RESERVE BANK INFORMATION AND TRANSFER SYSTEM

RITS Access and Security User Guide

October 2013

1. GETTING STARTED

1.1 Overview

This document is a guide to the process and procedures for accessing RITS. It covers:

- the preparations necessary to gain network connectivity to RITS;
- providing users' PCs with the RITS software;
- the administration of the RITS token;
- creating new users;
- obtaining RITS digital certificates for existing and new users;
- password and certificate administration; and
- the revocation and expiry of RITS digital certificates.

RITS functions discussed in this guide are explained in the *Member Administration User Guide*.

1.2 Public Key Infrastructure

RITS has adopted Public Key Infrastructure (PKI), together with Secure Socket Layer (SSL) technology, to provide a strong access control regime in terms of:

Authentication – The system restricts access to authorised users based on a valid RITS digital certificate and Token Codeword. **Confidentiality** – Using SSL encryption, data exchanged between RITS and Members are protected from unauthorised scrutiny.

Integrity – Data exchanged between RITS and Members are encrypted and digitally signed, protecting it from modification.

Protection from repudiation – The Member sending an update action to RITS cannot deny having created and sent that instruction. Update actions are digitally signed and logged to provide a record of the communication and details of the Member and user responsible for the action.

Technical information on the use of RITS tokens and certificates and implications for Members' environments is provided in the *RITS Technical Information Paper*. This paper is available in the *RITS Information Facility* and on the RBA's website at: http://www.rba.gov.au/rits/info/pdf/RITS_UI-Technical_Information_Paper.pdf.

1.3 Member Security Obligations

RITS Regulations

The RITS Regulations sets out Member obligations with respect to the security of access to RITS. Key points are:

- Members must ensure that all their users are familiar with their obligations regarding certificate and token administration;
- Members are responsible for ensuring that each user's RITS digital certificate correctly identifies the user;
- Members are liable for all the update actions (e.g. change status, enter Cash Transfers) of their users in RITS;
- Users must keep their RITS password and Token Codeword secret. Users must have their own RITS token. Sharing of RITS tokens is a breach of security; and
- Members must immediately revoke a user's certificate in RITS if a user has shared the Token Codeword, or no longer requires access to RITS.

Password Administrator and Certificate Administrator

To control user access via RITS, Members must nominate users to assume the responsibilities of 'Password Administrator' and 'Certificate Administrator'. The same staff member can be responsible for both, or the responsibilities can be separated, depending on the internal security arrangements of the Member.

Password Administrators are responsible for resetting passwords, controlling the status of each user, allocating roles/functions to users, linking users to branches to perform transactions for those branches, and assigning the privilege to authorise. Certificate Administrators are responsible for activating each user's certificate after they enrol, and for revoking a user's certificate.

Members' Procedures

It is strongly suggested that Members establish appropriate system and procedural safeguards to ensure security and continuity of access to RITS. These include:

- encourage users to remove the RITS token from the PC when the user moves away from the PC or when the PC is not in use;
- encourage users to store the RITS token in a safe place when not in use;
- subject to the Member's own security policies, encourage users to carry the RITS token with them, including taking it home overnight;
- encourage users to apply screen locks on PCs to limit the possibility of one user signing transactions for another user who has moved away from their desk;
- prohibit keystroke logging on PCs used for RITS transactions;
- do not store RITS tokens containing certificates in a central safe;
- ensure spare RITS tokens are available at both the Member's primary site and disaster recovery site;

- ensure that users are able to collect certificates onto their RITS tokens and that PCs are configured to enable USB ports for the RITS tokens;

- advise users that they must not share RITS tokens, or disclose their logons or passwords or token codewords; and

- other measures as appropriate to the Member's business that ensure that the security of RITS access is protected.

Important Points for Users

Users should be aware that use of certificates means that all transactions, instructions, and updates that they submit to RITS for processing are automatically digitally signed even if it is not apparent from the user perspective that a signature has been created. The digital signature uniquely identifies the transaction, instruction or update, as the Member's, and the Member is responsible for it. A log is maintained in RITS of every signed transaction.

Users must make every effort to comply with system and procedural safeguards put in place by Members to protect the security of RITS access.

1.4 Access to RITS away from Worksite

Access to RITS from outside the normal working environment must be undertaken with care. This is because the normal security controls that exist in the work environment may not exist at other locations. Members should satisfy themselves that the arrangements that they have in place for access to RITS from outside the workplace are adequate.

1.5 Shared Email Addresses

The RBA very strongly recommends that RITS users have their own email address to receive security information as part of the certificate enrolment procedure. These procedures are designed to ensure that only the authorised user may enrol for the certificate issued in their name. The use of shared email addresses by a Member may weaken the very high security built into the RITS certificate issuance process, by exposing them to a greater risk of internal misconduct, with resulting unauthorised issuance and use of certificates. It also means that a user may not receive certificate expiry reminder emails.

Where a Member's internal policies or environment do not allow each RITS user to have an individual email address, the RBA will require a written acknowledgement from that Member (signed by two RITS authorised signatories), that they will not provide all users with individual email addresses, and will rely on other internal security controls. These might, for example, involve the following:

- that the Password Administrators will have their own individual email addresses to receive notice of revocation emails and expiry emails;

- the owner of the shared email address will not be a RITS user given the role of Password Administrator;

- that users will format their own RITS tokens and set a token codeword known only to themselves; and

- each individual RITS user will enrol (i.e. receive certificate) via the internet. This should not be done by any other person.

1.6 Training

New RITS users must undertake training in the use of RITS. Training can be provided by the RBA.

Users are also expected to complete activities in the Pre-Production Environment to further familiarise themselves with RITS. The checklist can be found in the *RITS Information Facility* or on the RBA website at:

http://www.rba.gov.au/rits/info/pdf/Checklist_for_Activities_in_the_Pre-Production_Environment.pdf

2. PREPARATIONS TO ACCESS RITS

2.1 Key Points

To access RITS the following steps must be taken:

- Establish connectivity to RITS from one typical user's PC.
- Roll out the RITS software, PC and browser configurations to the PCs of all RITS users.
- Check performance and adjust settings.

2.2 Establish Connectivity to RITS

Members of RITS are required to test that connectivity to RITS can be established over the Austraclear network (ANNI), the internet or both. The *Network Policy for RITS* details the policy adopted by the RBA for Member network access.

To assist with this, the *Guide to Connectivity Testing* and the *RITS Technical Information Paper* are available and the RBA will provide assistance as required.

The *RITS Technical Information Paper* describes the network, PC and browser configurations required to access RITS.

The *Guide to Connectivity Testing* describes how the software that is required on the user's PC can be obtained from a CD (obtained from the RITS Help Desk) or downloaded from the internet at http://www.rba.gov.au/rits/, and how to establish connectivity to RITS.

Requests to obtain the CD should be directed to the RITS Help Desk (on 1800 659 360).

2.3 Check Performance

Optimum performance of RITS can be obtained by using the PC and browser settings set out in the *Technical Information Paper*.

If you are experiencing slow response times consult your System Administrator or the RITS Help Desk.

3. RITS TOKEN ADMINISTRATION

3.1 Key Points

Use the **Token Administration** link to:

- **View certificates** on the RITS token, and their details (e.g. expiry date, name on certificate, Member name).
- **Format a RITS token** to set it up for use with RITS. If the RITS token has already been used, formatting a RITS token will delete all certificates (RITS or otherwise).
- **Change the Token Codeword**.
- **Delete certificates** that are expired or unwanted on the RITS token. The RITS token can hold up to 9 certificates.
- **Delete orphan keys** on the RITS token. These are keys created by the RITS token but the action was interrupted. These should be deleted as the RITS token has a very small memory space.

In a **contingency**, when attending a disaster recovery or backup site, the user should take their RITS token with them. If they fail to do so, the user's certificate will need to be revoked and the user will need to re-enrol and collect a new certificate to gain access to RITS. This will be very inconvenient in a contingency.

3.2 Obtaining a RITS Token, Including in a Contingency

RITS digital certificates must be downloaded directly onto a RITS token. Users can obtain a RITS token from their Password/Certificate Administrator. Supplies of the RITS tokens are available from the RITS Help Desk. Members should consider nominating a person to manage spare RITS tokens.

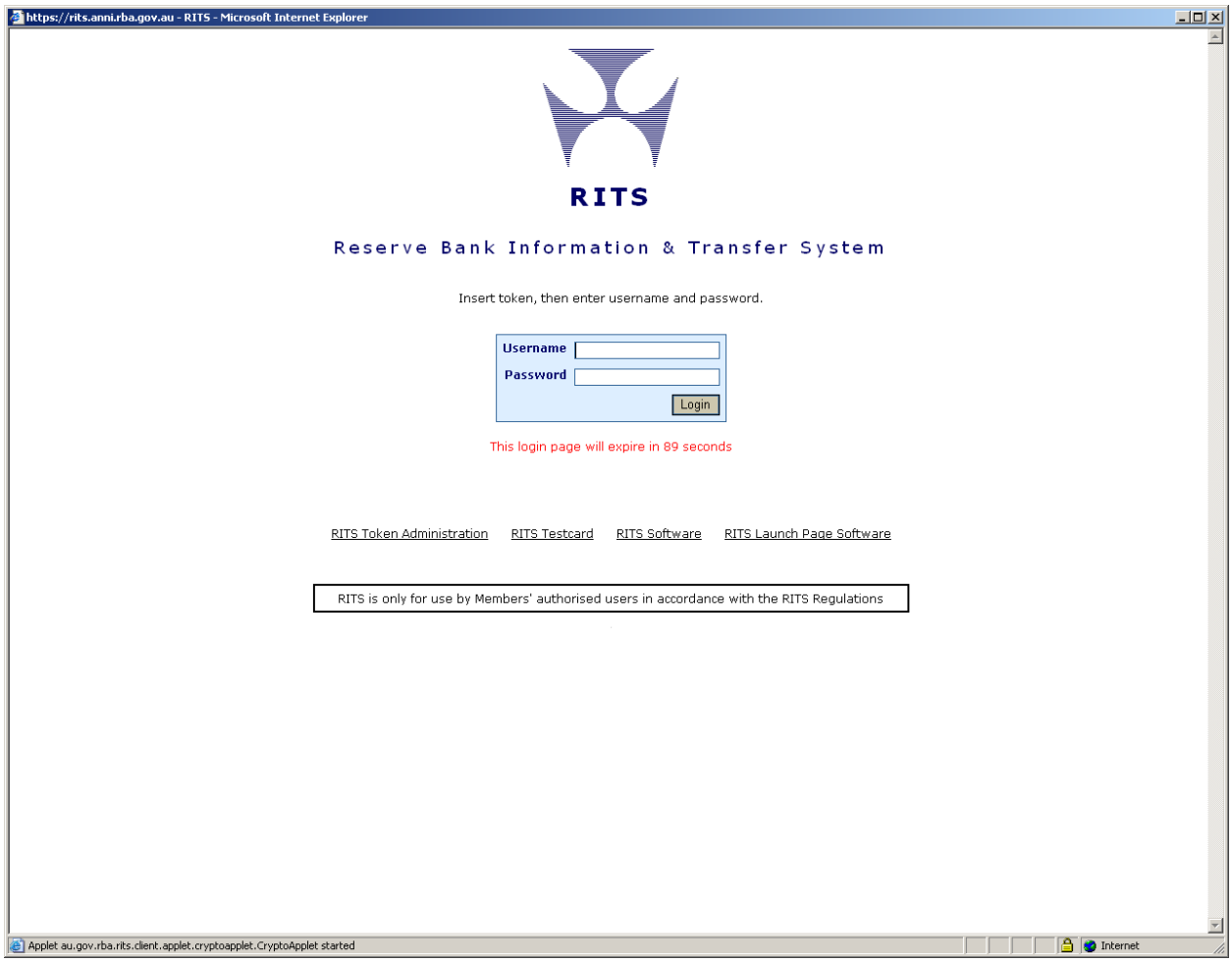
It is recommended that Members keep spare blank RITS tokens at both their head offices and at any disaster recovery/backup sites.

In a contingency, RITS users must take their RITS token with them to the disaster recovery/backup site to login to RITS at that location. Users are not allowed to have two certificates/RITS tokens and therefore cannot store a RITS token at that site or 'copy' the digital certificate to a PC at that site. RITS digital certificates can reside only on the RITS token.

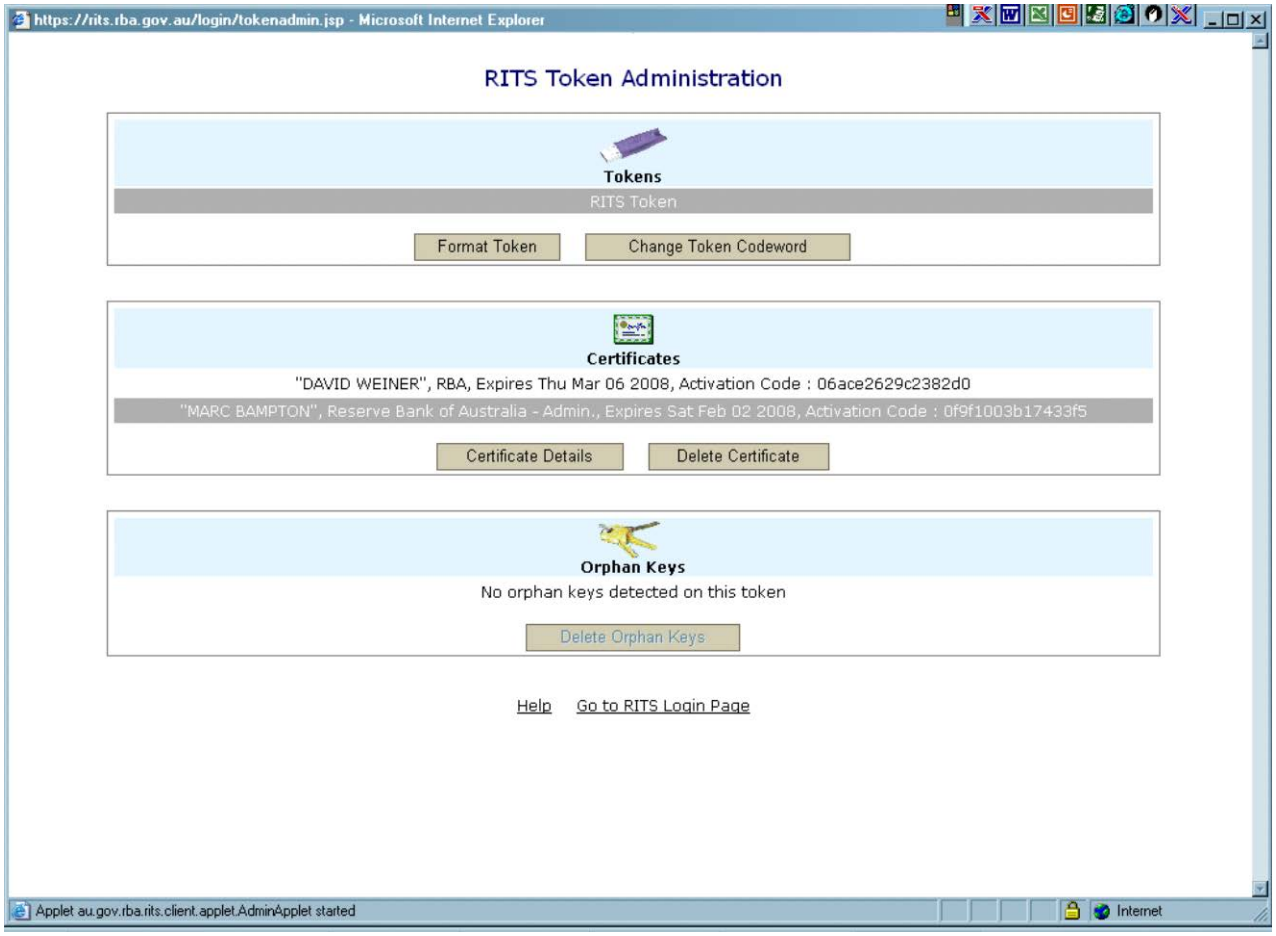
If a RITS user attends a disaster recovery/backup site without a RITS token, then they must arrange to have their RITS digital certificate revoked and re-enrol for a new certificate using a spare blank RITS token already held at that site. In a company's contingency training, users should be reminded to take their RITS token with them when attending disaster recovery/backup sites.

3.3 Format RITS Token

At the **RITS Login** screen, select the **RITS Token Administration** link.

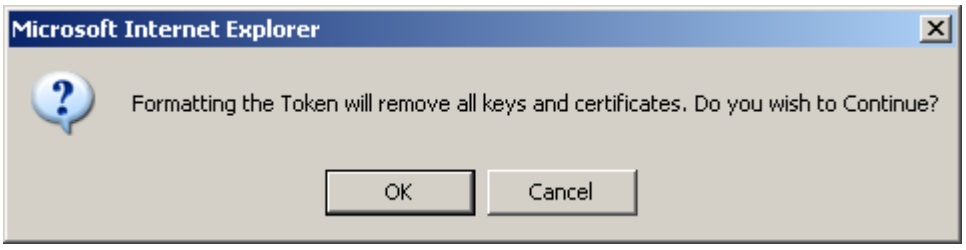


This opens the RITS Token Administration screen. If a RITS token is present in a USB port of the PC, then the words 'RITS Token' will appear and the details of the highlighted certificate will be shown (see below). The user can view the certificates on multiple RITS tokens by inserting them into the USB ports of the PC. The RITS Token Administration screen will automatically refresh if the user enters more RITS tokens and list them under **'Tokens'** (under the picture of the token).



Formatting a RITS token removes all existing certificates (if any) and sets it up for use with RITS. It also requires the user to set a **Token Codeword**, which must be kept secret and not shared. A user does not need to know the existing token codeword (if there is one) to format a RITS token.

By selecting **Format Token** button on the RITS Token Administration screen, the following dialogue box is displayed.



Select **OK** to remove all the keys and certificates on the RITS token and proceed.

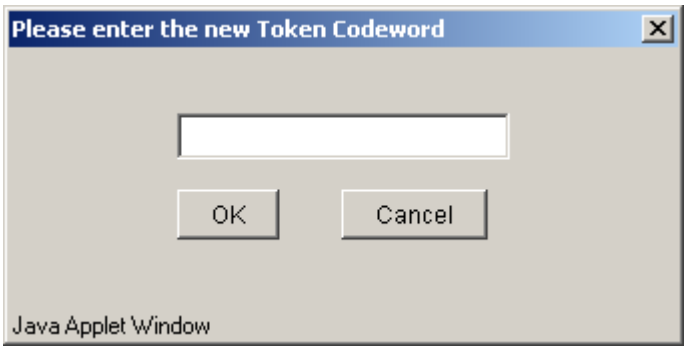
If a user inadvertently formats a RITS token that contains a valid RITS digital certificate, the user who owns that certificate must have it revoked and re-enrol to collect another certificate before they can access RITS again.

If a user is given a RITS token that is already formatted with a **Token Codeword**, the user should set a new Token Codeword in the **Change Token Codeword** function before using the RITS token. No other user, even the Password/Certificate Administrator, should know a user's Token Codeword.

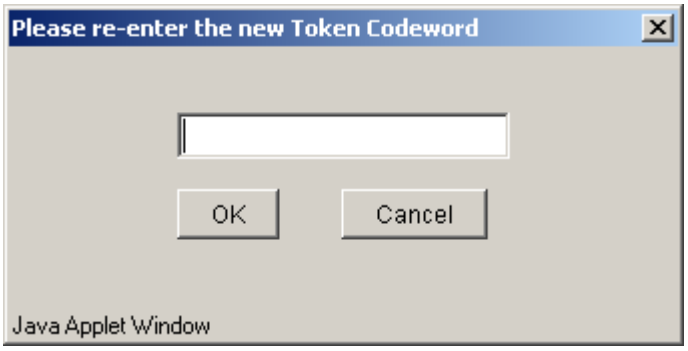
3.4 Change Token Codeword

The user may change their Token Codeword at any time. By selecting the **Change Token Codeword** button on the RITS Token Administration screen, the following sequence of dialogue boxes is displayed.

Firstly, enter the existing Token Codeword and select **OK**.



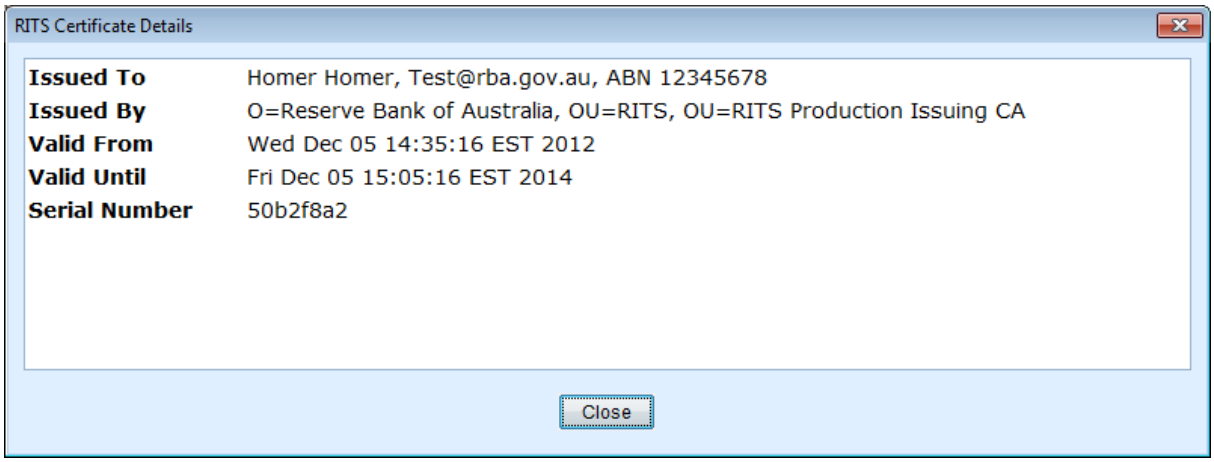
Type in a new **Token Codeword** and select **OK**. Rules for the Token Codeword are set out in chapter 5.6 of this user guide.



Re-enter the new **Token Codeword** and select **OK**.

3.5 View Certificate Details

To view a certificate owner (and hence the RITS token owner), view under **Certificate Details on the RITS Token Administration screen** (the Token Codeword is not needed). If a number of tokens are entered into the PC, select the RITS token first, then press the **Certificate Details** button. A screen similar to the following will appear:



The following certificate details are provided:

Issued to: This is the Distinguished Name (DN) of the certificate and is made up of First Name, Last Name, Email and Australian Business Number of the RITS Member.

Issued by: The name of the Certificate Authority issuing RITS digital certificates is the 'RITS CA'. The RITS environment is 'Production' and the Reserve Bank of Australia is the issuing organisation.

Valid From: This is the day that the certificate was enrolled. The time is fixed at 12.00 midnight GMT but is converted to Australian Eastern Standard Time.

Valid To: This is the expiry date and time of the certificate, after which it can no longer be used to access RITS. The expiry time is 12.00 midnight GMT but is converted to Australian Eastern Standard Time.

Serial No: This is a unique identifier for this RITS digital certificate. It is used by RITS and the Internet Explorer browser, but not RITS users. It is not the Activation Code used to activate a newly enrolled certificate that is found on the main screen for Token Administration next to the certificate name.

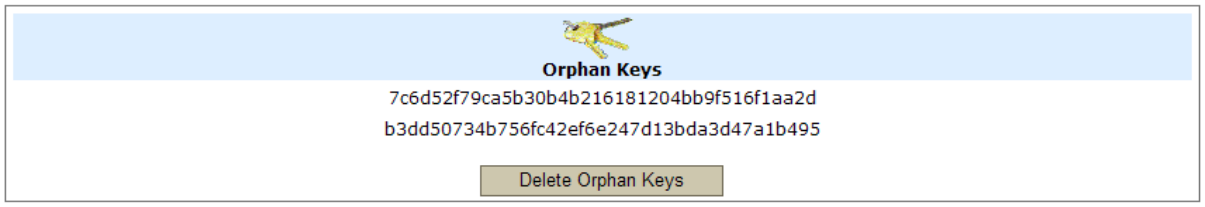
3.6 Delete Certificate

The memory space on the RITS token is limited to around 9 certificates. Therefore, a user should consider cleaning up the RITS token if they have expired or unused RITS (or other) certificates. A RITS token with too many certificates will be inoperable, and will require reformatting, which would require the user to revoke and re-enrol for their RITS digital certificate.

To delete a certificate, on the RITS Token Administration screen select a certificate from the list under the heading 'Certificates' and press the **Delete Certificate** button. The user will be required to enter their Token Codeword and press OK and the certificate will then be deleted.

3.7 Delete Orphan Keys

Orphan keys are private and public keys that have not been signed with a certificate. This usually arises when the enrolment process has been interrupted (e.g. the RITS token is removed before the keys are signed, or if the user does not follow the instructions correctly). Given that RITS token storage is limited to 32k, it is a good practice to periodically look for and clean up orphan keys by deleting them. On the RITS Token Adminstration screen press the **Delete Orphan Keys** button, enter the token codeword and the orphan keys will be removed.



4. ENROL FOR A RITS DIGITAL CERTIFICATE

4.1 Summary of Enrolment Steps

- The Member completes a *User Access Request Form*, which must be signed by two RITS Authorised Signatories and sends it to the RITS Help Desk. (See chapter 8 of this user guide for a description of the form.)

- The user obtains a RITS token from their Password/Certificate Administrator. (Supplies are available from the RITS Help Desk.)

- The user **formats the RITS token** and sets a **Token Codeword**. (See chapter 3 of this user guide for detailed instructions.)

- On receipt of the *User Access Request Form*, the RITS Help Desk pre-enrols the user. RITS sends an email to the user's email address. The email contains a **Private Reference Code** and a link to **'enrol for a RITS Certificate'**.

- At the same time RITS Help Desk phones the **Password Administrator** to advise the **Secret Password**, which is to be passed to the user.

- The user inserts the formatted RITS token into a USB port of a PC (configured to enable USB ports for the RITS tokens) and clicks the **'enrol for a RITS certificate'** link located in the email. This opens the RITS Certificate Enrolment screen.

- The user enrols by entering the information required on the screen, that is, the not-case-sensitive **Secret Password** supplied by the Password Administrator, and the numeric **Private Reference Code** found in the email. The certificate will be loaded onto the RITS token. This takes around three minutes. The certificate must be collected within 7 days as the pre-enrolment will expire after this time.

- Upon notification of a successful enrolment, the user must get the certificate activated by obtaining the **Activation Code** of the certificate, which can be viewed/ copied from the **RITS Token Administration** screen and passed to their Certificate Administrator for entry into RITS. There is a link to the Token Administration screen in the notification of a successful enrolment screen, or the user can go to the RITS Login page and select Token Administration. In the Token Administration screen, the user selects the new certificate, copies its **Activation Code** and passes it (by email is acceptable) to their Password/Certificate Administrator.

- The Password/Certificate Administrator must enter the Activation Code into the function **User Privileges** by selecting the user from the list and on the next screen, selecting the **Certificate Administration** button and entering the **Activation Code**.

- The process for obtaining a digital certificate is now complete. The user may now log on to RITS. For new users, the **Secret Password**, which was passed to the user by the Password Administrator, is also the initial RITS Login **Password**. After successfully logging on, the user is required to change the password.

4.2 Pre-Enrolment Email

Acting on the *User Access Request Form*, the RITS Help Desk 'pre-enrols' the user into RITS. RITS automatically sends an email to the user. The email contains enrolment instructions, the **Private Reference Code** and a link to enrol for a RITS Certificate .

The **Private Reference Code** is uniquely generated with a numeric code of 8 characters. A sample Pre-Enrolment email is attached below.

Dear User,

The RITS Help Desk has received a request from Chris Bank to provide you with access to RITS. You will need to enrol for a RITS Certificate. Refer to the relevant section depending on whether you are a NEW USER or EXISTING USER.

Refer to the RITS Information Facility "Certificates and Tokens" tab for information about certificates. If you require assistance, contact the RITS Help Desk on 1800 659 360.

NEW USER

· Before proceeding, check that your technical staff have provided you with network access to RITS and loaded the RITS software onto your PC.

· Ensure you have obtained a RITS USB token from your RITS Password/Certificate Administrator.

Collecting your RITS certificate

1. Insert the RITS USB token into your PC.

2. At the RITS Launch Page, select **Information & Setup** then follow the **RITS Token Administration** link. Select Format Token. Set a Token Codeword known only to you. This Codeword does not expire.

3. Obtain the Secret Password from your RITS Password/Certificate Administrator. (The RITS Help Desk has phoned this Secret Password to your Password/Certificate Administrator.)

4. Note your Private Reference Code: **49927165**

5. Click this **enrol for a RITS Certificate** link. You need Internet access to enrol.

6. Type in your Private Reference Code and Secret Password.

7. After being notified of a successful enrolment, open the RITS Launch Page, select **Information & Setup**, then the **RITS Token Administration** screen and obtain the Activation Code for your RITS Certificate.

8. Pass the Activation Code to your RITS Password/Certificate Administrator.

9. [For Certificate Administrator only] In Member Admin/User Privileges, select the User and enter the Activation Code.

10. At the RITS Launch Page, select **Information & Setup** link, then select **RITS Testcard**. Ensure all requirements receive green ticks.

11. Login to RITS by entering your Username and Password. For your first login, the Password is the Secret Password. Select the certificate and enter your Token Codeword.

EXISTING USER

Renewing your RITS certificate
1. Obtain the Secret Password from your RITS Password/Certificate Administrator. (The RITS Help Desk has phoned this Secret Password to your Password/Certificate Administrator.)

2. Note your Private Reference Code: **49927165**

3. Click this **enrol for a RITS Certificate** link. You need Internet access to enrol.

4. Type in your Private Reference Code and Secret Password.

5. After being notified of a successful enrolment, open the RITS Launch Page, select **Information & Setup**, then the **RITS Token Administration** screen and obtain the Activation Code for your RITS Certificate.

6. Pass the Activation Code to your RITS Password/Certificate Administrator.

7. [For Password/Certificate Administrator only] In Member Admin/User Privileges, select the User and enter the Activation Code.

8. Login to RITS by entering your Username and **current** Password. Select the certificate and enter your Token Codeword.

Kind regards,

RITS Help Desk

4.3 User Receives Secret Password from Password Administrator

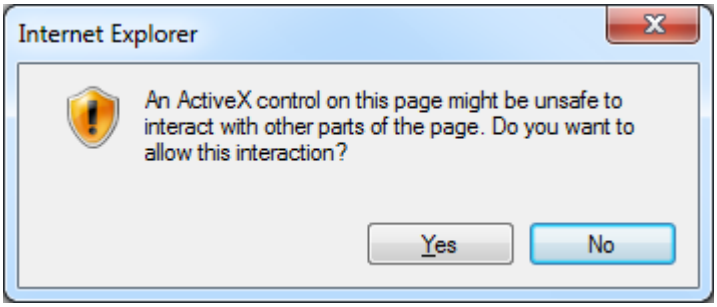
The RITS Help Desk telephones the Password Administrator and provides the User ID and Secret Password for the enrolling user. The Password Administrator should quickly pass the User ID and the Secret Password to the enrolling user. The Secret Password is not case-sensitive.

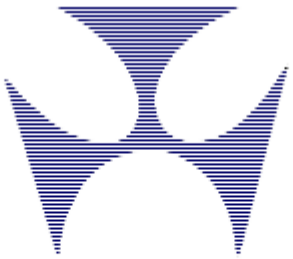
4.4 Enrol for a RITS Digital Certificate

4.4.1 Link in the Enrolment Email

Once the Secret Password has been received by the enrolling user from the Password/ Certificate Administrator, the user may enrol for a certificate.

Insert the formatted RITS token into the USB port of a PC (configured to enable USB ports for RITS tokens). Select the link to 'enrol for a RITS Certificate' provided in the Pre-Enrolment email to open the **RITS Certificate Collection** screen. If an ActiveX control prompt appears like that shown below, select Yes.





RITS Certificate Collection

Enter your RITS Certificate information
You must enter a value for every field.

Private Reference Code (from email)

Secret Password (from Password Administrator)

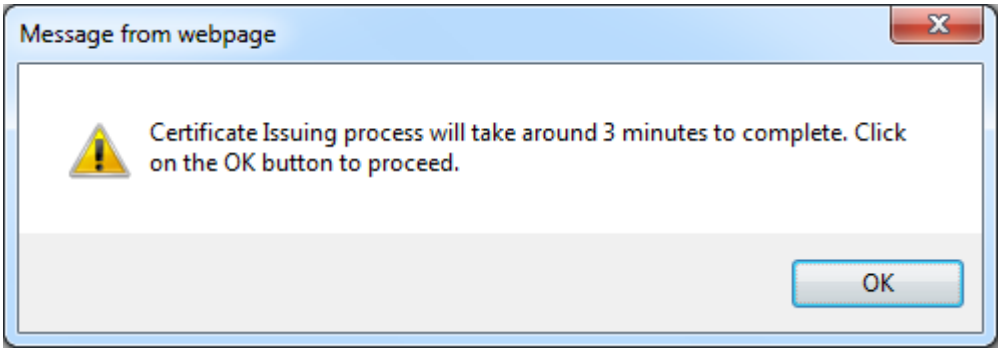
Submit Cancel

Please Note :
After clicking on Submit button the certificate issuing process will take around three minutes to complete. You must not close the browser during this time.

4.4.2 Entry Fields

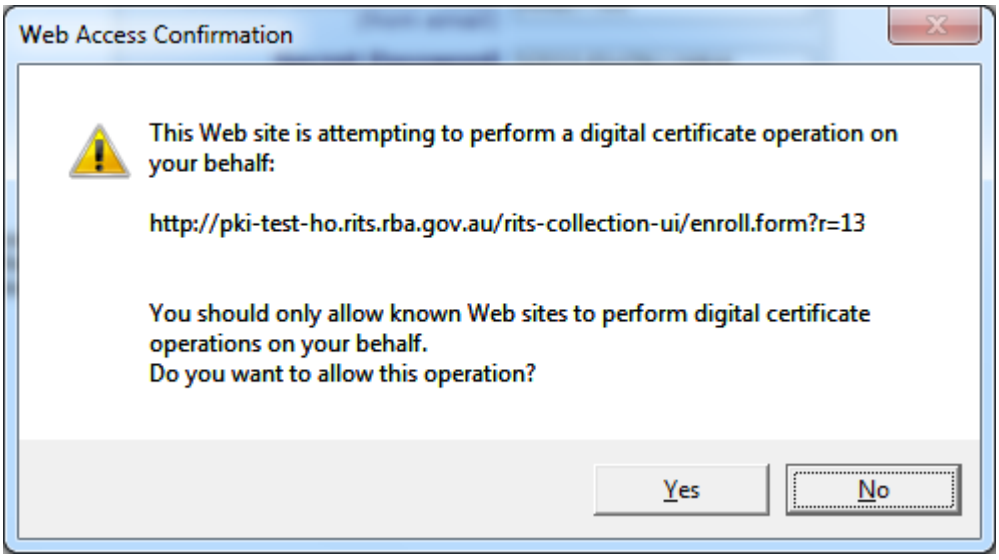
Field	Description
Private Reference Code (from email)	Type in your numeric Private Reference Code given to you in the email from the RITS Help Desk.
Secret Password (from Password Administrator)	Type in your Secret Password given to you by your Password Administrator. The Secret Password is case-insensitive.
Submit	Select **Submit** to enrol for the RITS certificate.
Cancel	Select **Cancel** to clear entries and return to the RITS Certificate Enrolment screen.

When **Submit** is selected, the following screen is displayed.



Press **OK to proceed.**.

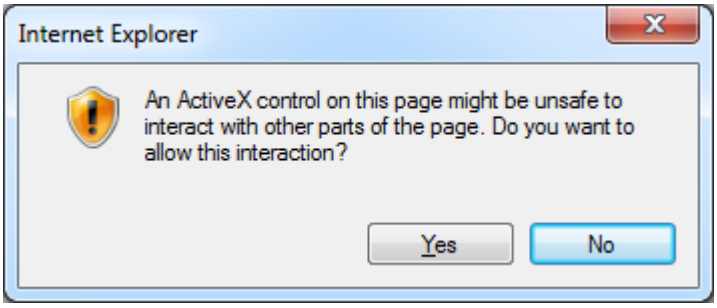
The following screen is now displayed.

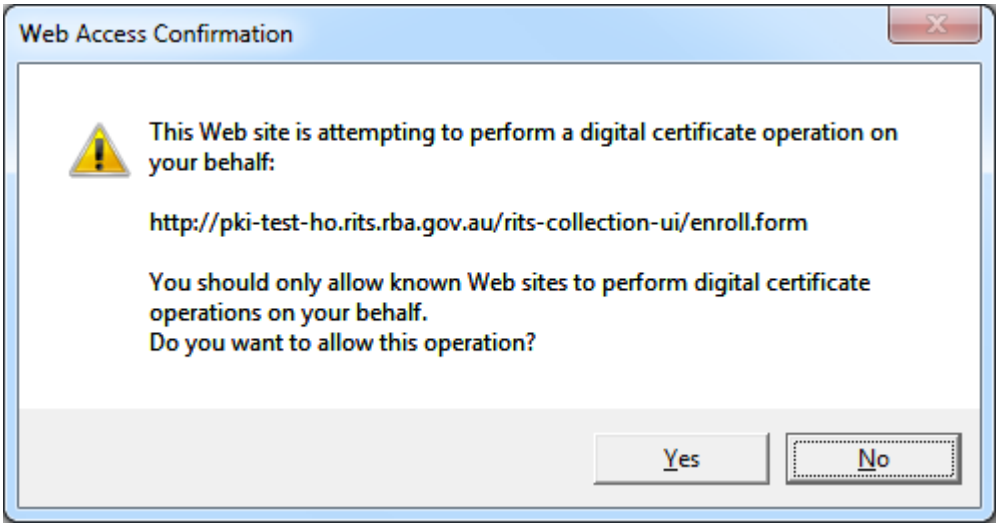


Select **Yes** to request the certificate. If **No** is selected, the enrolment will not occur.

The following screen is now displayed. Enter your token codeword and click on **OK**.

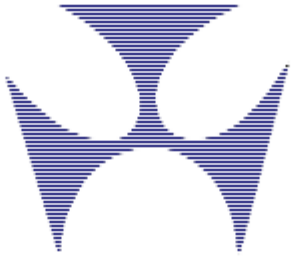
If an ActiveX control prompt appears for the second time, select Yes.





Select **Yes** to proceed.

After this screen (which says '**Installing certificate. Please wait …**'), the following screen is displayed, which shows that that user has completed the **RITS Certificate** enrolment process.



RITS Certificate Collection

Congratulations!
You have successfully enrolled for a RITS Certificate, and it has been installed on your token.
The next step is to pass the certificate Activation Code to your organisation's password/certificate administrator who will activate the certificate in User Privileges.
You will find your Certificate Activation code on the Token Administration page.

Your RITS Certificate:

cn=
ou=
ou=RITS
ou=RITS
o=Reserve Bank of Australia
o=GOV
c=AU

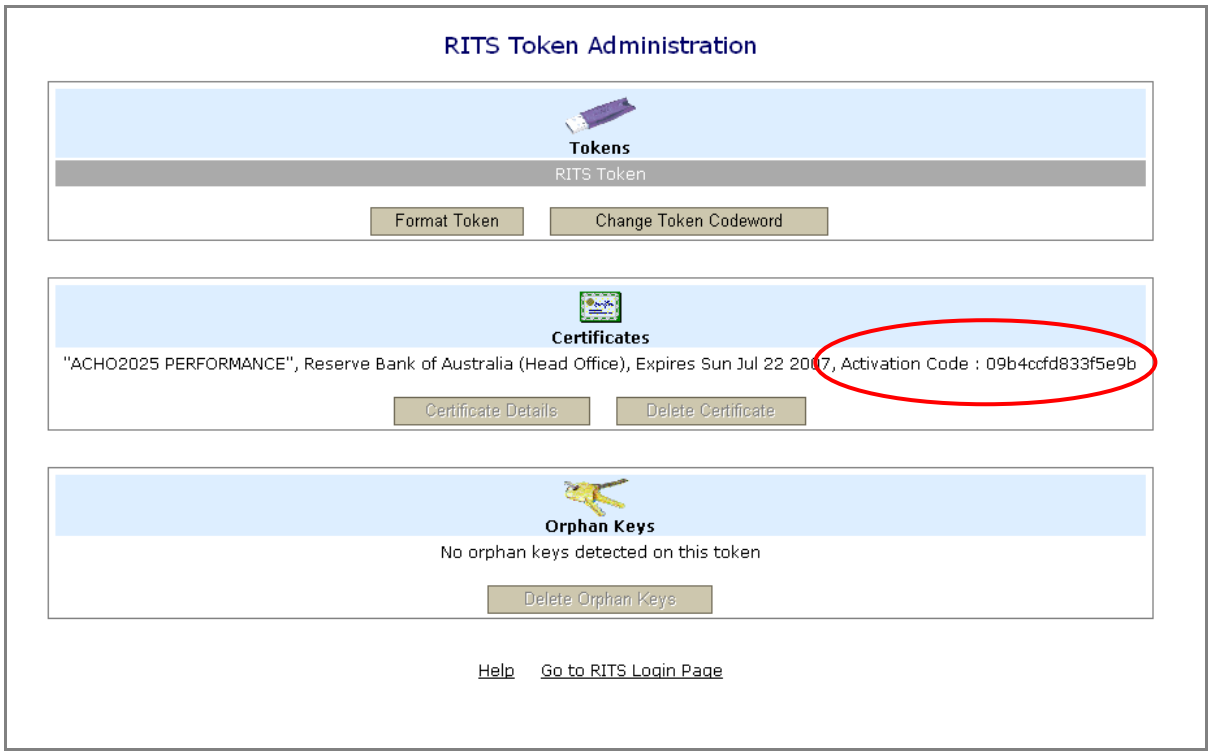
Organisation Unit = Australian Business Number

4.5 Activation of Certificate in RITS

The next step is to activate the certificate in RITS. Certificates must be activated **within 7 days of pre-enrolment**. Certificates that are not activated within 7 days of pre--enrolment will be revoked by the RBA.

To activate the certificate in RITS, the user goes to the **RITS Token Administration** screen, either via the link in the previous screen notifying a successful enrolment or via the link on the RITS Login page.

At the Token Administration screen, the user obtains the **Activation Code** for the newly enrolled certificate (as shown below) and passes it to their Password/Certificate Administrator for entry into RITS via the function **User Privileges**. The Password/Certificate Administrator selects the enrolling user in User Privileges, selects the **Certificate Administration** button and then the **Activate Certificate** button to enter the Activation Code. For further information, see information on User Privileges in the *Member Administration Guide*.



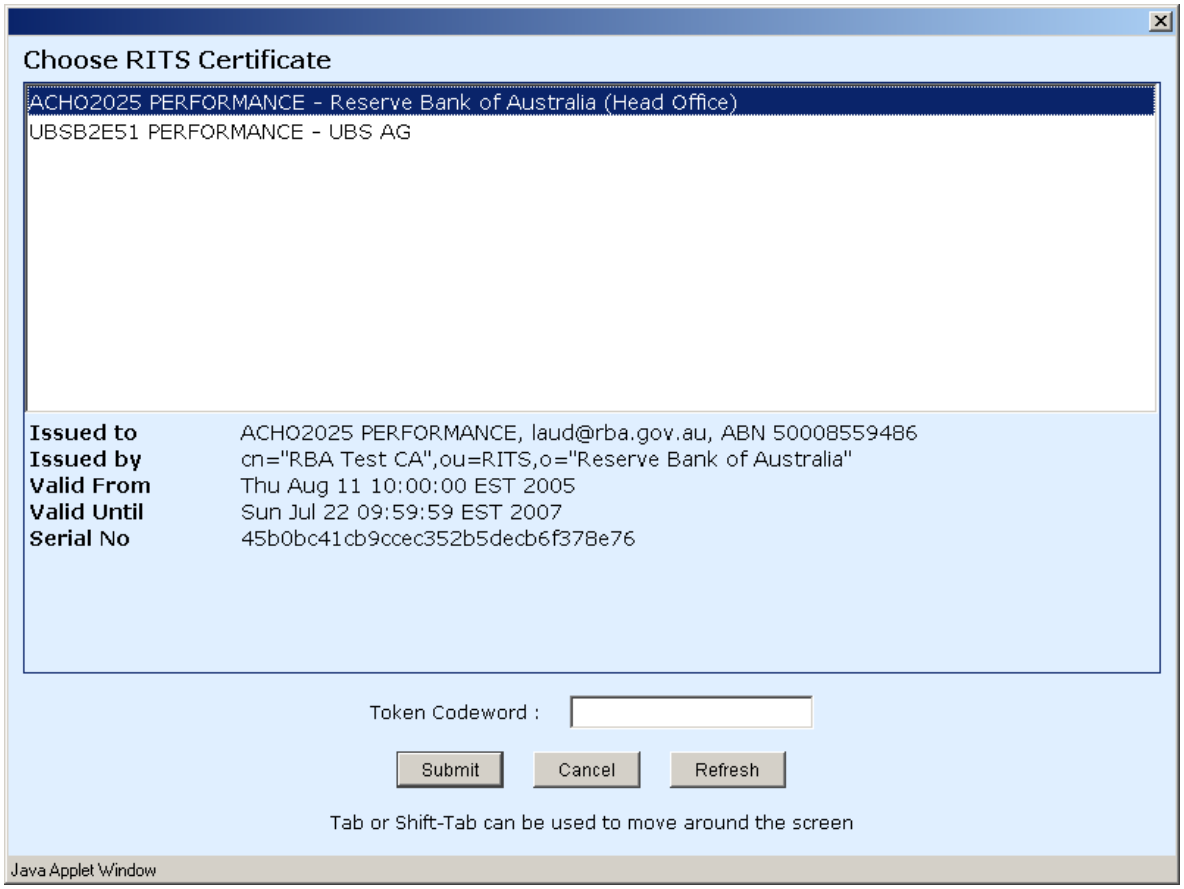
4.6 First Login to RITS

After the user's RITS digital certificate has been activated, the user can now log in to RITS. A RITS launch page icon should have already been set up by the user's IT staff.

Click on the link to RITS and at the **RITS Login** screen enter the **Username** (e.g. BANK2003) and **Password**, which for new users will be the same **Secret Password** obtained from the Password Administrator used to enrol for the RITS digital certificate. (Users re-enrolling prior to expiry should enter their existing password.)

Press the **Login** button. New users will be asked to set and verify a new RITS password, which should be only be known to the user.

At the following screen, select the **RITS Certificate** and enter the **Token Codeword**. (The Token Codeword is set when the RITS token is formatted.) Press **Submit** to login.



A successful login will bring the user to the RITS homepage, where the user can choose a menu option to proceed.

5. LOGGING IN TO RITS

5.1 Key Points

- A RITS digital certificate downloaded onto a formatted RITS token is a pre-requisite for accessing RITS.
- RITS may be accessed over the Austraclear network (ANNI) or via the Internet. Dial-up access is not available.
- Minimum hardware and software specifications are required for RITS access. See the *Technical Information Paper* in the *RITS Information Facility* for more information.
- The RITS Launch Page automates logging on, by detecting the site at which RITS is available (primary or secondary) and the available network path (the Austraclear network or the internet). A manual override option is also available. See the *Overview of Functionality Guide* for a description of the features of the Launch Page.
- If two or more users are sharing the same PC each user must have their own RITS token and certificate and must open a session for themselves using the Launch Page.

5.2 Pre-Requisites

5.2.1 Enrolled with RITS Digital Certificate

A RITS digital certificate downloaded onto a formatted RITS token is a prerequisite for accessing RITS. The RITS token must be in place to login to RITS and to perform transactions. RITS tokens are not required to perform enquiry functions once a user is logged in.

See chapter 3.2 of this user guide for details on how to obtain a RITS digital certificate.

5.2.2 Network Access Set-Up

The Reserve Bank and the ASX have agreed that access to RITS will continue to be across the Austraclear network (ANNI) in the medium term, providing continued cost-effective access to both RITS and the Austraclear System.

Smaller institutions can access RITS via the Internet.

Use of the Internet involves strict security controls, and is subject to certain restrictions, particularly in relation to the types of institutions that may use it as their only means of connection to RITS.

For details on network access arrangements please refer to the RITS *Technical Information Paper* and the *Network Policy for RITS*.

5.2.3 RITS PC Software in Place

For system standards and software requirements, please refer to the RITS *Technical Information Paper* available in the RITS Information Facility.

See the *Guide to Connectivity Testing* for instructions on obtaining the RITS Software on a CD available on request from the RITS Help Desk or via download from the internet.

5.3 Sharing PCs

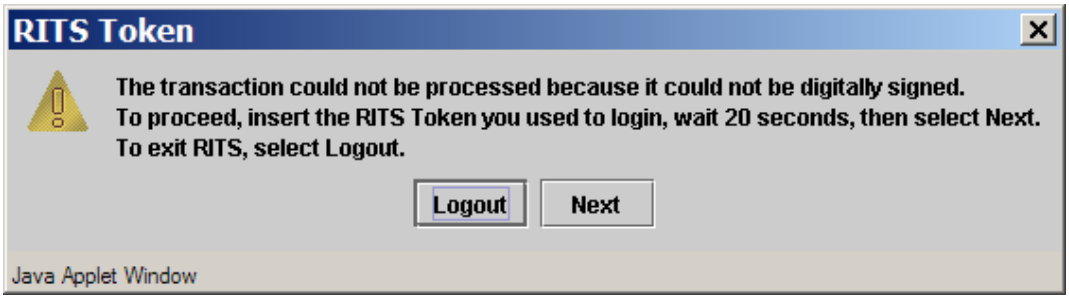
If two or more users are sharing the same PC, each user must have their own RITS token and RITS digital certificate and must access RITS via a separate session.

To open a separate session, each user must click on the RITS icon on the desktop and then select to access RITS or RITS Pre-Production in the Launch Page. Details of the operation of the Launch Page are described below.

5.4 RITS Tokens and the Digital Signing of Updates

The RITS token that was used to login must be in the USB port of the PC when updates are submitted, as all updates must be signed by the digital certificate that is stored on the RITS token. However, if the user has already logged into RITS, it is possible to undertake enquiries with no RITS token in the PC.

If the RITS token used to login is removed from the PC, removed and re-inserted or replaced by another RITS token, and an update is submitted, the following message is displayed.



Insert the RITS token used to login into the PC (if removed) and press **Next**. You are then prompted to enter the Token Codeword. If the Token Codeword is correct, the update is processed.

If **Next** is pressed with no RITS token in the PC or one that is not the one used to login, or the Token Codeword is invalid, the following screen is displayed:

Press **OK** to terminate the session and login again.

5.5 Launch Page

RITS Production is available from the primary and secondary (backup) sites.

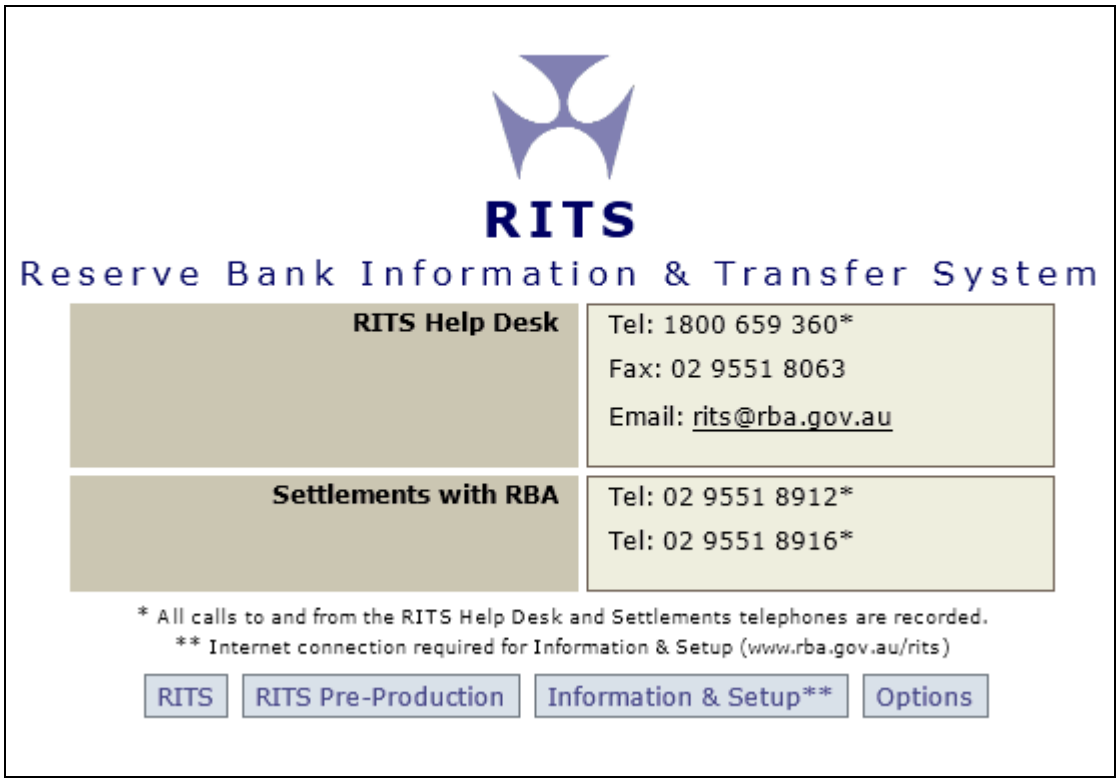
RITS Pre-Production is only available at one site.

To log on to RITS, place the RITS token into a USB port on the PC and double click on the RITS Launch Page icon on the desk top.

The **Launch Page** is displayed.

(If the Launch Page does not open after you have selected the RITS icon on the desktop it is possible that the cause is the setting on your browser to block pop-ups.)

To check this setting, open an Internet Explorer session and access the Tools menu. Click 'Internet Options', go to the 'Privacy' tab, under 'Pop-up Blocker' untick the check box to turn it off.)

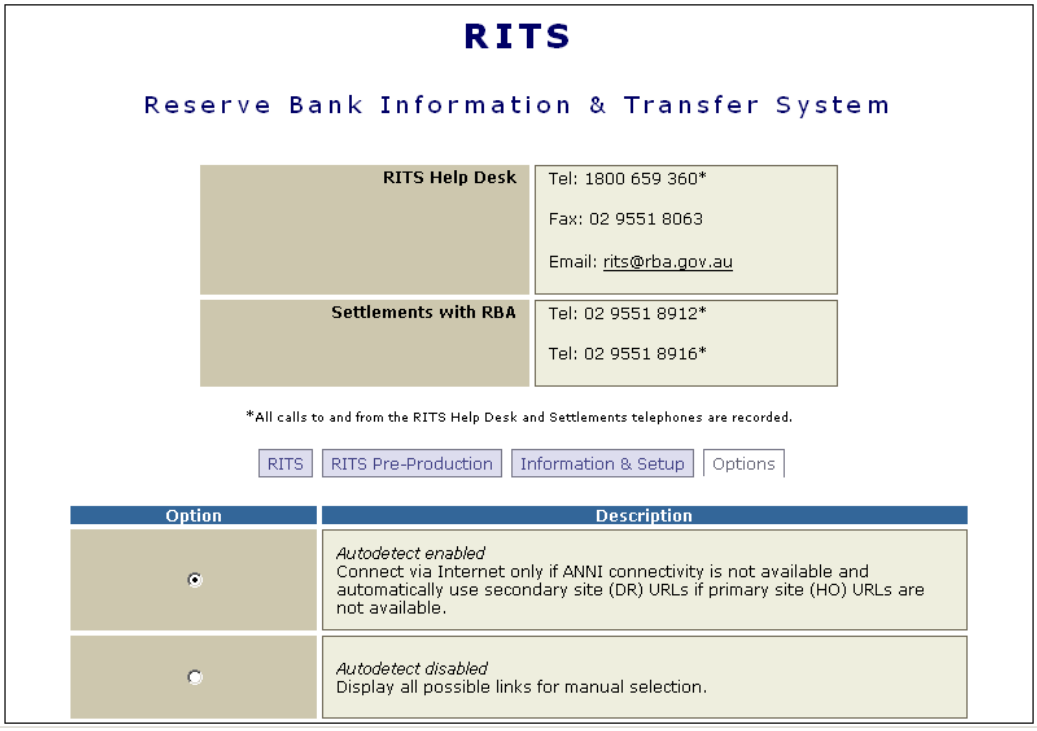


The default mode is '*Autodetect enabled'.* To login to Production RITS in this mode, select the **RITS** tab. The Launch Page automatically detects the RITS environment (at the primary or secondary sites) and the network path (ANNI or the internet) that is available.

Alternatively, the user can select the **RITS Pre-Production** tab. The Launch Page detects the network path available to the environment – there is only one instance of the Pre-Production environment.

To manually select the environment or the network path the Launch Page must be placed in '*Autodetect disabled'* mode.

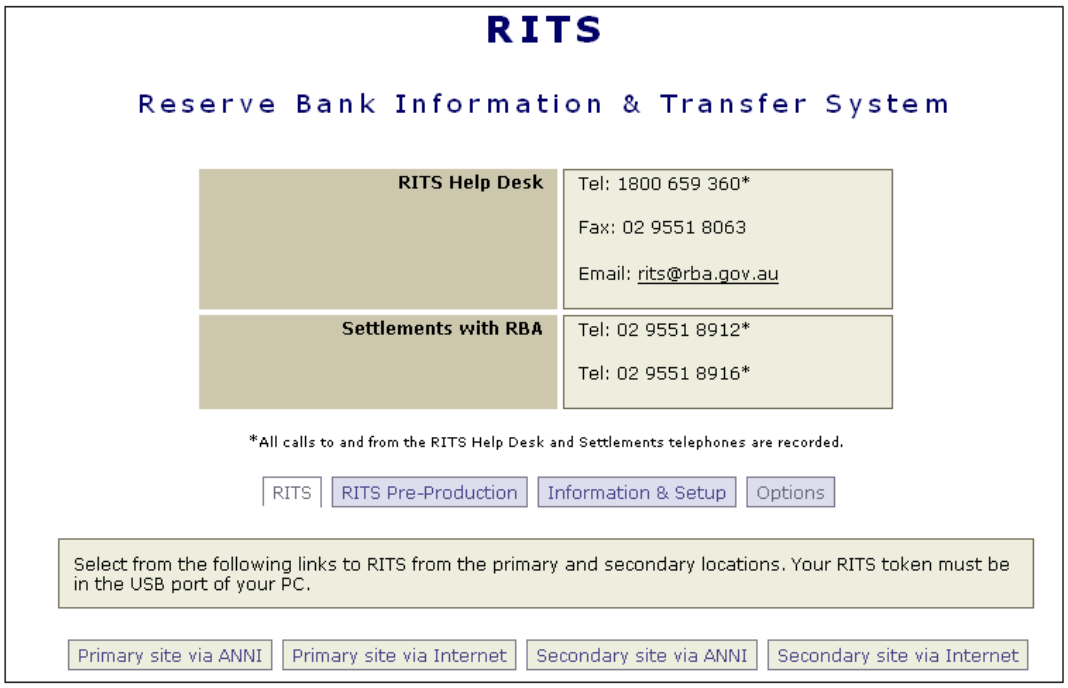
Select the **Options** tab to select the mode of operation of the Launch Page.



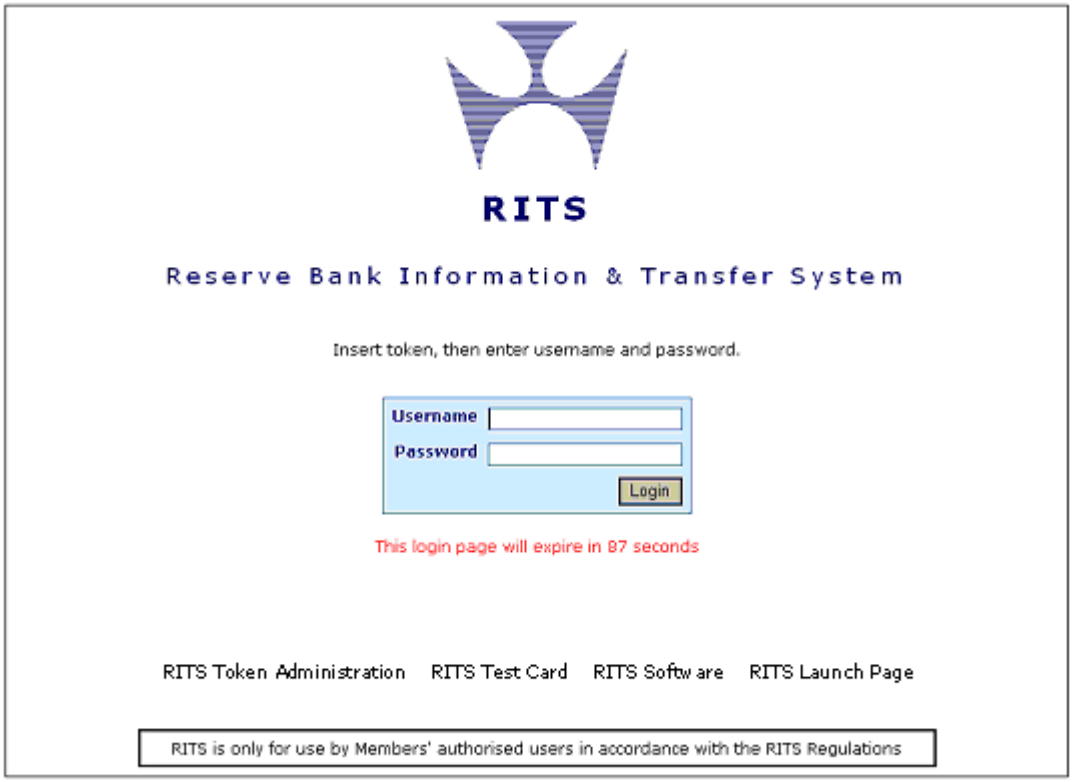
In the screen above select the '*Autodetect disabled'* radio button.

For Production, select **RITS**. Four options are displayed at the bottom of the screen. (For **RITS Pre-Production** two options are displayed.)

Select from these options to access RITS. The screen below is for RITS Production. [Note that the Options selection defaults to '*Autodetect enabled'* after any selection of **RITS** or **RITS Pre-Production**.]

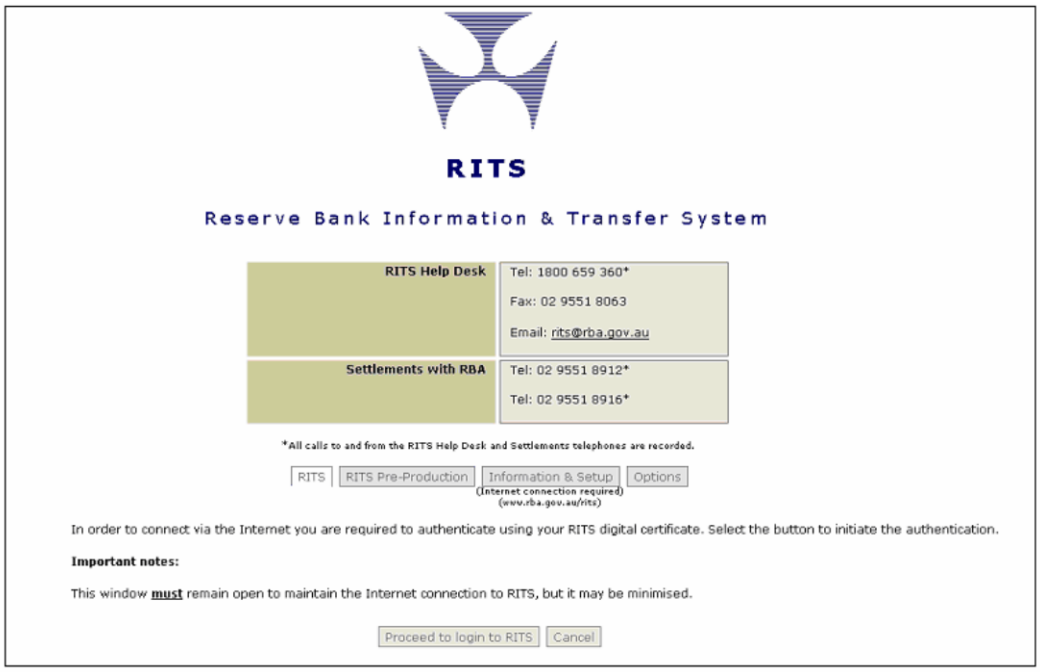


If the path chosen (either automatically by the Launch Page or manually by the user) is **ANNI**, the **RITS Login screen** will next appear. (Section 5.7 outlines use of the login screen.)



If the path chosen (either automatically by the Launch Page or manually by the user) is the internet, it is necessary to authenticate the user's RITS digital certificate before the login screen can be displayed.

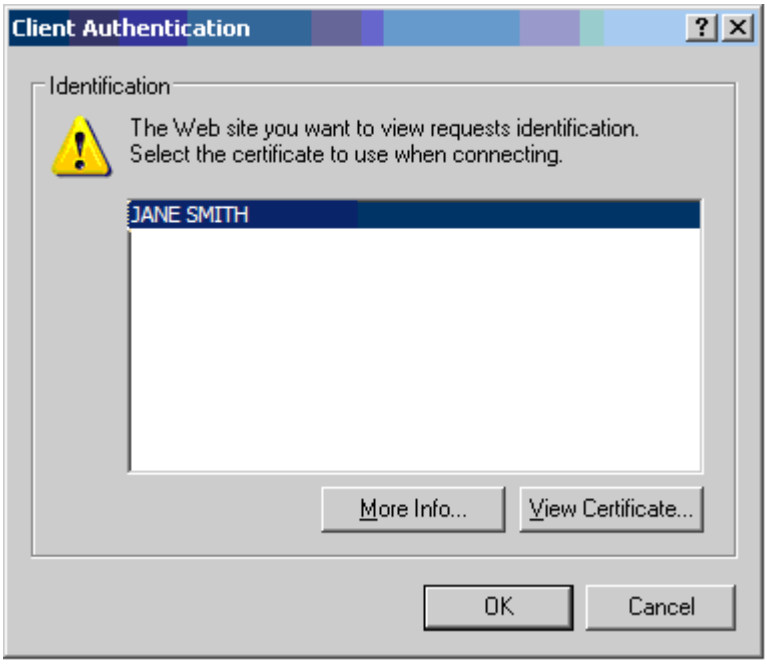
The following screen is displayed.



Important: This screen must be kept open to maintain internet access.

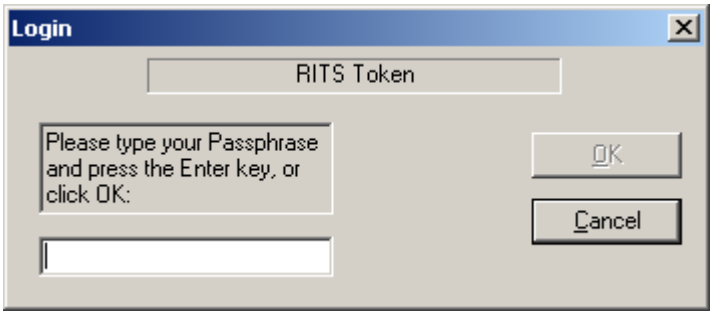
Select the **Proceed to login to RITS** button.

The following screen is displayed.



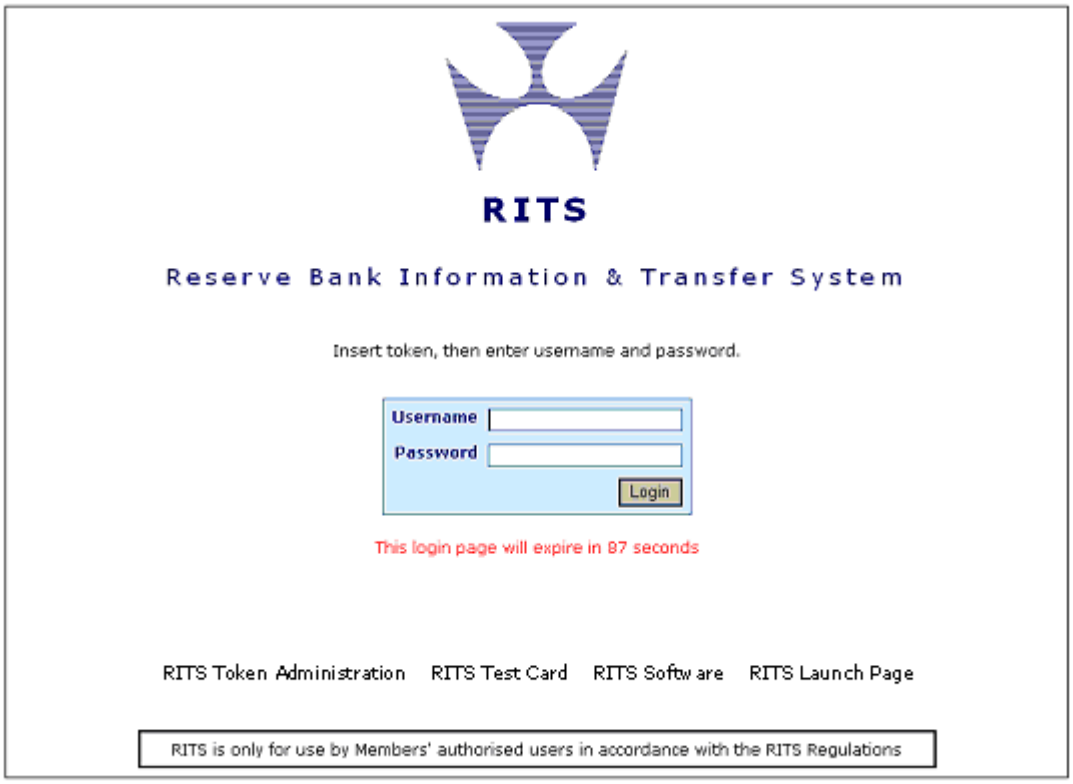
Highlight the digital certificate by clicking on it and press **OK**.

The following screen is displayed.



Enter your Token Codeword and press **OK**.

The **RITS Login screen** will next appear. (Section 5.7 outlines use of the login screen.)



5.6 Requirements for RITS Passwords and Token Codewords

The requirements for RITS Passwords and Token Codewords are set out in the following table.

	RITS Passwords	Token Codewords
Length	8 – 12 characters	4 – 20 characters
Format	Mix of alpha-numeric (at least one non-alphabetical character)	Alpha or numeric or a mix
Case-sensitive	Yes	Yes
Re-use of password	Passwords used in the last 12 months cannot be re-used	Passwords can be re-used
Expiration	30 days (users are prompted 5 days before expiry)	Do not expire
What happens after a password expires	The user is able to login with the expired password, but is immediately required to set a new password	N/A
Number of wrong attempts allowed	3	10
Display of number of failed attempts	In function **User Privileges**	N/A
Reset of the failed attempts counter	Upon successful login or 24 hours after first failure.	After successful login.
What to do if the number of wrong attempts is exceeded	User's status becomes '*Inactive*'. User has to ask their Password Administrator to change the user's status to '*Active*' and may request the password to be reset.	RITS Token must be reformatted (all certificates will be deleted) and user has to re-apply for a replacement certificate using the *Request to Revoke/ Issue Certificates/ Replace Certificates Form*.
Password resetting	Can be reset any time by the user in the 'Change Password' function, by the Password Administrator in 'Password Administration', or by contacting the RITS Help Desk.	Can be reset at any time by the user in the 'Token Administration' function. No other resetting facility is available.
What to do if user forgets password	User has to contact the Password Administrator or RITS Help Desk (in writing), to reset.	Member has to request the RITS Help Desk to revoke old certificate and enrol for a new certificate.
How to 'lock' a user's account	Revoke the user's certificate.	Reformat the RITS token to remove all certificates.

5.7 RITS Login Screen

At the **RITS Login screen** Username and Password must be entered within 90 seconds of opening this page. If the page times-out, select the link provided in the timeout screen to refresh it.

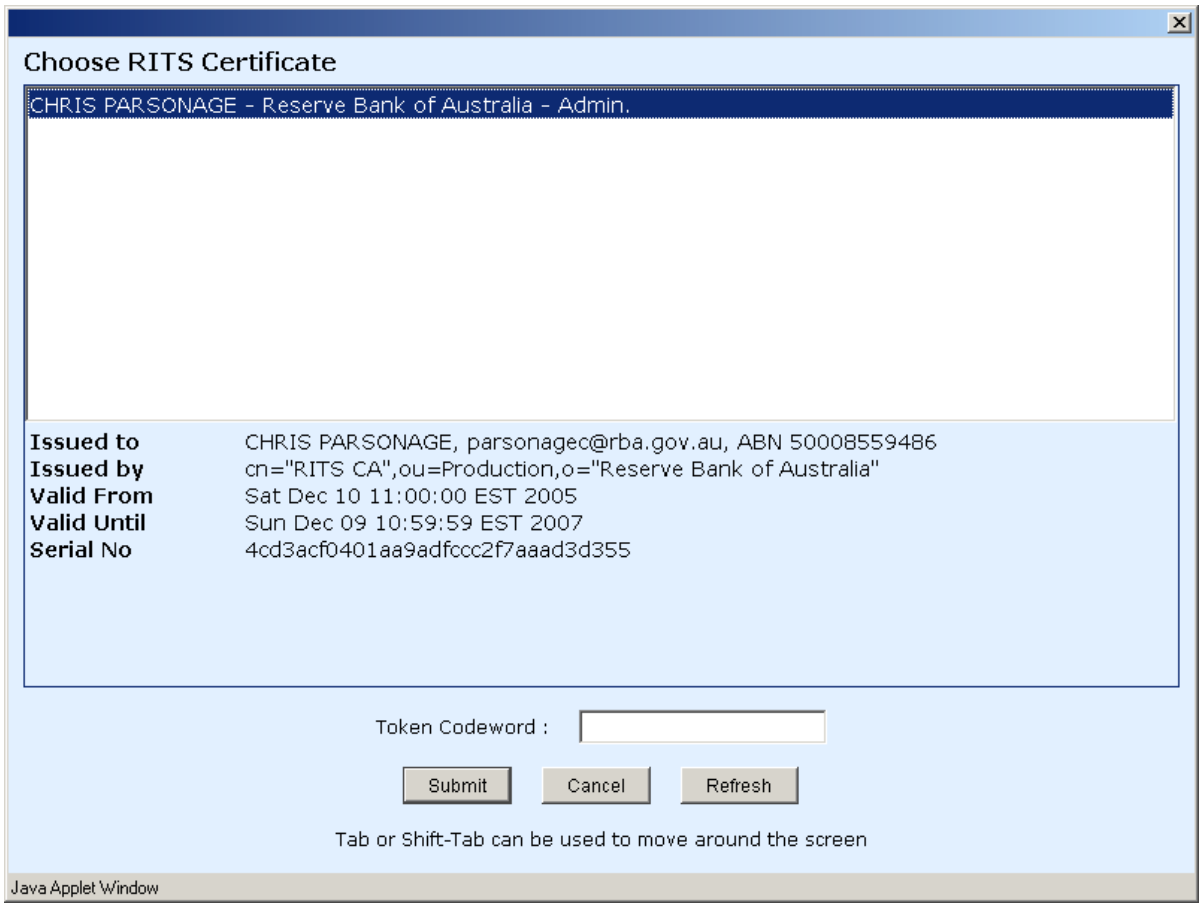
Username: At the **Username** prompt, enter the RITS Username (e.g. BANK2001). The RITS Username is an eight character code entry consisting of:

- the Member Mnemonic (a four character identifying code for the Member of RITS - e.g. BANK); and
- four numbers/characters that represent the user's personal User Mnemonic (e.g. 2E01, 2001).

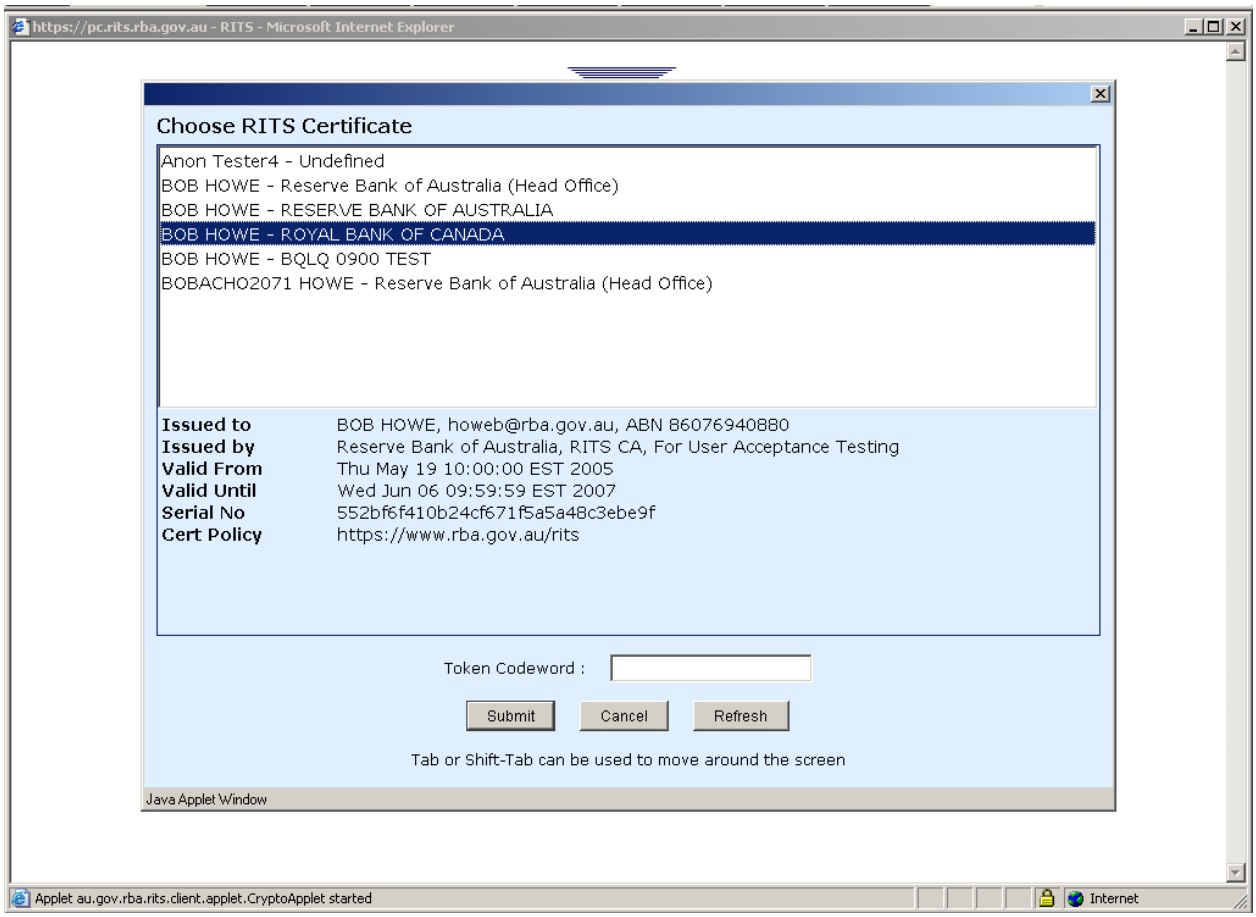
Password: Next press the 'Tab' key or click into the password box. Enter the Password in the **Password** field. The password will appear as asterisks on the screen. See chapter 5.6 of this user guide for details of the RITS password requirements.

If this is the first time you are accessing RITS or if your password has been reset, you will be prompted to change your password immediately after inputting your **Username** and (newly allocated) **Password**. Password length must be at least 8 characters, with at least one non-alphabetical character.

After submitting the Username and Password, the following screen is displayed. The RITS certificate is automatically highlighted and the cursor is in the Token Codeword box, awaiting the entry of the **Token Codeword**.

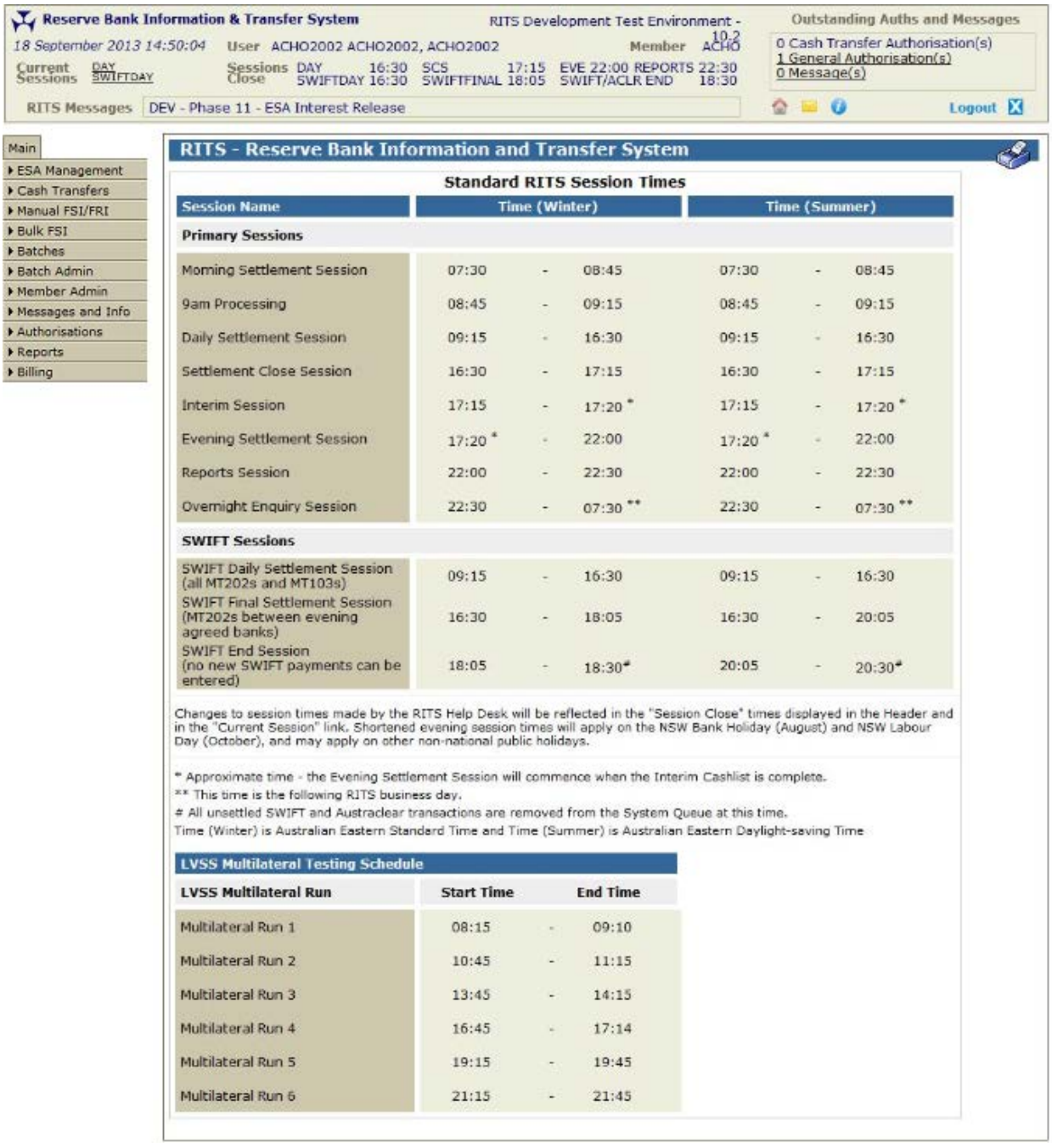


If a different RITS token or certificate is to be selected, use the mouse or the Tab and Shift Tab keys to navigate.



The user should enter their **Token Codeword** and press then select **Submit** to proceed or **Cancel** to exit. Use **Refresh** if the RITS token has just been inserted into the USB port of the computer.

A successful login will bring the user to the RITS homepage as follows.



If the user has made a mistake during login, they will then be returned to the **RITS Login** screen with the message **'Login Failed. Please Retry'.**

5.7.1 Unsuccessful Login Attempts – RITS Username and Password

After three unsuccessful attempts to enter the correct **Username** and **Password**, the status of the user in **User Privileges** will be set to ***Inactive***. RITS does not provide an on-screen error message in this situation. However, a counter in **User Privileges** (User Details screen) records the number of failed login attempts.

To be re-instated, the Member's Password Administrator must:

- change the user's status from ***Inactive*** to ***Active*** in the function **User Privileges**; and
- if the user requests a password re, set a new RITS password in the function **Password Administration**, and notify the user to try again.

When the user logs in with this new password they will be asked to immediately change it.

5.7.2 Unsuccessful Login Attempts – Token Codeword

After 10 unsuccessful attempts at the **Token Codeword**, the RITS token will be locked out and the Token Codeword cannot be reset. The count of unsuccessful attempts starts anew after each successful entry.

After the final attempt the following message is displayed:

"Login Failed. Your token has been locked because the limit of incorrect codewords has been exceeded. Before you can use your token again, you must format it using the RITS Token Administration page. This will erase all certificates on your token. To be issued with a new RITS Certificate, please provide a User Access Request Form to the RITS Help Desk."

After locking a RITS token, the user must:

- format the RITS token and reset the Token Codeword;
- arrange for the Member's Password/Certificate Administrator to revoke the certificate; and
- enrol for a new RITS digital certificate.

During this process the user cannot access RITS.

Users should change their Token Codewords regularly to ensure the security of RITS access. Token Codewords do not expire and users can change them any time in **'Token Administration'**.

5.7.3 Expired RITS Password

RITS Passwords expire every 30 days.

RITS will prompt the user to change the password on each of the 5 days prior to its expiry.

Once the RITS Password has expired the user must enter a new password. The old Password is needed to enter a new one.

If a RITS password has expired and the user has forgotten the old password, the user must request their **Password Administrator** to reset it.

5.7.4 Changing RITS Password and/or Token Codeword

You may change a **RITS Password** and **Token Codeword** at any time:

- change the RITS Password in the function **Change Password**; (note: the current

password must be entered before you enter the new password) and

- change the Token Codeword by selecting **'Token Administration'** on the RITS Login screen. Then choose **'Change Token Codeword'** and follow the prompts.

5.7.5 RITS Session Time-Out Period

After a period of 15 minutes of inactivity, access to RITS will be automatically terminated and the user will be required to login again.

Password Administrators may extend this to 30 minutes or 60 minutes for selected users who, because of their work, spend extended periods of time in RITS.

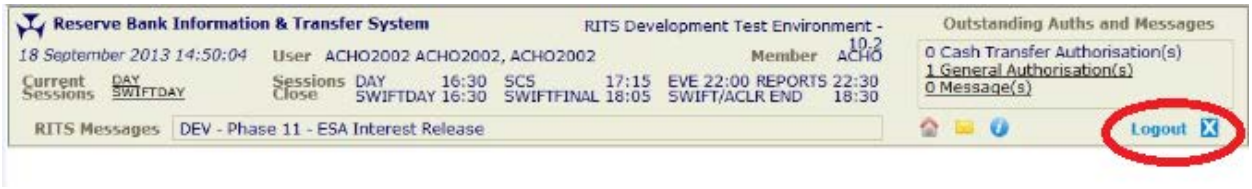
Because extended settings impact system performance and raise potential security risks, it is recommended that the Password Administrators allocate extended session time-outs to selected users only.

Users who have been granted extended session time-out should ensure the security of their RITS login by removing the RITS token when they leave their PC.

The approach adopted by Members should be consistent with their own internal security policies.

5.8 Logging Out

It is important to log out correctly, using the **'Logout'** icon located at the top right of the RITS Header.



6. PASSWORD AND CERTIFICATE ADMINISTRATION

The role of the Password and Certificate Administrator is fully described in the *Overview of Functionality* (chapter 15).

Detailed instructions on the use of the functions used in password and certificate administration are contained in the *Member Administration User Guide*.

Detailed instructions on the process of enrolling for a RITS digital certificate are provided in chapter 4 of this user guide.

6.1 The Roles of Password & Certificate Administrators

A Member's **Password/Certificate Administrator(s)** are vital 'gatekeepers' in the RITS security structure. To control user access to RITS, Members must assign the responsibilities of 'Password Administrator' and 'Certificate Administrator' to at least two staff. Password Administrators are set up by the RITS Help Desk. The same staff member can be responsible for both, or the responsibilities can be separated, depending on the internal security arrangements of the Member.

Password Administrators are responsible for:

- resetting passwords;
- controlling the status of each user;
- setting an extended session time-out;
- allocating roles/ functions to users;
- linking users to branches to perform transactions for those branches;
- assigning the privilege to authorise; and
- ensuring that the authorisations required by the Member are in place.

Certificate Administrators are responsible for:

- activating a newly enrolled user's RITS digital certificate;
- revoking a user's certificate (e.g. if they leave the company); and
- managing users' expiring certificates and their replacements.

This flexibility allows each Member to tailor the allocation of these roles to suit their internal security policies.

All users are automatically given enquiry-only access to **User Privileges**, and can therefore view the profile of all users in a RITS membership. This includes the RITS user status, certificate status and access to various functionalities.

7. PROVISIONING USERS

The **Password Administrator** is responsible for providing users with authorised access to RITS functionality. Functionality is applied to users in 'roles', which are allocated in the function **User Privileges**. Newly allocated roles, and roles removed from the user, take effect after the user's next login to RITS.

The roles have been designed to give the Member a high degree of flexibility in allocating functionality to users.

Users must also be linked to a branch to be able to login to RITS. Details follow.

7.1 Establishing User/Branch Links

User/branch links are set in the function **User Privileges.**

All users must be linked to a branch to be able to login to RITS.

Establish a link for every user to your **main operational branch**, usually the 2E branch. User/branch links can be changed (see the examples below) but there **must** always be one in place.

User/branch links, in conjunction with role allocation, are also used to provision specific users with the ability to enter into certain branch related transactions for branches to which the user is linked.

For the linked branch the user can enter into the following activities, subject to the appropriate roles being allocated to the user:

- Enter, amend or delete Cash Transfers (role: Cash Transfer Entry)
- authorise Cash Transfers (role: Authorise Cash Transfer Entry)
- enquire upon Cash Transfers (role: Member Enquiries)
- manage the Cash Account Status of queued transactions (role: Cash Account Status Queue Management)
- set the override Cash Account Status (role: Override Cash Account Status – Set Override)
- set the Cash Account Sub-Limit: (role: Cash Account Sub-Limit – Set Sub-Limit)
- enquire on batches in the batch facility (role: Member Enquiries)
- perform batch administration in the batch facility (roles: Batch Entry, Batch Commit, Batch Manage).

These transactions can also be conducted for other branches by linking users to these branches. The following examples show how user/branch links and roles can be used to provision users for these activities.

Examples:

1. A user is required to enter Cash Transfers for the 2E branch. Establish the user/branch link to the 2E branch and allocate the role 'Cash Transfer Entry'.

2. The same user is also required to enter Cash Transfers for the 20 branch. In addition to the link to the 2E branch, establish another user/branch link to the 20 branch.

3. A user is required to enter Cash Transfers for the 20 (or 30 branch) branch but not the 2E branch. Change the user/branch link from the 2E (if one has been established earlier) and establish a link to the 20 or 30 branches as required.

4. A user who is responsible for authorising Cash Transfers must be linked to all of the branches that the user is responsible for, and the role 'Authorise Cash Transfer Entry' must be allocated.

5. A user who needs to view the Cash Transfer enquiry must be linked to the branches that are to be viewed and the role 'Member Enquiries' must be allocated.

6. A user who is responsible for managing the Cash Account Status of queued transactions must be linked to the branches that own the transactions and the role 'Cash Account Status Queue Management' must be allocated.

Changes to user/branch links can be made at any time but do not take effect until after the user's next login.

Other activities that affect the whole Member (e.g. ESA and Credit Status management of queued transactions, setting the ESA Sub-Limit, setting Cash Account Limits and making enquiries on settled payments), do not require specific user/branch links. To engage in these activities it is sufficient to allocate the appropriate roles.

7.2 Suggested Role Allocation

It is mandatory that every user has the role called **All Users**. This provides basic functionality to change passwords, view user privileges and other information. It also provides access to the menu of functions.

7.2.1 Roles for ESA and Liquidity Managers

- Member Enquiries
- ESA Status Queue Management
- Override ESA Status – Set Override
- ESA Sub-Limit – Set Sub-Limit

7.2.2 Roles for Credit Managers

- Member Enquiries
- Credit Status Queue Management
- Override Credit Status – Set Override
- Cash Account Limit – Set Limit

7.2.3 Roles for Settlements Authorisers

- Member Enquiries
- Authoriser
- Authorise Cash Transfer Entry

7.2.4 Roles for Settlements Staff (not Authorising)

- Member Enquiries
- Cash Transfer Entry
- Batch Entry (if applicable)

7.2.5 Password Administrator Role

- Password Administrator
- Activation Code Entry and Revoke Certificate if the user is also a Certificate Administrator

7.2.6 Certificate Administrator Role

- Activation Code Entry
- Revoke Certificate
- Password Administrator if the user is also a Password Administrator

A description of each role is available in the document *Overview of Functionality* (chapter 16). Assistance in allocating roles can be obtained from the RITS Help Desk.

8. RITS REQUEST FORMS

8.1 Key Points

Use the appropriate form when requesting the RITS Help Desk to do the following:

- **User Access Request Form** – create/pre-enrol a new user for a RITS digital certificate, assign the Password Administrator role and/or request supplies of RITS tokens.
- **User Access Request Multiple Users Form** – create/pre-enrol new users for RITS digital certificates, assign the Password Administrator roles and/ or request supplies of RITS tokens.
- **Member Authorisations Maintenance Form –** place (or remove) an authorisation on a RITS function so that it requires two staff to complete an action (one to enter and one to authorise).
- **Changes to an Existing User Form –** request the RITS Help Desk to make emergency changes to a user's profiles.
- **Request to Revoke/ Issue Certificates/ Replace Expiring Certificates Form –** issue replacement RITS digital certificate(s) in anticipation of expiry of the current certificate(s), revoke and/ or issue a replacement/new certificate.

These forms are available from the *RITS Information Facility* or from the RITS Help Desk.

8.2 User Access Request Form

Use this form to request the RITS Help Desk to:

- provide RITS tokens;
- create a new user;
- pre-enrol a new user for a RITS digital certificate; and/ or
- assign the Password Administrator role.

RITS digital certificates are issued to individuals. The form must contain the first name, last name and email address of the user and must be signed by two RITS authorised signatories.

8.3 User Access Request Multiple Users Form

Use this form to request the RITS Help Desk to:

- provide RITS tokens;
- create multiple new users;

- pre-enrol new users for RITS digital certificates; and/ or
- assign the Password Administrator role.

Each user's first name, last name and email address must be listed. This form must be signed by two RITS authorised signatories.

8.4 Member Authorisation Maintenance Form

Use this form to request the RITS Help Desk to add or remove authorisation requirements on eligible RITS functions. A function with an authorisation requires two people to complete. Only the RITS Help Desk can make changes to a Member's authorisation settings.

The current setting for authorisations is shown in the function *Authorisations by Function*.

This form must be signed by two RITS authorised signatories.

8.5 Changes to an Existing User Form

Use this form to request the RITS Help Desk to make any of the following urgent changes to an existing user's details when their Password/Certificate administrator(s) are unavailable:

- change the user's status in the Production and/or Pre-Production environment – *Active* or *Inactive*;
- add or remove the user's links to a branch or branches;
- add or remove the user's roles;
- add or remove the user's authorisation privileges;
- reset the user's RITS Password; and/or
- activate or revoke the user's RITS digital certificate.

This form must be signed by two RITS authorised signatories.

8.6 Request to Revoke/ Issue Certificates/ Replace Expiring Certificates Form

Use this form to request the RITS Help Desk to:

- issue a certificate to a new user:
- issue replacement RITS digital certificate(s) for user(s) in anticipation of expiry of the current certificate(s);
- revoke a user's certificate.

This form must be signed by two RITS authorised signatories.

9. CERTIFICATE EXPIRY

9.1 Key Points

- The owner of a RITS digital certificate and all Password Administrators of the Member will receive an email 30, 60 and 90 days prior to certificate expiry to enrol for a new certificate.
- An expired certificate cannot be used to access RITS.
- Certificates are issued with a lifespan of 2 years from the date of collection..
- During the expiry window and after enrolment for a new certificate, the activation of the new certificate will cause the old certificate to be automatically revoked. The new certificate will commence operation in a seamless changeover.

9.2 Enrolling for a New Certificate Prior to Expiry

The owner of a certificate and the Password Administrators will both receive an **Expiry Email** 30, 60 and 90 days prior to the expiry of the certificate. It is highly recommended that users enrol for a new certificate immediately, and not put it off. This will avoid the situation where a user cannot access RITS (e.g. in the morning in preparation for the 9am Batch) because the certificate has expired. Note: if a certificate expires, the user will be required to re-enrol for a new RITS digital certificate. This process will take approximately 20 to 30 minutes.

The time between receiving the Expiry email and Certificate expiry is called the Expiry Window. During that time, the user should enrol for a replacement RITS certificate. To enrol for a replacement certificate, the user or the Password/ Certificate Administrator needs to complete a ***Request to Revoke/ Issue Certificates/ Replace Expiring Certificates Form*** and send it to the RITS Help Desk. At the activation of the replacement certificate, the old certificate will be automatically revoked, and the new certificate will commence operation with the user's existing password. This provides a seamless changeover.

The expiry date of the certificate can be seen in **User Privileges** and by selecting the certificate in **Token Administration** and pressing the **Certificate Details** button.

Note that Password Administrators are able to view the complete list of users whose passwords are expiring in the next 90 days in the function *User Privileges*. Multiple users whose passwords are expiring within the next 90 days can be listed and attached to the same *Request to Revoke/ Issue Certificates/ Replace Expiring Certificates Form* to alleviate the need for multiple forms to be completed and sent to the RITS Help Desk. Note that replacement certificates are issued with a lifespan of 2 years.

A sample Expiry Email sent to the user and Password Administrator is shown below:

Subject: RITS Certificate Expiry

The RITS Certificate of Cameron Cook (cookc@abc.org.au) will expire on 12 October 2008 preventing access to the following RITS logon/s:

BANK2001, ABCD2004

To arrange for this user to be enrolled for a replacement RITS Certificate, the user should contact their Password/Certificate Administrator (the name of this person is found by viewing the first screen of User Privileges). Either the user or the Password/Certificate Administrator is required to send in, to the RITS Help Desk, a completed *Request to Revoke/ Issue Certificates/ Replace Expiring Certificates Form*. It is recommended that this be arranged immediately. The form is available on the RITS Information Facility and the RITS website http://www.rba.gov.au/rits/info/. Further information is available in chapter 9 of the *RITS Access and Security User Guide*.

Please note that a copy of this email has been sent to your Password/Certificate Administrators(s).

The following steps are required to complete the enrolment and activation process:

1. Enrolment
After receiving the form, the RITS Help Desk will send a Pre-enrolment email to the user which includes the Private Reference Code and link to enrol. The Help Desk will also telephone a Secret Password to the organisation's Password/Certificate Administrator, who must pass it to the user. At enrolment, the user must enter both the Private Reference Code and the Secret Password. The certificate must be collected within 7 days as the pre-enrolment will expire after this time.

2. Activate certificate in RITS
Upon successfully enrolling, and prior to logging on, the RITS Certificate must be activated in RITS. The user should go to the Token Administration screen, obtain the Certificate Activation Code and pass it to the Password/Certificate Administrator. At Activation, the old certificate will be automatically revoked and the new certificate will be ready for use.

3. Login to RITS
Once the user's certificate is activated, the user may login to RITS using their existing RITS logon and password.

4. Delete old certificate from token
After successfully logging in, the user should go to Token Administration link at the login screen and delete the old certificate and any Orphan Keys from the token.

Note for Password/Certificate Administrators

Password/Certificate Administrators are able to view the complete list of users whose passwords are expiring in the next 90 days in the function *User Privileges*. Multiple users whose passwords are expiring within the next 90 days can be listed and attached to the same *Request to Revoke/ Issue Certificates/ Replace Expiring Certificates Form* to alleviate the need for multiple forms to be completed and sent to the RITS Help Desk. Note that replacement certificates are issued with a lifespan of 2 years.

If you require further information, please contact the RITS help desk on 1800 659 360 or email rits@rba.gov.au.

Kind regards,

RITS Help Desk

9.3 Failure to Request Certificate Re-Issue Before Expiry

If the user fails to obtain a new certificate prior to the expiry date of the existing certificate, the user will not be able to access RITS until a replacement certificate is issued.

A user with an expired certificate must enrol for a new RITS digital certificate to access RITS again (see chapter 4 of this user guide for details). This process will take approximately 20 to 30 minutes.

Expired or revoked certificates will not be automatically removed from the RITS token. However, users may delete old certificates using the **RITS Token Administration** function.

10. CERTIFICATE REVOCATION

10.1 Key Points

- Certificates can be revoked prior to expiry by the Member's Password/Certificate Administrator or the RITS Help Desk.
- Revoking a user's certificate will immediately prevent that user from logging in to RITS, including after being timed out of the current RITS session. While logged in, but without a valid certificate, the user cannot perform action updates.
- Where a user's certificate is revoked (e.g. when the user has left the Member's employment), the user's status should also be changed to '*Inactive*'.
- Certificates that have not been collected or activated within 7 days of pre-enrolment will be revoked. The RITS Help Desk monitors certificate issuance and will revoke certificates that have not been activated in the time allowed.
- The revocation of a certificate and the issuance of a new certificate will take around 20 - 30 minutes.
- Refer the *Member Administration User Guide* for instructions on how to revoke certificates.

10.2 Revocation by a Member's Password/Certificate Administrator

A Member's Password/Certificate Administrator can revoke a user's certificate in **User Privileges**, using the **Revoke Certificate** tab.

After the certificate is revoked the user can no longer login to RITS. If the user is connected to a current RITS session when the certificate is revoked, the user will not be able to enter or update transactions, but enquiries will be possible. When the user's session is timed out, the user will not be able to login again.

See the *Member Administration User Guide* for details.

10.3 Revocation Scenarios

The following scenarios provide guidance in the handling of different situations.

10.3.1 Certificate has not been Collected or Activated within 7 days of Pre-Enrolment

If a certificate has not been collected or activated within 7 days of pre-enrolment it will be revoked by the RBA.

10.3.2 Temporarily Inactivating a User

If a user's status in RITS is changed to '*Inactive'*, the certificate is not automatically revoked. This provides flexibility as the user may again be made an *Active* user of RITS at a later time.

10.3.3 Various Scenarios Where the Certificate Must Be Revoked and Re-Issued for an Existing User

Under the following circumstances, the certificate must be revoked and a replacement certificate issued:

- the RITS token is lost;
- the RITS token is left at home and the user needs to access RITS;
- the Token Codeword has been shared;
- the certificate does not work;
- the RITS token is accidentally reformatted;
- the certificate has been accidentally deleted from the token; or
- the Token Codeword has been forgotten.

The revocation of a certificate and the issuance of a new certificate will take around 20 - 30 minutes.

10.3.4 User Resigns and is Replaced: Revoke Certificate and Request New User

If a user resigned from the position or moved elsewhere, and a new user is to take the position, the following steps must be taken. **Either**:

- the Password/Certificate Administrator revokes the certificate of the resigning user;
- the Password Administrator changes the status of the resigning user to '*Inactive*'; and
- the new user or the Password/Certificate Administrator sends in a completed *User Access Request Form* to the RITS Help Desk for the creation of a new user; **or**
- the user or the Password/Certificate Administrator requests the RITS Help Desk (using the *Request to Revoke/Issue Certificates/Replace Expiring Certificates Form*) to revoke the existing certificate and commence the process of obtaining a certificate for the new user (using the *User Access Request Form*).

10.3.5 Revoke Certificate and Remove an Existing User from RITS

When a RITS user is no longer required and will not be replaced by another person using the same RITS Username (e.g. BANK2001), the Password/Certificate Administrator should revoke the user's certificate in **User Privileges**. The RITS Help Desk can also revoke a user's certificate upon receiving the *Request to Revoke/Issue Certificates/Replace Expiring Certificates Form.* In this case the RITS Help Desk will remove the user's name.

Note that the Password/Certificate Administrator is not able to remove a user's name, the Password/Certificate Administrator can only make users *Inactive* or revoke users' certificates.

10.4 Revocation by the RITS Help Desk

The RITS Help Desk will revoke a user's certificate under the following circumstances:

- if requested to do so in a *Changes to an Existing User Form* received from a Member, duly signed by two Authorised RITS Signatories;
- if requested to do so in a *Request to Revoke/ Issue Certificates/ Replace Expiring Certificates Form* received from a Member, duly signed by two Authorised RITS Signatories;
- if a written request to revoke a user's certificate is received from a Member, duly signed by two Authorised RITS signatories
- if the RBA believes that the security arrangements for a user have been compromised or were attempted to be compromised, including the sharing of a Token Codeword; and
- if a certificate has not been collected or activated within 7 days of pre-enrolment.

The RBA can revoke certificates at its absolute discretion without a request from a Member or without any prior notice to the users or to the Member.

Requests over the telephone by a user will not be accepted. The RITS Help Desk will revoke a certificate as soon as practicable following receipt and verification of a revocation request. If a revocation request is received over a weekend or holiday, action on the request would occur at the next business day.