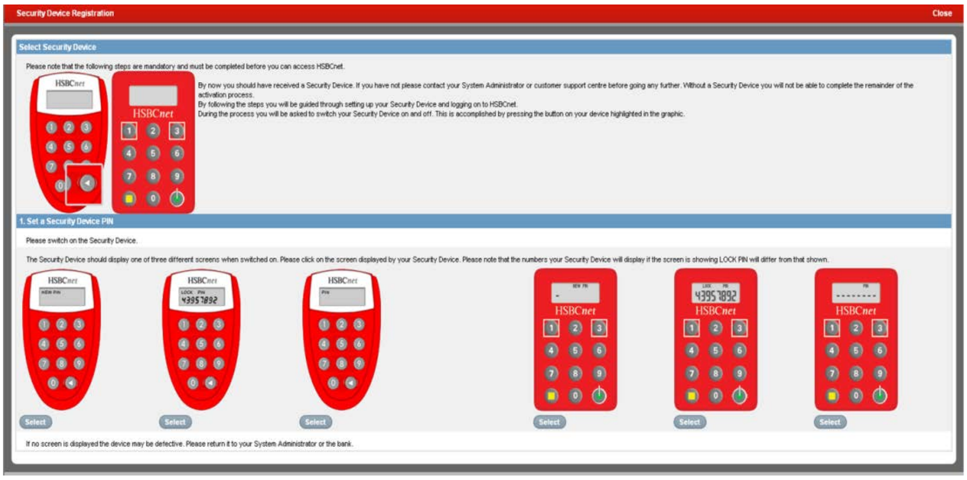
Step 2 : Enter your password

Please enter the **1st**, **2nd** , and **6th** characters of your password. Alternatively, you can reset your password.

	1st	**2nd**	**6th**
Password *	●	●	●

4. The Security Device Registration page appears. Choose the **Select** button under the image that displays the **NEW PIN** message.

Security Device activation page



Security Device Registration

Select Security Device

Please note that the following steps are mandatory and must be completed before you can access HSBCnet.

By now you should have received a Security Device. If you have not please contact your System Administrator or customer support centre before going any further. Without a Security Device you will not be able to complete the remainder of the activation process.
By following the steps you will be guided through setting up your Security Device and logging on to HSBCnet.
During the process you will be asked to switch your Security Device on and off. This is accomplished by pressing the button on your device highlighted in the graphic.

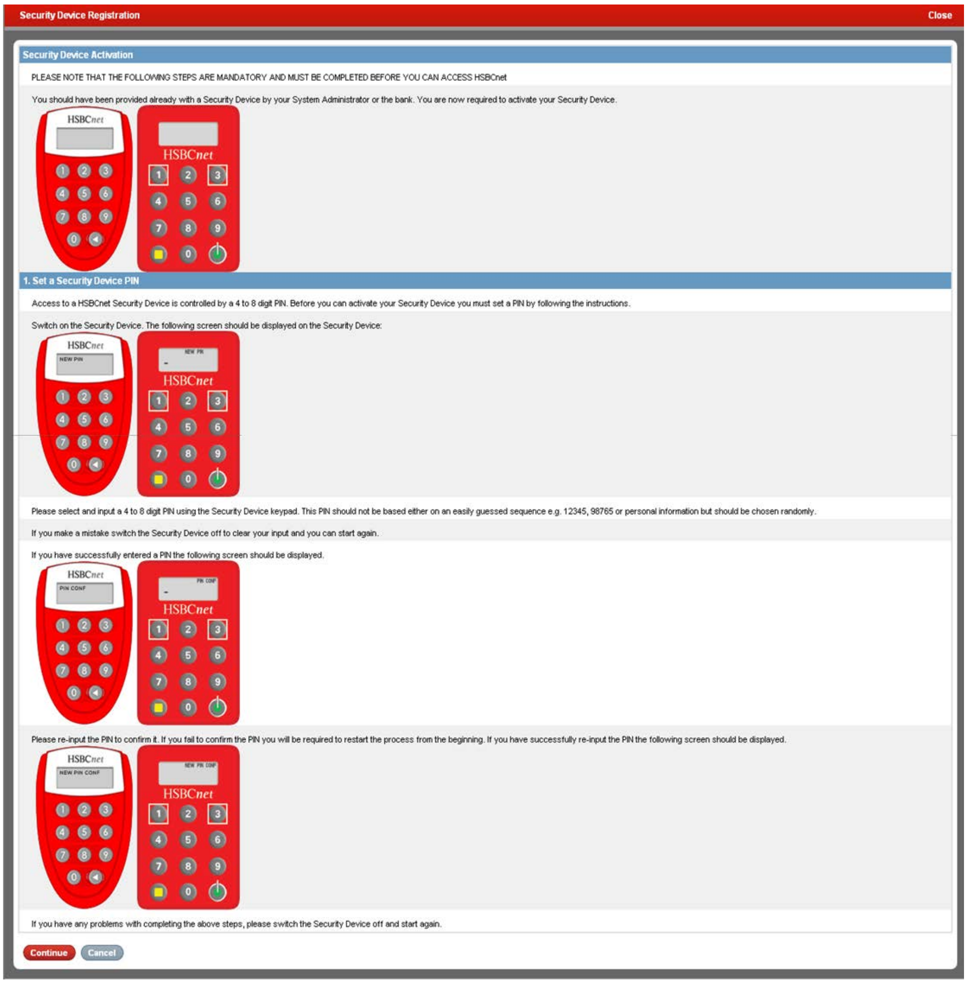
1. Set a Security Device PIN

Please switch on the Security Device.

The Security Device should display one of three different screens when switched on. Please click on the screen displayed by your Security Device. Please note that the numbers your Security Device will display if the screen is showing LOCK PIN will differ from that shown.

If no screen is displayed the device may be defective. Please return it to your System Administrator or the bank.

5. The Security Device Activation page appears. Set up your PIN using your new device. Refer to the section on **Setting your PIN** for a step by step procedure. Select **Continue** to proceed.



Security Device Registration

Security Device Activation

PLEASE NOTE THAT THE FOLLOWING STEPS ARE MANDATORY AND MUST BE COMPLETED BEFORE YOU CAN ACCESS HSBCnet

You should have been provided already with a Security Device by your System Administrator or the bank. You are now required to activate your Security Device.

1. Set a Security Device PIN

Access to a HSBCnet Security Device is controlled by a 4 to 8 digit PIN. Before you can activate your Security Device you must set a PIN by following the instructions.

Switch on the Security Device. The following screen should be displayed on the Security Device:

Please select and input a 4 to 8 digit PIN using the Security Device keypad. This PIN should not be based either on an easily guessed sequence e.g. 12345, 98765 or personal information but should be chosen randomly.

If you make a mistake switch the Security Device off to clear your input and you can start again.

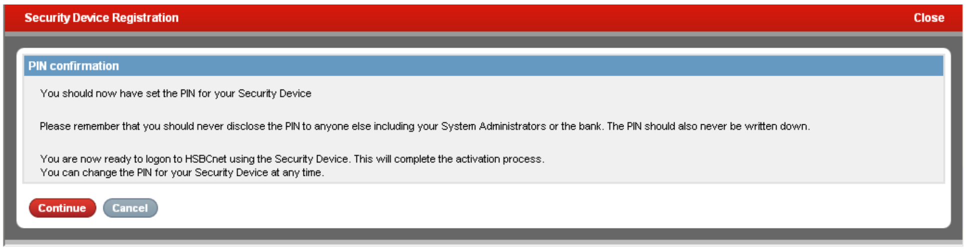
If you have successfully entered a PIN the following screen should be displayed.

Please re-input the PIN to confirm it. If you fail to confirm the PIN you will be required to restart the process from the beginning. If you have successfully re-input the PIN the following screen should be displayed.

If you have any problems with completing the above steps, please switch the Security Device off and start again.

6. On the PIN confirmation page, select **Continue**.

Security Device PIN Confirmation page



PIN confirmation

You should now have set the PIN for your Security Device

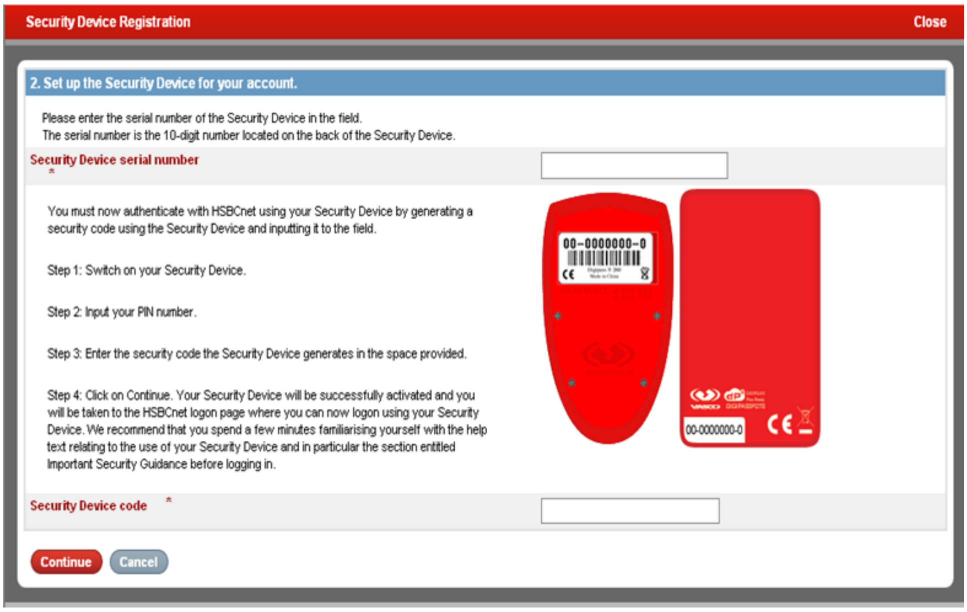
Please remember that you should never disclose the PIN to anyone else including your System Administrators or the bank. The PIN should also never be written down.

You are now ready to logon to HSBCnet using the Security Device. This will complete the activation process.
You can change the PIN for your Security Device at any time.

7. On step 2 of the Security Device setup page, enter the 10-digit serial number located on the back of your Security Device without the dashes.

8. Turn on your Security Device by pressing down the Green circle button on your device for two seconds. Using the Device key pad, key in the PIN you selected earlier. Enter the security code that the device generates in the on-screen **Security Device code** field and select **Continue**. If the information you provided is correct, the HSBC*net* home page appears. If not, an error message appears requiring you to resubmit the correct information.

Security Device activation step 2



2. Set up the Security Device for your account.

Please enter the serial number of the Security Device in the field.
The serial number is the 10-digit number located on the back of the Security Device.

Security Device serial number *

You must now authenticate with HSBCnet using your Security Device by generating a security code using the Security Device and inputting it to the field.

Step 1: Switch on your Security Device.

Step 2: Input your PIN number.

Step 3: Enter the security code the Security Device generates in the space provided.

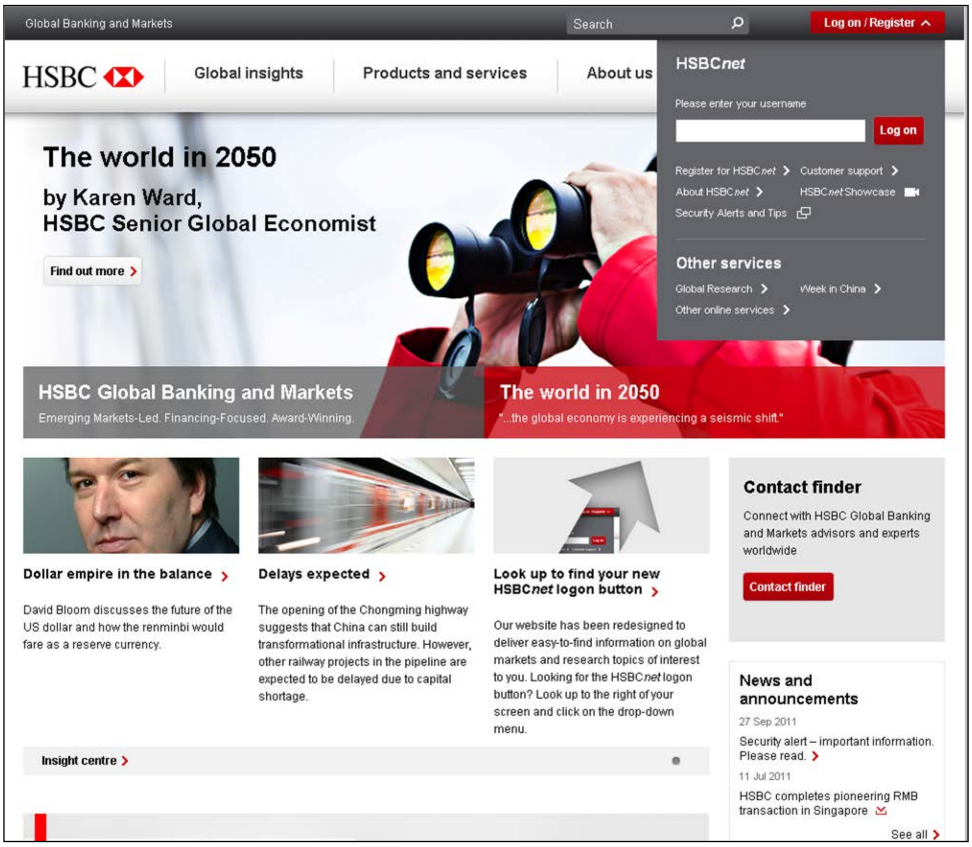
Step 4: Click on Continue. Your Security Device will be successfully activated and you will be taken to the HSBCnet logon page where you can now logon using your Security Device. We recommend that you spend a few minutes familiarising yourself with the help text relating to the use of your Security Device and in particular the section entitled Important Security Guidance before logging in.

Security Device code *

9. On the top right corner of the HSBC*net* home page, select **Log on/Register.** A drop-down window appears.

10. Enter your username and select **Log on**.

HSBCnet Home page



HSBC*net*

Please enter your username

The world in 2050

by Karen Ward,
HSBC Senior Global Economist

HSBC Global Banking and Markets

Emerging Markets-Led. Financing-Focused. Award-Winning.

The world in 2050

"...the global economy is experiencing a seismic shift."

Dollar empire in the balance

David Bloom discusses the future of the US dollar and how the renminbi would fare as a reserve currency.

Delays expected

The opening of the Chongming highway suggests that China can still build transformational infrastructure. However, other railway projects in the pipeline are expected to be delayed due to capital shortage.

Look up to find your new HSBC*net* logon button

Our website has been redesigned to deliver easy-to-find information on global markets and research topics of interest to you. Looking for the HSBC*net* logon button? Look up to the right of your screen and click on the drop-down menu.

Contact finder

Connect with HSBC Global Banking and Markets advisors and experts worldwide

News and announcements

27 Sep 2011

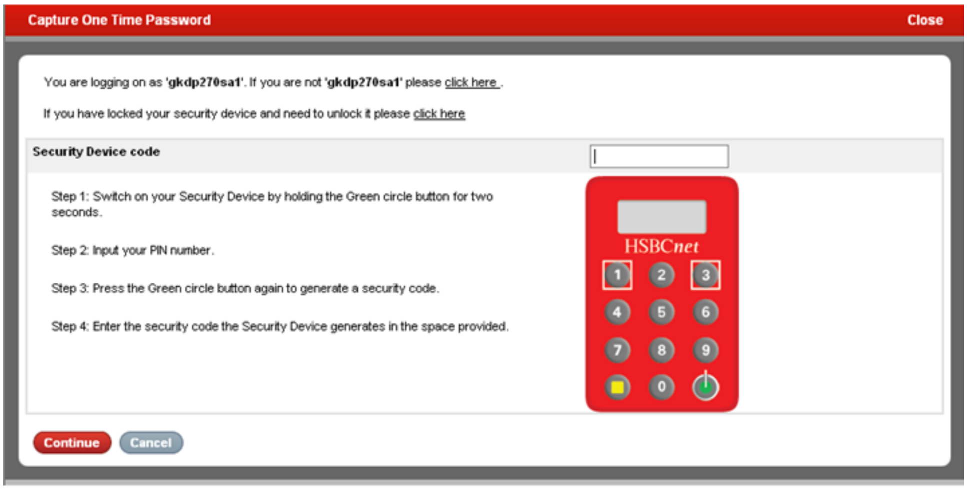
Security alert – important information. Please read.

11 Jul 2011

HSBC completes pioneering RMB transaction in Singapore

11. In the future, every time you log on, authenticate yourself using the security code generated by the device. You do not need your memorable answer and password unless you are making changes to your personal profile or security information.

Security Device authentication page



You are logging on as '**gkdp270sa1**'. If you are not '**gkdp270sa1**' please click here .

If you have locked your security device and need to unlock it please click here

Security Device code

Step 1: Switch on your Security Device by holding the Green circle button for two seconds.

Step 2: Input your PIN number.

Step 3: Press the Green circle button again to generate a security code.

Step 4: Enter the security code the Security Device generates in the space provided.

Note: The first time you log on after activating your Security Device, you will be notified of the HSBC*net* Terms and Conditions. Read the document carefully and select **I accept** to display your personal page and begin using the services.

Initial log on by new System Administrators or new End Users

If you are a new System Administrator or End User and are logging on for the first time, you need to complete the following steps to activate your Security Device. Refer to the section on Activating your Security Device for more information.

Subsequent log on by all users

Except for the initial log on, complete the following steps to authenticate your Security Device when logging on or authorising transactions and/or administrative changes.

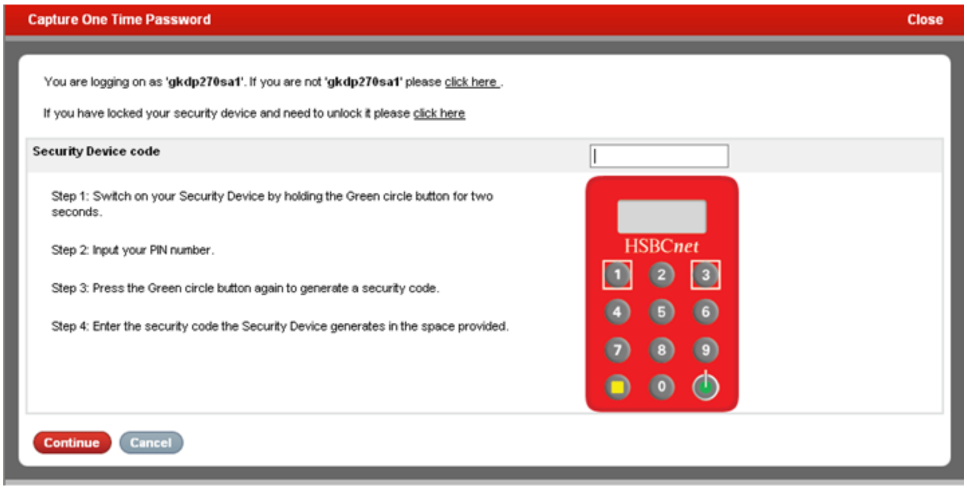
1. To turn on your Security Device press and hold the Green circle button in the bottom right corner of the last row of the keypad for two seconds.

2. Using the Device key pad, enter your PIN.

3. Enter the security code displayed in the window of the device into the on-screen **Security code** field. Select **Continue** to proceed.

Note: The security code is only valid for a few seconds. If you get an error message, generate a new security code by repeating steps 1 to 3.

Security Device authentication page



Capture One Time Password

Close

You are logging on as '**gkdp270sa1**'. If you are not '**gkdp270sa1**' please click here .

If you have locked your security device and need to unlock it please click here

Security Device code

Step 1: Switch on your Security Device by holding the Green circle button for two seconds.

Step 2: Input your PIN number.

Step 3: Press the Green circle button again to generate a security code.

Step 4: Enter the security code the Security Device generates in the space provided.

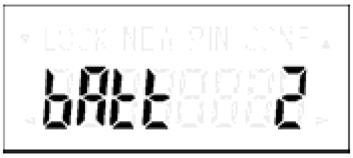
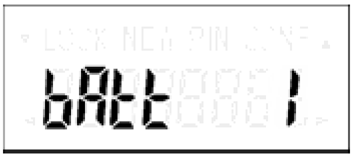
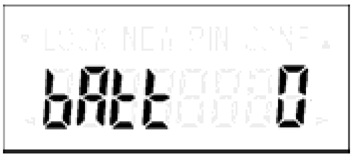
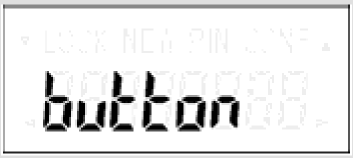
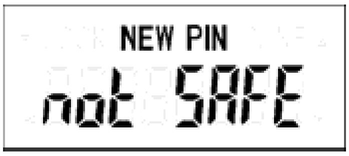
Authorising administrative changes

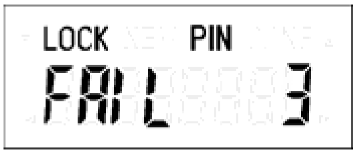
You are required to authenticate yourself when authorising administrative changes. Follow the same authentication steps as listed in the Subsequent log on by all users section above.

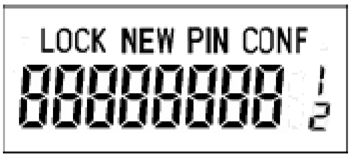
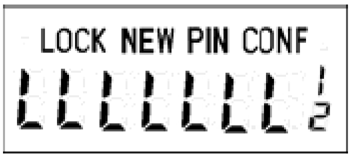
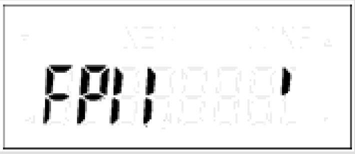
Troubleshooting Security Devices

Use the information and examples in the table below to troubleshoot issues you may encounter when using your new Security Device. This guide only applies to Users with the Security Device shown here.

For detailed information about using Security Devices refer to the relevant sections in this guide. System Administrators can get detailed information about managing Security Devices from the **System Administration: User Management** User Guide.

Message Displayed	SYMPTOM	PROBABLE CAUSES	ACTION REQUIRED
  	**bAtt 2** message followed by **bAtt1** and **bAtt0** messages appear in the device window	This is a low battery message. The low battery counter starts at 2 indicating a battery life of about 2 months. After its first appearance, the **bAtt** message appears for 2 seconds each time the device is powered on. After 2 seconds the device resumes normal operation.	Request your System Administrator to allocate a new Security Device. Your existing Security Device must first be deactivated before a new device can be allocated. **Note**: Please dispose of the deactivated device in an environmentally safe manner.
	**button** message appears in the device window	This indicates that a button is being pressed and held (accidentally) for a certain time (between 7-9 seconds). It results in the device switching off to preserve battery life.	Ensure that a button is not being accidentally held down.
	When selecting a new PIN a **not SAFE** message appears briefly in the device window before reverting to **NEW PIN** message.	The new PIN you have selected is unsafe or weak.	Resume selecting a new PIN and ensure that the PIN you select does not contain numbers that are repetitive or sequential (example 11111 or 123456). **Note**: The new PIN should be 4 to 8 digits in length

Message Displayed	SYMPTOM	PROBABLE CAUSES	ACTION REQUIRED
   	PIN FAIL message appears in the device window (for example, **PIN FAIL 1**, **PIN FAIL 2**, **PIN FAIL 3**)	1. You have entered an invalid PIN.	1. Press the Green circle button briefly and when prompted, enter the correct PIN again
		2. Lost or forgotten PIN	2. Reset your Security Device PIN. To unlock the device, refer to the section on Resetting your Security Device PIN in this User Guide.
		3. The Security Device may not have been allocated to you.	3. Check with your System Administrator to ensure the device you are using is allocated to you.
 	When entering the unlock code into the device, it displays a **LOCK PIN FAIL** message. (for example, **LOCK PIN FAIL 1**, **LOCK PIN FAIL 2**)	You have entered the incorrect unlock code	Wait for the device to turn off. Press the Green Circle button briefly and, when prompted, enter the correct unlock code again.
	1. When unlocking my Security Device, it displays a **LOCK PIN FAIL 3** message which will not go away.	1. You have entered the unlock code incorrectly into the device three times. As a result, for security reasons, you will not be allowed to operate the device for one hour. (also called **Unlock Retry Delay** period) If after one hour, you again enter the incorrect unlock code, the device will display a **LOCK PIN FAIL 4** message preventing you from operating the device for an additional hour (you have to wait for two hours before you can again attempt to enter the unlock code). This will continue to occur for up to 6 hours if you keep entering the incorrect unlock code.	1. Wait till the device turns off after the **Unlock Retry Delay** period. Press the Green Circle button to turn on the device. Then enter the correct Unlock Code. Note: The **Unlock Retry Delay** period is determined by the number of unsuccessful attempts to enter the unlock code.
	2. The Device displays a **LOCK PIN FAIL 3** message briefly before displaying an 7-digit code.	2. You have entered the incorrect PIN three times and your device is locked for security reasons	2. Unlock your device and reset your Security Device PIN. To unlock the device, refer to the section on Resetting your Security Device PIN in this User Guide.
	When entering a new PIN a second time to confirm, my Security Device displays a **FAIL Pin** message	The PIN you have entered does not match the previous PIN entry.	Ensure that the PIN you have entered matches the previous entry.

Message Displayed	SYMPTOM	PROBABLE CAUSES	ACTION REQUIRED
 	The Device window displays multiple incoherent messages one after another (see some sample messages on the left)	The device is no longer working.	1. Ask your System Administrator to deactivate the device and issue a new device. 2. Ask your System Administrator to contact your local HSBC*net* Support Helpdesk to record this issue.
	The Device window displays messages with incomplete characters	The device display is no longer working.	1. Ask your System Administrator to deactivate the device and issue a new device. 2. Ask your System Administrator to contact your local HSBC*net* Support Helpdesk to record this issue.
This message appears on HSBC*net* **"Error(s) occurred. The details you have entered do not match our records. We may suspend access to your service if there are too many unsuccessful attempts to log on. (LOG_0010)"**	HSBC*net* does not recognise the security code entered.	1. The Security Device may not have been allocated to you.	1. Check with your System Administrator to ensure the device you are using is allocated to you.
		2. Security code has timed out. Each generated code is only valid for a few seconds.	2. Turn off and turn on the Security Device and generate a new code. Enter this code immediately into the on-screen field.
		3. Security Device needs re-synchronising	3. System Administrator must resynchronise the Device. For information on how to resynchronise a Security Device, refer to the **System Administration: User Management** User Guide.
Not applicable	User Security Device has been lost or cannot be accounted for	User has lost or not returned his/her Security Device.	Deactivate the Security Device, and if necessary, set up the User with a new Security Device. For information on how to deactivate a security device, refer to the **System Administration: User Management** User Guide.

Password only Guide

About Password only authentication

HSBC*net* customers with Mixed Security profile can set up Users with Password Only authentication option. This will allow such Users to log on to HSBC*net* to enquire on the customer's banking information without using a physical device (Smart Card or Security Device). However, these Users will not be able to access any transaction banking tools which require a Smart Card or Security Device.

Note: Customers with Security Device profile cannot set up a User with **Password Only** authentication.

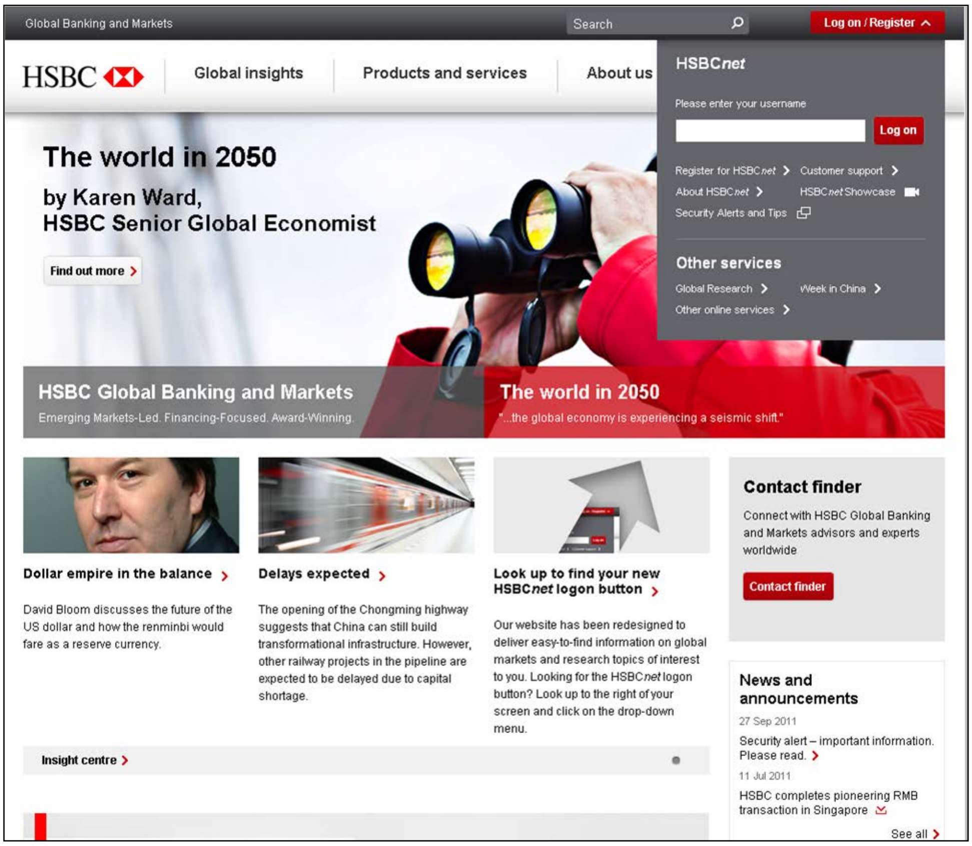
Using Password only to access HSBC*net*

To log on to HSBC*net* using only your Username and Password, compete the following steps:

1. On the top right corner of the HSBC*net* home page, select **Log on/Register**. A drop-down window appears.

2. Enter your username and select **Log on.**

HSBCnet Home page



The world in 2050

by Karen Ward,
HSBC Senior Global Economist

HSBC Global Banking and Markets

Emerging Markets-Led. Financing-Focused. Award-Winning.

The world in 2050

"...the global economy is experiencing a seismic shift."

Dollar empire in the balance

David Bloom discusses the future of the US dollar and how the renminbi would fare as a reserve currency.

Delays expected

The opening of the Chongming highway suggests that China can still build transformational infrastructure. However, other railway projects in the pipeline are expected to be delayed due to capital shortage.

Look up to find your new HSBC*net* logon button

Our website has been redesigned to deliver easy-to-find information on global markets and research topics of interest to you. Looking for the HSBC*net* logon button? Look up to the right of your screen and click on the drop-down menu.

Contact finder

Connect with HSBC Global Banking and Markets advisors and experts worldwide

News and announcements

27 Sep 2011

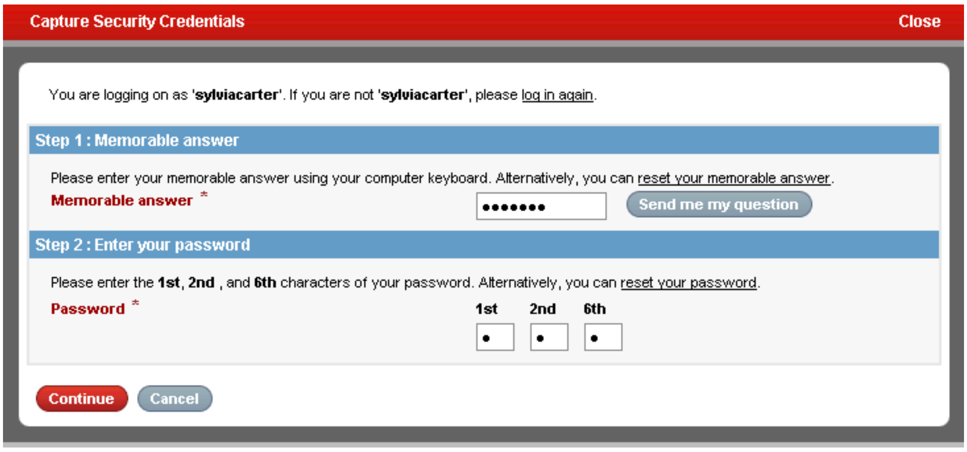
Security alert – important information. Please read.

11 Jul 2011

HSBC completes pioneering RMB transaction in Singapore

3. On the Capture Security Credentials page, enter your memorable answer. Next, enter the three requested characters of your password. Select **Continue** to proceed.

Capture Security Credentials page



You are logging on as '**sylviacarter**'. If you are not '**sylviacarter**', please log in again.

Step 1 : Memorable answer

Please enter your memorable answer using your computer keyboard. Alternatively, you can reset your memorable answer.

Memorable answer * ●●●●●●●

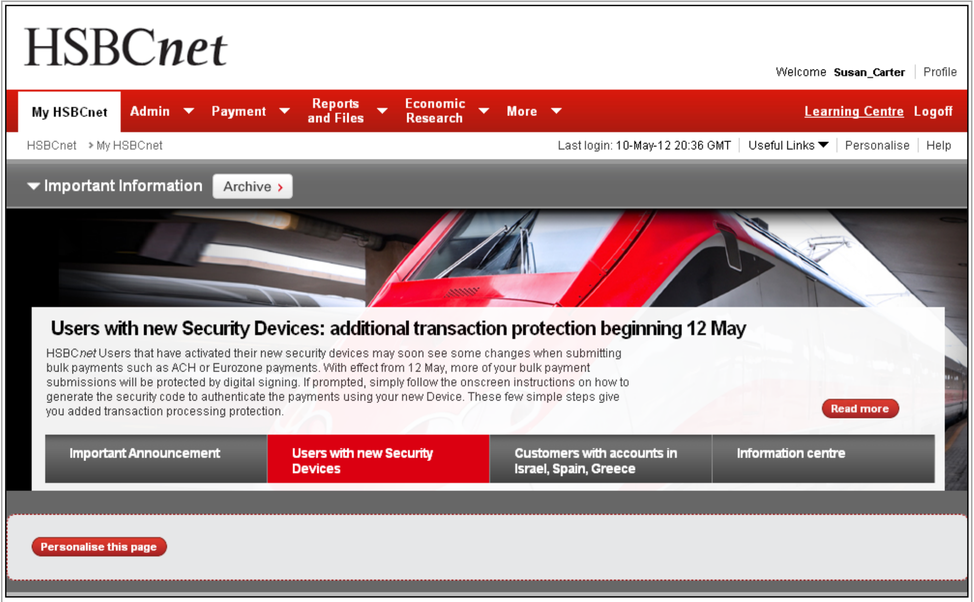
Step 2 : Enter your password

Please enter the **1st**, **2nd** , and **6th** characters of your password. Alternatively, you can reset your password.

Password * **1st** ● **2nd** ● **6th** ●

4. If the information you provided is correct, your HSBC*net* Personal page appears.

HSBCnet Personal page



Users with new Security Devices: additional transaction protection beginning 12 May

HSBC*net* Users that have activated their new security devices may soon see some changes when submitting bulk payments such as ACH or Eurozone payments. With effect from 12 May, more of your bulk payment submissions will be protected by digital signing. If prompted, simply follow the onscreen instructions on how to generate the security code to authenticate the payments using your new Device. These few simple steps give you added transaction processing protection.

Read more
Important Announcement
Users with new Security Devices
Customers with accounts in Israel, Spain, Greece
Information centre
Personalise this page

Resetting security information

During initial log on, you are required to provide correct security information to authenticate yourself. If your authentication is successful, you are only required to provide your security code to authenticate subsequent log on attempts or allowed to reset your Security Device PIN.

However, if you forget or provide incorrect security information, you are directed to reset your security information. Resetting security information involves two different processes.

- Online Reset (performed by User)
- Offline Reset (performed by System Administrators)

Note: After the initial log on, Security Device Users can update/reset their security information using **Edit My Profile** feature.

Online Reset during Initial Log on

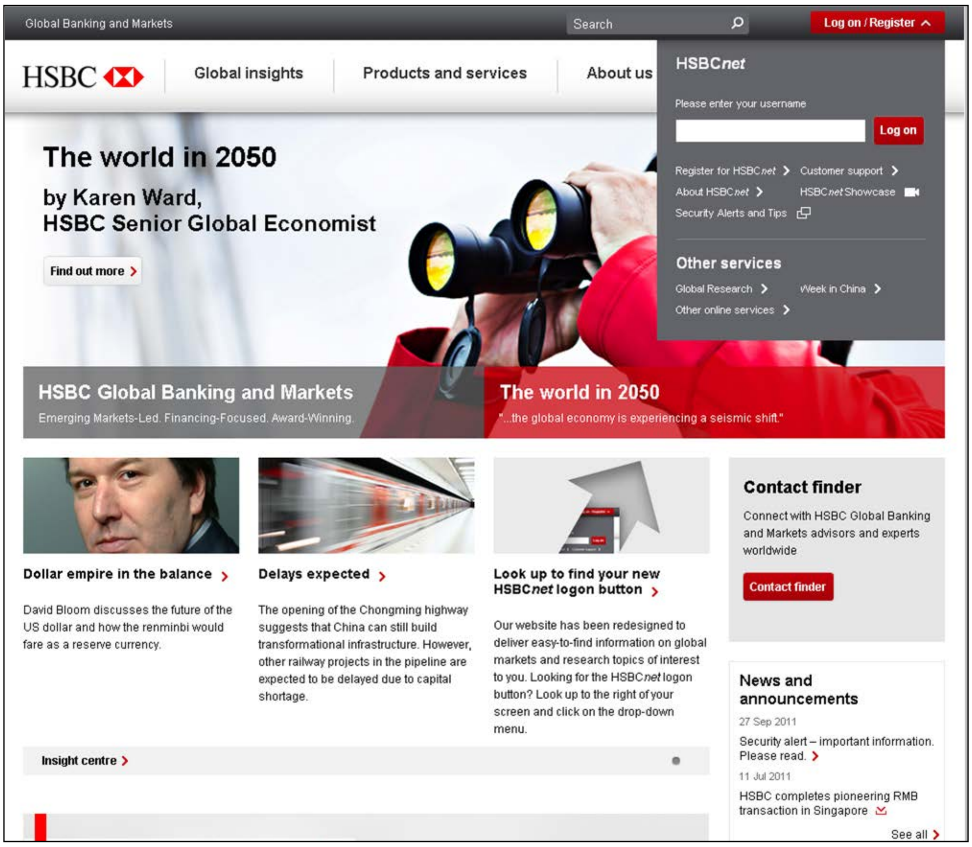
If during log on, you provide incorrect security information such as memorable answer and/or password, you are directed to reset that security information online by answering the security questions selected by you during registration. Such security information reset is immediate and does not require approval by your System Administrator(s). This process of resetting security information is called Online Reset.

To do an Online Reset of your security information during initial log on, complete the following steps.

1. On the top right corner of the HSBC*net* home page, select **Log on/Register**. A drop-down window appears.

2. Enter your username and select **Log on.**

HSBCnet Home page



Global Banking and Markets

Search

Log on / Register

HSBC

Global insights

Products and services

About us

HSBC*net*

Please enter your username

Log on

Register for HSBC*net* >

Customer support >

About HSBC*net* >

HSBC*net* Showcase

Security Alerts and Tips

Other services

Global Research >

Week in China >

Other online services >

The world in 2050

by Karen Ward,
HSBC Senior Global Economist

Find out more >

HSBC Global Banking and Markets

Emerging Markets-Led. Financing-Focused. Award-Winning.

The world in 2050

"...the global economy is experiencing a seismic shift."

Dollar empire in the balance >

David Bloom discusses the future of the US dollar and how the renminbi would fare as a reserve currency.

Delays expected >

The opening of the Chongming highway suggests that China can still build transformational infrastructure. However, other railway projects in the pipeline are expected to be delayed due to capital shortage.

Look up to find your new HSBC*net* logon button >

Our website has been redesigned to deliver easy-to-find information on global markets and research topics of interest to you. Looking for the HSBC*net* logon button? Look up to the right of your screen and click on the drop-down menu.

Contact finder

Connect with HSBC Global Banking and Markets advisors and experts worldwide

Contact finder

News and announcements

27 Sep 2011

Security alert – important information. Please read. >

11 Jul 2011

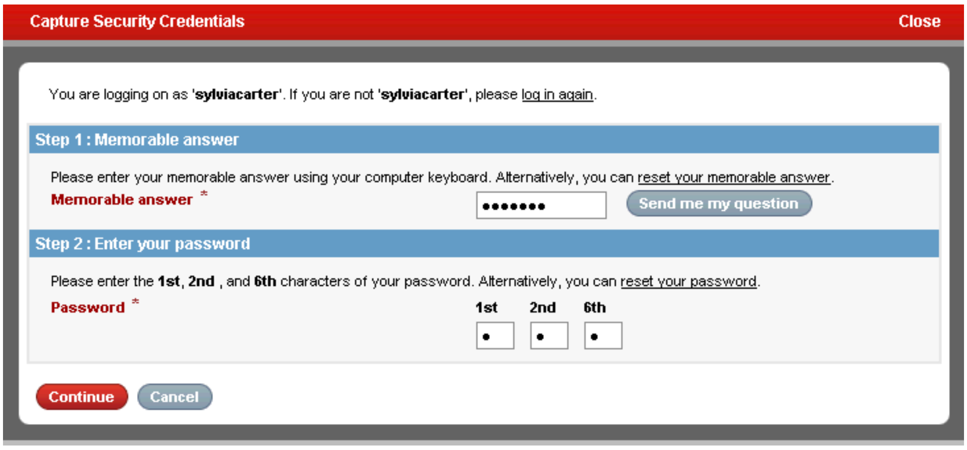
HSBC completes pioneering RMB transaction in Singapore

See all >

Insight centre >

3. On the Capture Security Credentials page, enter your memorable answer. Then enter the three requested characters of your current password. Select **Continue** to proceed.

Online Reset: Enter memorable answer and password



Capture Security Credentials

Close

You are logging on as '**sylviacarter**'. If you are not '**sylviacarter**', please log in again.

Step 1 : Memorable answer

Please enter your memorable answer using your computer keyboard. Alternatively, you can reset your memorable answer.

Memorable answer * ●●●●●●●

Send me my question

Step 2 : Enter your password

Please enter the **1st**, **2nd** , and **6th** characters of your password. Alternatively, you can reset your password.

Password *

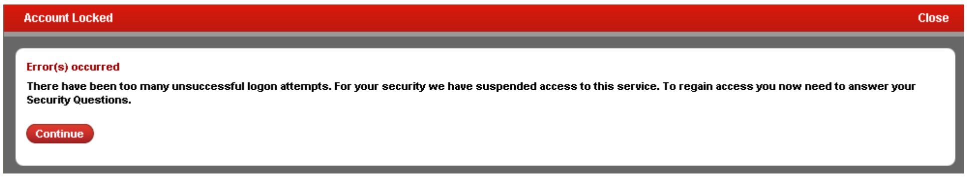
1st	2nd	6th
●	●	●

Continue

Cancel

4. If you entered the incorrect security information (memorable answer, password) three times, the following error message appears and you are presented with the Online Reset options.

Online Reset: Error message



Account Locked

Close

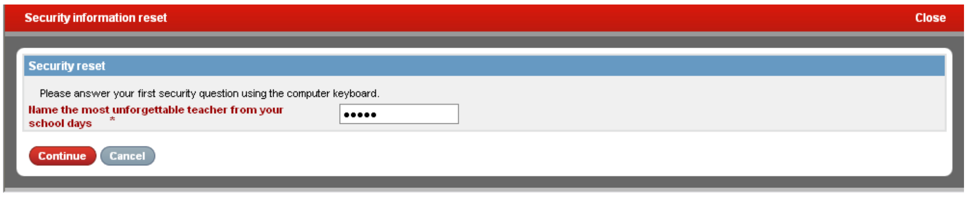
Error(s) occurred

There have been too many unsuccessful logon attempts. For your security we have suspended access to this service. To regain access you now need to answer your Security Questions.

Continue

5. Answer the first security question correctly. The second security question appears.

Online Reset: First security question



Security information reset

Close

Security reset

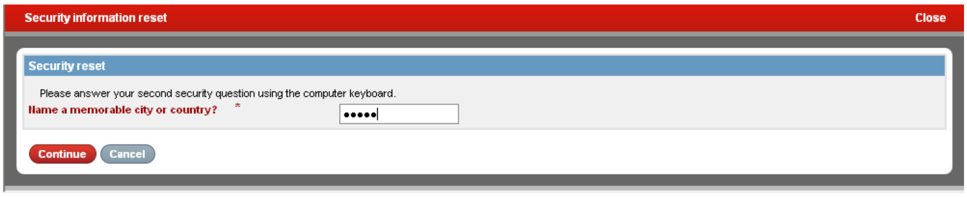
Please answer your first security question using the computer keyboard.

Name the most unforgettable teacher from your school days * •••••

Continue Cancel

6. Answer the second security question. The memorable answer **OR** the password page (depending on which one you entered incorrectly) appears.

Online Reset: Second security question



Security information reset

Close

Security reset

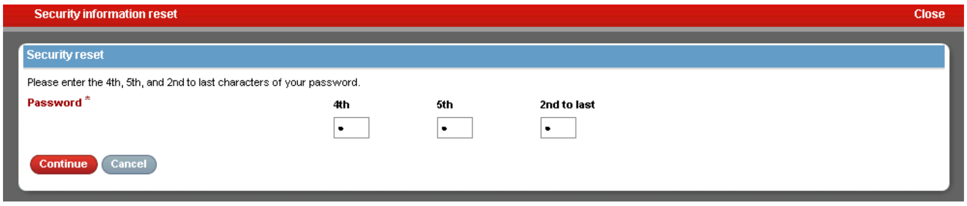
Please answer your second security question using the computer keyboard.

Name a memorable city or country? * •••••

Continue Cancel

7. Enter the three requested characters of your current password.

Online Reset: Enter password



Security information reset

Close

Security reset

Please enter the 4th, 5th, and 2nd to last characters of your password.

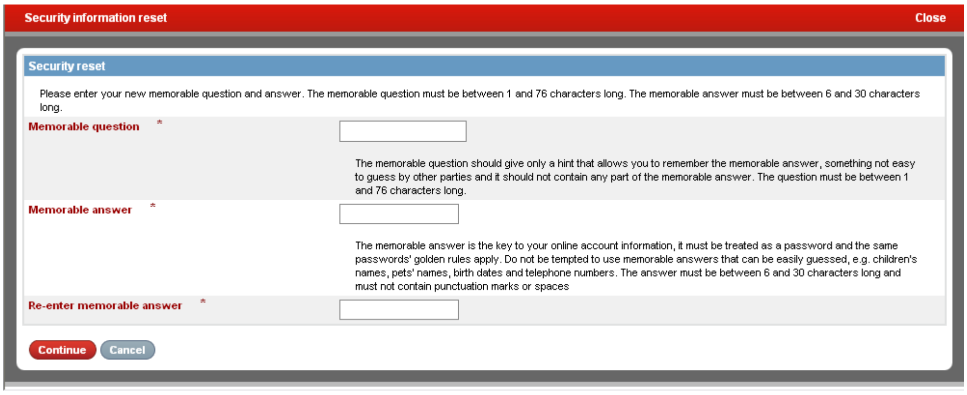
	4th	5th	2nd to last
Password *	•	•	•

Continue Cancel

8. Depending on which security information you entered incorrectly (memorable answer or password), you are required to reset that incorrect information. Accordingly, the memorable answer OR password reset page appears.

    - Reset your password, OR
    - Reset your memorable answer

Online Reset: Reset your memorable answer



Please enter your new memorable question and answer. The memorable question must be between 1 and 76 characters long. The memorable answer must be between 6 and 30 characters long.

Memorable question *

The memorable question should give only a hint that allows you to remember the memorable answer, something not easy to guess by other parties and it should not contain any part of the memorable answer. The question must be between 1 and 76 characters long.

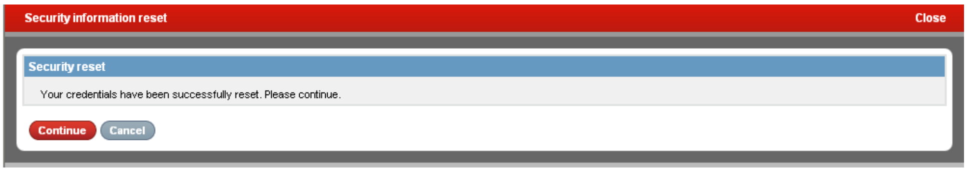
Memorable answer *

The memorable answer is the key to your online account information, it must be treated as a password and the same passwords' golden rules apply. Do not be tempted to use memorable answers that can be easily guessed, e.g. children's names, pets' names, birth dates and telephone numbers. The answer must be between 6 and 30 characters long and must not contain punctuation marks or spaces

Re-enter memorable answer *

9. An acknowledgment confirms your action.

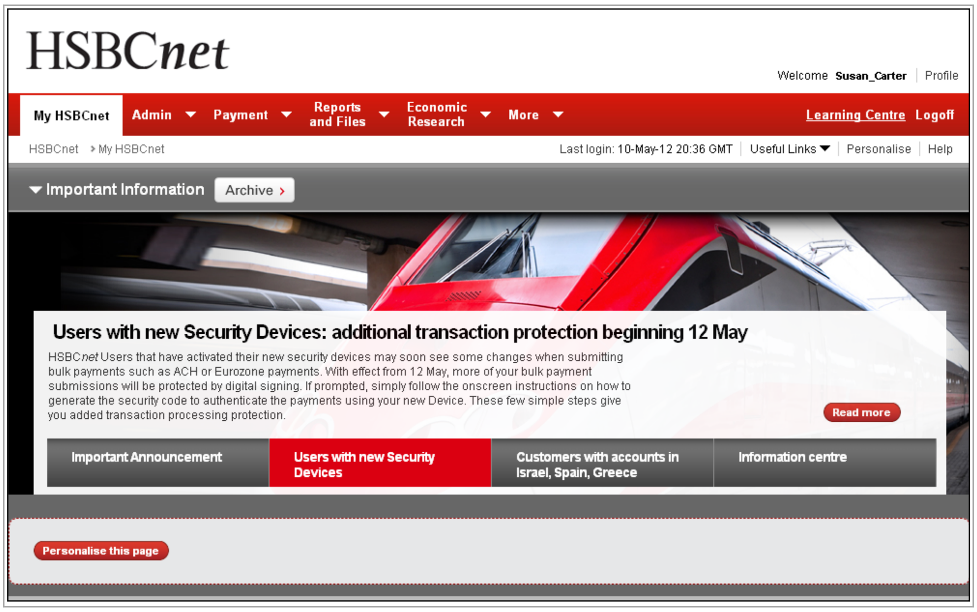
Online Reset: Successful reset acknowledgment



Your credentials have been successfully reset. Please continue.

10. You can log on again with your new security information.

Online Reset: HSBCnet personal page



Last login: 10-May-12 20:36 GMT

Users with new Security Devices: additional transaction protection beginning 12 May

HSBC*net* Users that have activated their new security devices may soon see some changes when submitting bulk payments such as ACH or Eurozone payments. With effect from 12 May, more of your bulk payment submissions will be protected by digital signing. If prompted, simply follow the onscreen instructions on how to generate the security code to authenticate the payments using your new Device. These few simple steps give you added transaction processing protection.

Offline Reset (OFR) during Initial Log on

If during initial log on, you provide incorrect security information such as memorable answer and/or password, you are directed to reset that security information online (OLR) by answering the security questions selected by you during registration.

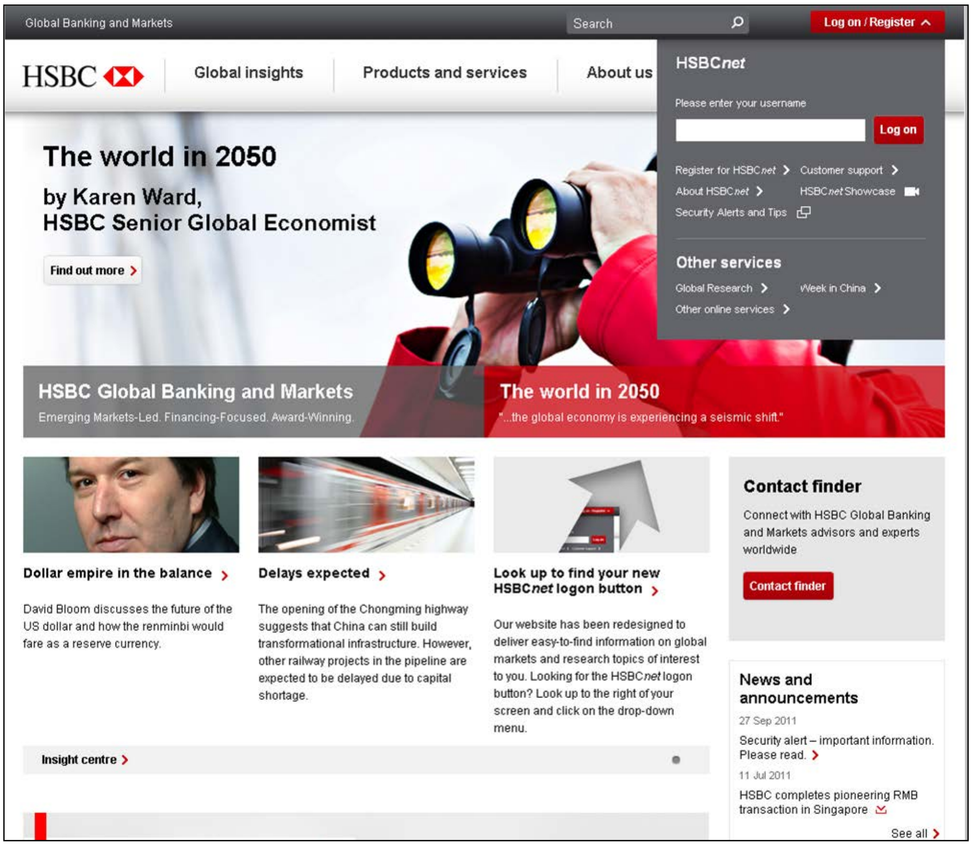
However, if you are unable to provide correct answers to the security questions and memorable answer or password, you are locked out of your HSBC*net* account. Online Reset is not available. You can then submit a Security Information Reset (SIR) form, allowing you to choose new security information. The SIR requires approval by your System Administrator(s). This process of resetting security information is called Offline Reset.

To do an Offline Reset of your security information, complete the following steps. Some steps may differ depending on your unique log on status or when you are resetting your security information from the **Edit My Profile** tool.

1. On the top right corner of the HSBC*net* home page, select **Log on/Register**.

2. Enter your username and select **Log on**.

Offline Reset: Log on



The world in 2050

by Karen Ward,
HSBC Senior Global Economist

HSBC Global Banking and Markets

Emerging Markets-Led. Financing-Focused. Award-Winning.

The world in 2050

"...the global economy is experiencing a seismic shift."

Dollar empire in the balance

David Bloom discusses the future of the US dollar and how the renminbi would fare as a reserve currency.

Delays expected

The opening of the Chongming highway suggests that China can still build transformational infrastructure. However, other railway projects in the pipeline are expected to be delayed due to capital shortage.

Look up to find your new HSBC*net* logon button

Our website has been redesigned to deliver easy-to-find information on global markets and research topics of interest to you. Looking for the HSBC*net* logon button? Look up to the right of your screen and click on the drop-down menu.

Contact finder

Connect with HSBC Global Banking and Markets advisors and experts worldwide

News and announcements

27 Sep 2011

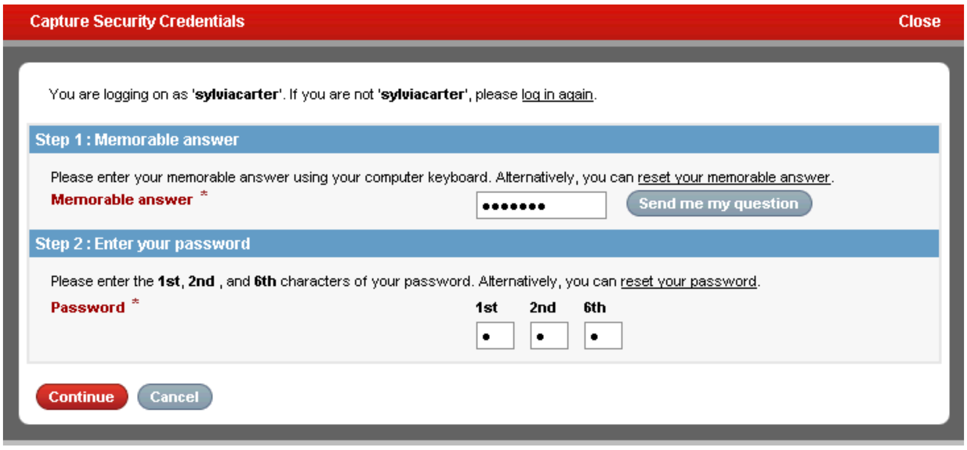
Security alert – important information. Please read.

11 Jul 2011

HSBC completes pioneering RMB transaction in Singapore

3. The Capture Security Credentials page appears. Enter your memorable answer. Enter the three requested characters of your password. Select **Continue** to proceed.

Offline Reset: Enter memorable answer and password



Capture Security Credentials — Close

You are logging on as '**sylviacarter**'. If you are not '**sylviacarter**', please log in again.

Step 1 : Memorable answer

Please enter your memorable answer using your computer keyboard. Alternatively, you can reset your memorable answer.

Memorable answer *	•••••••	Send me my question

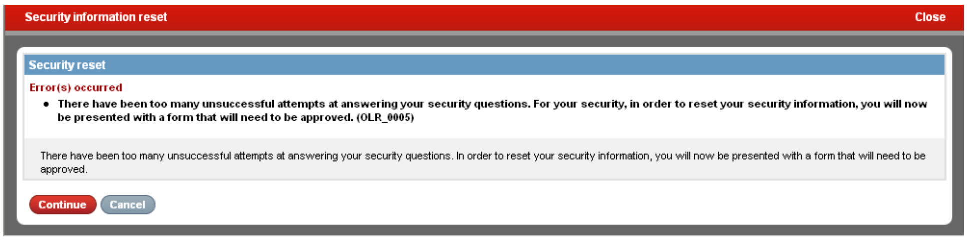
Step 2 : Enter your password

Please enter the **1st**, **2nd** , and **6th** characters of your password. Alternatively, you can reset your password.

	1st	2nd	6th
Password *	•	•	•

4. If you entered the incorrect security information (memorable answer, password) and also failed the Online Reset process, the following Account Locked error message appears. You are presented with the Offline Security Information Reset (SIR) form requiring you to reset all security information.

Offline Reset: Account Locked error message



Security information reset — Close

Security reset

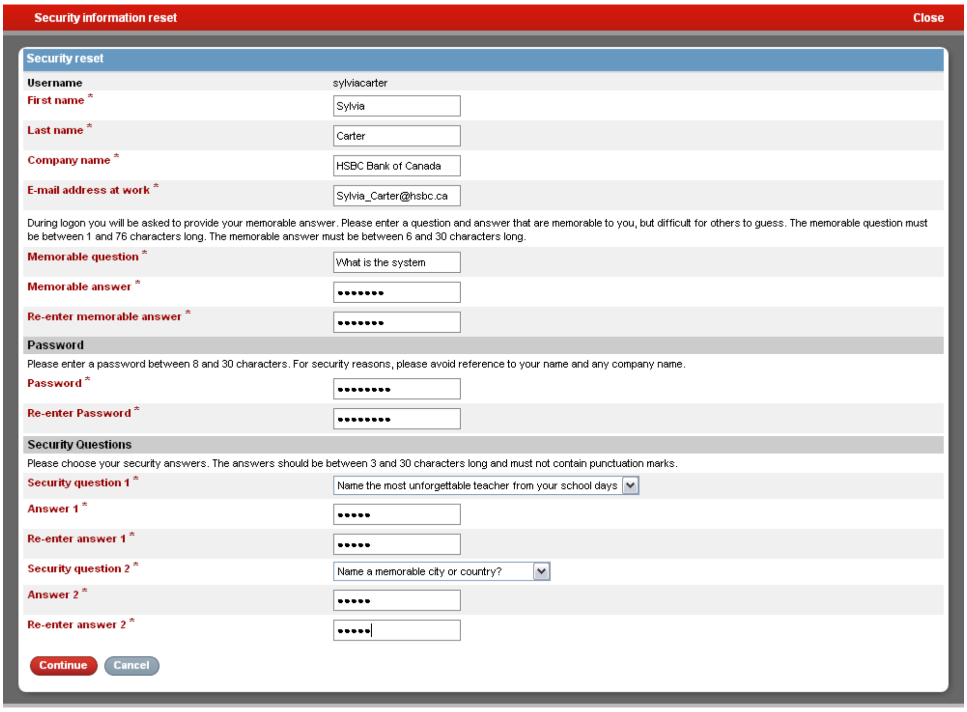
Error(s) occurred

- There have been too many unsuccessful attempts at answering your security questions. For your security, in order to reset your security information, you will now be presented with a form that will need to be approved. (OLR_0005)

There have been too many unsuccessful attempts at answering your security questions. In order to reset your security information, you will now be presented with a form that will need to be approved.

5. Complete the SIR form and select **Continue**. Mandatory information is marked with an asterisk (*).

Offline Reset: SIR form



Security information reset — Close

Security reset

Username	sylviacarter
First name *	Sylvia
Last name *	Carter
Company name *	HSBC Bank of Canada
E-mail address at work *	Sylvia_Carter@hsbc.ca

During logon you will be asked to provide your memorable answer. Please enter a question and answer that are memorable to you, but difficult for others to guess. The memorable question must be between 1 and 76 characters long. The memorable answer must be between 6 and 30 characters long.

Memorable question *	What is the system
Memorable answer *	•••••••
Re-enter memorable answer *	•••••••

Password

Please enter a password between 8 and 30 characters. For security reasons, please avoid reference to your name and any company name.

Password *	•••••••••
Re-enter Password *	•••••••••

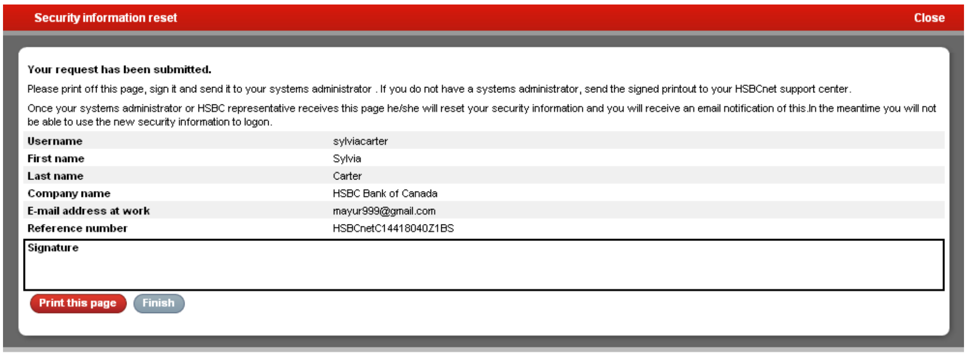
Security Questions

Please choose your security answers. The answers should be between 3 and 30 characters long and must not contain punctuation marks.

Security question 1 *	Name the most unforgettable teacher from your school days
Answer 1 *	•••••
Re-enter answer 1 *	•••••
Security question 2 *	Name a memorable city or country?
Answer 2 *	•••••
Re-enter answer 2 *	•••••

6. An acknowledgement confirms your submission. Print, sign and submit the page to your System Administrator.

Offline Reset: SIR submission acknowledgement



Your request has been submitted.

Please print off this page, sign it and send it to your systems administrator . If you do not have a systems administrator, send the signed printout to your HSBCnet support center.

Once your systems administrator or HSBC representative receives this page he/she will reset your security information and you will receive an email notification of this.In the meantime you will not be able to use the new security information to logon.

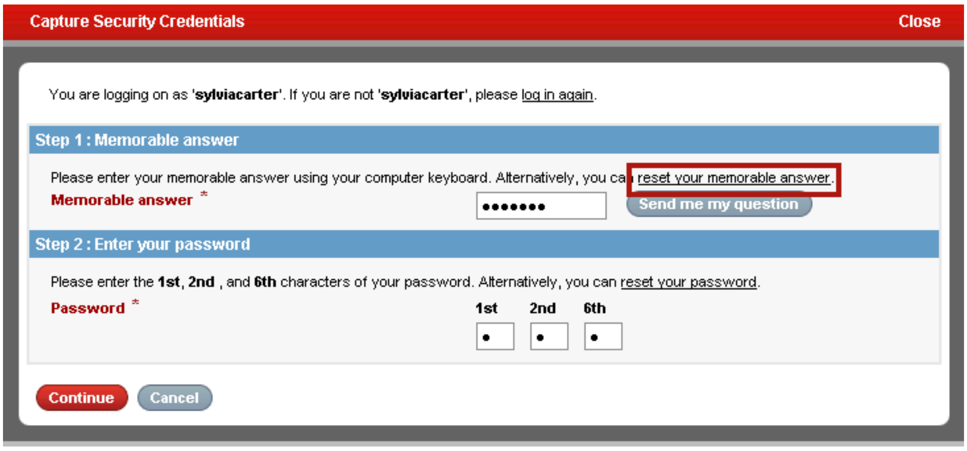
Username	sylviacarter
First name	Sylvia
Last name	Carter
Company name	HSBC Bank of Canada
E-mail address at work	mayur999@gmail.com
Reference number	HSBCnetC14418040Z1BS
Signature	

Note: The remaining procedure is completed by your System Administrator.

Resetting your memorable answer

During initial log on, if you do not remember your memorable answer, you can reset it from the Capture Security Credentials page before making any attempts to log on.

Memorable answer: Online Reset



You are logging on as '**sylviacarter**'. If you are not '**sylviacarter**', please log in again.

Step 1 : Memorable answer

Please enter your memorable answer using your computer keyboard. Alternatively, you ca reset your memorable answer.

Memorable answer * •••••••

Step 2 : Enter your password

Please enter the **1st**, **2nd** , and **6th** characters of your password. Alternatively, you can reset your password.

Password * **1st** • **2nd** • **6th** •

To reset your memorable answer, complete the following steps:

1. From the Capture Security Credentials page, select the **reset your memorable answer** link.

2. In the pages that follow, answer the first and second security questions and provide the three requested characters of your current password.

3. Choose a new memorable question and answer in the next page.

4. An acknowledgement confirms the successful reset of your credentials.

5. Proceed to your HSBC*net* personal page.

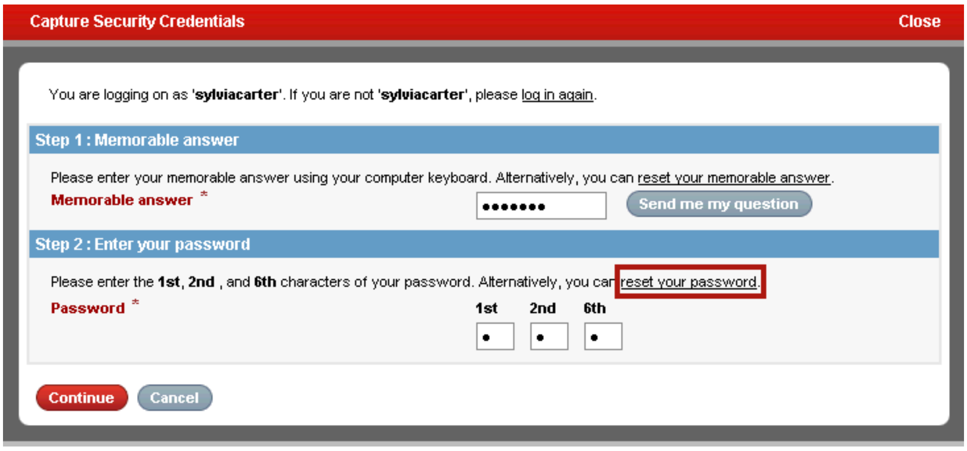
Memorable question and answer must conform to the following character rules:

- Memorable question must be one (1) to seventy-six (76) characters. Alphanumeric (A-Z, 0-9) plus special characters underscore (_), hyphen (-), space ( ), apostrophe (‘), and period (.)
- Memorable answer must be six (6) to thirty (30) characters. Alphanumeric (A-Z, 0-9) plus special characters (@), underscore (_), hyphen (-), space ( ), apostrophe (‘) and period (.). It must not be the same as the existing memorable answer

Resetting your password

During initial log on, if you do not remember your password, you can reset it from the Capture Security Credentials page before making any attempts to log on.

Password: Online Reset



Capture Security Credentials

You are logging on as '**sylviacarter**'. If you are not '**sylviacarter**', please log in again.

Step 1 : Memorable answer

Please enter your memorable answer using your computer keyboard. Alternatively, you can reset your memorable answer.

Memorable answer * •••••••

Step 2 : Enter your password

Please enter the **1st**, **2nd** , and **6th** characters of your password. Alternatively, you can reset your password.

Password * 1st • 2nd • 6th •

To reset your password, complete the following steps:

1. From the Capture Security Credentials page, select the **reset your password** link.
2. In the pages that follow, answer the first and second security questions, and provide your memorable answer.
3. Choose a new password in the next page.
4. An acknowledgement confirms the successful reset of your credentials.
5. Proceed to your HSBC*net* personal page. New password chosen must be eight (8) to thirty (30) characters, alpha-numeric (A-Z, 0-9). It must not be the same as the existing password.

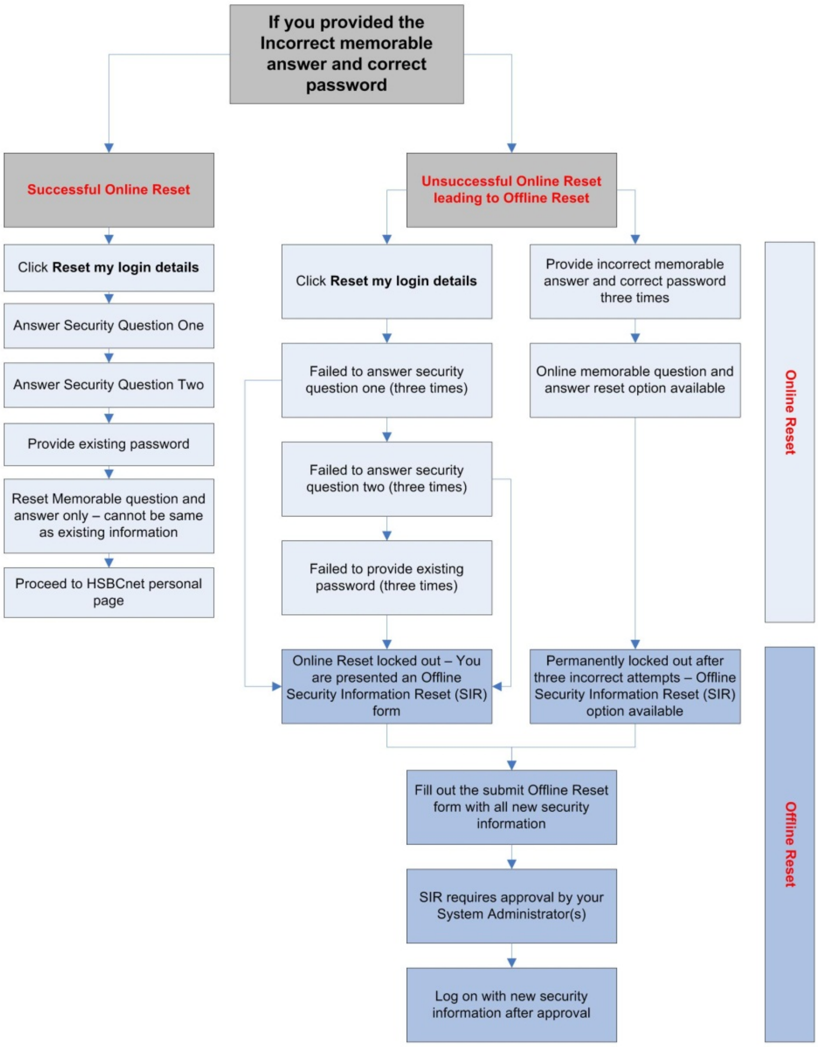
Resetting your security information—Scenarios

During the initial log on process, if an error message appears, you may have entered incorrect security information. Depending on your current log on status, use one of the following scenarios as a guide to reset your security information.

- Incorrect memorable answer and correct password
- Correct memorable answer and incorrect password

Incorrect memorable answer and correct password

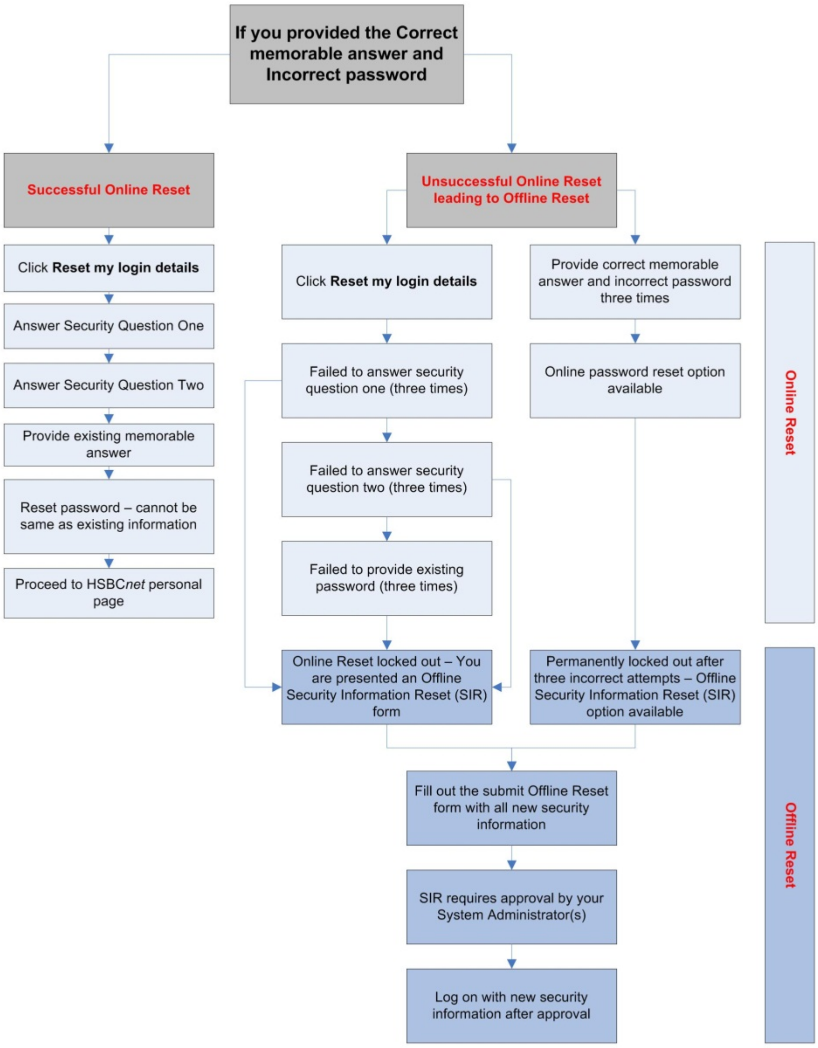
If, during the initial log on process, you provided an incorrect memorable answer but correct password, you could either complete an online or offline security information reset. Refer to the following figure for one of three step-by-step processes to reset your security information.


If you provided the Incorrect memorable answer and correct password
Successful Online Reset
Click **Reset my login details**
Answer Security Question One
Answer Security Question Two
Provide existing password
Reset Memorable question and answer only – cannot be same as existing information
Proceed to HSBCnet personal page
Unsuccessful Online Reset leading to Offline Reset
Click **Reset my login details**
Failed to answer security question one (three times)
Failed to answer security question two (three times)
Failed to provide existing password (three times)
Online Reset locked out – You are presented an Offline Security Information Reset (SIR) form
Provide incorrect memorable answer and correct password three times
Online memorable question and answer reset option available
Permanently locked out after three incorrect attempts – Offline Security Information Reset (SIR) option available
Fill out the submit Offline Reset form with all new security information
SIR requires approval by your System Administrator(s)
Log on with new security information after approval
Online Reset
Offline Reset

Note: Offline Reset of your security information is completed by your System Administrator.

Correct memorable answer and incorrect password

If, during the initial log on process, you provided a correct memorable answer but incorrect password, you could either complete an online or offline security information reset. Refer to the following figure for one of three step-by-step processes to reset your security information.


If you provided the Correct memorable answer and Incorrect password
Successful Online Reset
Click **Reset my login details**
Answer Security Question One
Answer Security Question Two
Provide existing memorable answer
Reset password – cannot be same as existing information
Proceed to HSBC*net* personal page
Unsuccessful Online Reset leading to Offline Reset
Click **Reset my login details**
Failed to answer security question one (three times)
Failed to answer security question two (three times)
Failed to provide existing password (three times)
Online Reset locked out – You are presented an Offline Security Information Reset (SIR) form
Provide correct memorable answer and incorrect password three times
Online password reset option available
Permanently locked out after three incorrect attempts – Offline Security Information Reset (SIR) option available
Fill out the submit Offline Reset form with all new security information
SIR requires approval by your System Administrator(s)
Log on with new security information after approval
Online Reset
Offline Reset

Note: Offline Reset of your security information is completed by your System Administrator.

Issued by HSBC Bank plc