

RITS Training

Accessing RITS

Password Administration

Certificate Administration



Contents

- Accessing RITS
 - Setting up your PC
 - Network and internet access to RITS
 - Connectivity testing
- Security features
 - Logging on to RITS with digital certificates
 - Information about digital certificate technology
 - The rules applying to certificates
 - Session time-out



Contents

- Password and Certificate Administration
 - Responsibilities of the Password/Certificate Administrator(s)
 - RITS Forms
 - Obtaining a RITS digital certificate (step-by-step guide)
- Help and information
 - RITS Information Facility
 - The Help Desk
 - User guides and further information



Accessing RITS: Setting up your PC

- RITS software must be loaded onto your PC
- This software is available:
 - as a download from the RITS website at www.rba.gov.au/rits, and
 - on CD (available on request from the RITS Help Desk)
- A testcard is available to check the settings of your PC
- PCs must run Internet Explorer 6.0 or later
- Settings for IE and other minimum PC requirements are set out in the **Technical Information Paper** available from the RITS Information Facility



RITS Testcard

- All items must be ticked to run the RITS software

Machine Requirements			Token Requirements		
1) Explorer	<p>For the RITS application you are required to use Microsoft Internet Explorer version 6.0 or later. You are running IE version 6.0.</p> <p>You have met this requirement.</p>	✓	7) Token DLL Version	<p>You are required to have Token DLL version 2.0 installed.</p> <p>Installed Version: 2.0</p>	✓
2) Javascript	<p>You are required to have a javascript version later than 1.1. Your javascript version is 1.3.</p> <p>You have met this requirement.</p>	✓	8) iKey Driver Version	<p>You are required to have IKey Driver version dkck201 installed.</p> <p>Installed Version: dkck201.dll</p>	✓
3) Screen Resolution	<p>You are required to have a screen resolution of at least 1024 by 768.</p> <p>Screen Height is:1024 Screen Width is:1280</p> <p>You have met this requirement.</p>	✓	9) Check Token Label	<p>Token Label should be RITS Token</p> <p>Token Label: RITS Token</p>	✓
4) Applet	<p>Applets are working in your browser.</p>	✓	10) Check Certificate Validity	<p>Checking for valid certificate attributes...</p> <p>Certificate Validity Results:</p> <p>Cert Name: DANIELLE LAU, laud@rba.gov.au, ABN 50008559486</p> <ul style="list-style-type: none">• Is issued by a RITS CA• Is valid until [Thu Jun 26 09:59:59 EST 2008]• This certificate is valid for RITS.	✓
5) JRE Version	<p>You are required to have JRE 1.4.2_10 or later You have JRE version 1.4.2_10 from Sun Microsystems Inc.</p> <p>You have met this requirement.</p>	✓	11) Test Token Signing	<p>Logging in and performing test signing of token...</p> <p>Test signing was successful.</p>	✓
6) Applet To Javascript	<p>Applet to Javascript calls are enabled.</p>	✓			



Accessing RITS: Network and Internet Access

- The Austraclear network (ANNI) will continue to be the primary connection to RITS for larger Members
- Smaller institutions will access via the Internet
- ANNI has been upgraded by the ASX to provide increased capacity
- Internet access is direct to the RBA (RITS), not via the ASX
- Internet access includes DR options




Accessing RITS: Connectivity testing

- Members will need to establish and prove connectivity to RITS
- Connectivity testing ensures that network and firewall settings are correct
- The RITS Help Desk can assist Members with the connectivity testing



Security features: Digital Certificates

- RITS uses digital certificate technology to strengthen security surrounding RITS
- Each user must have their own Rainbow iKey security token. Supplies are available from the RITS Help Desk 
- The RITS digital certificate is downloaded onto a token
- A Token Codeword must be set and maintained by the user
- Each RITS transaction is digitally signed and can be traced back to the Member and user
- The certificate (and token) must be used to access and use RITS, in addition to the traditional user login and password



Security features: How to logon to RITS with token/digital certificates

- Firstly, insert the token into a USB port on your PC
- Select the RITS icon on the desktop (or link) to access the RITS login screen




- In the logon screen enter your user name (4-letter Member mnemonic and user's own logon name) and your RITS password
- In the next screen select your digital certificate and enter the Token Codeword



RITS Launch Page

RITS - Windows Internet Explorer provided by Reserve Bank of Australia



RITS

Reserve Bank Information & Transfer System

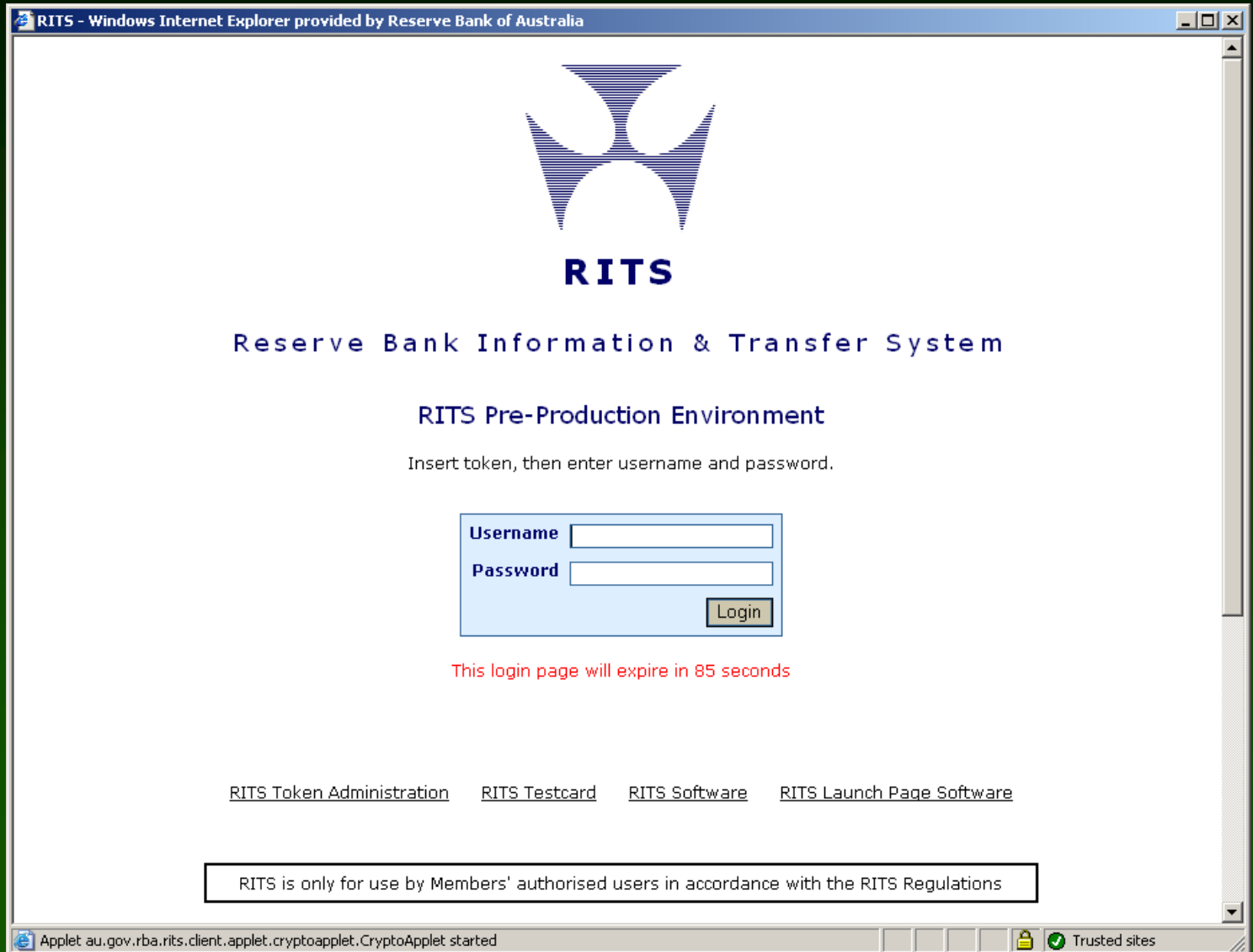
RITS Help Desk	Tel: 1800 659 360* Fax: 02 9551 8063 Email: rits@rba.gov.au
Settlements with RBA	Tel: 02 9551 8912* Tel: 02 9551 8916*

* All calls to and from the RITS Help Desk and Settlements telephones are recorded.
** Internet connection required for Information & Setup (www.rba.gov.au/rits)

[RITS](#) [RITS Pre-Production](#) [Information & Setup**](#) [Options](#)

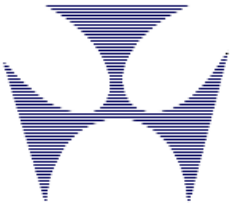


RITS Log-in Page



The screenshot shows a web browser window titled "RITS - Windows Internet Explorer provided by Reserve Bank of Australia". The page features the RITS logo, which is a stylized blue and white emblem. Below the logo, the text "RITS" is displayed in a bold, blue font. Underneath, the full name "Reserve Bank Information & Transfer System" is written in a smaller blue font. The page is identified as the "RITS Pre-Production Environment". A instruction reads: "Insert token, then enter username and password." Below this is a login form with two input fields: "Username" and "Password", and a "Login" button. A red warning message states: "This login page will expire in 85 seconds". At the bottom of the page, there are four links: "RITS Token Administration", "RITS Testcard", "RITS Software", and "RITS Launch Page Software". A footer box contains the text: "RITS is only for use by Members' authorised users in accordance with the RITS Regulations". The browser's status bar at the bottom shows the address "Applet au.gov.rba.rits.client.applet.cryptoapplet.CryptoApplet started" and a "Trusted sites" icon.

RITS - Windows Internet Explorer provided by Reserve Bank of Australia



RITS

Reserve Bank Information & Transfer System

RITS Pre-Production Environment

Insert token, then enter username and password.

Username

Password

Login

This login page will expire in 85 seconds

[RITS Token Administration](#) [RITS Testcard](#) [RITS Software](#) [RITS Launch Page Software](#)

RITS is only for use by Members' authorised users in accordance with the RITS Regulations

Applet au.gov.rba.rits.client.applet.cryptoapplet.CryptoApplet started Trusted sites



RITS Certificate Selection Page

Choose RITS Certificate

ACHO2020 ACHO2020 - RBA
ACHO2023 ACHO2023 - RBA
BQLQ2E02 BQLQ2E02 - BQLQ 0900 TEST
BQLQ2E30 BQLQ2E30 - BQLQ 0900 TEST
ROYC2E02 ROYC2E02 - ROYAL BANK OF CANADA
ROYC2E57 ROYC2E57 - ROYAL BANK OF CANADA

Issued To	BQLQ2E02 BQLQ2E02, zornb@rba.gov.au, ABN 32009656740
Issued By	Reserve Bank of Australia, RITS CA, For User Acceptance Testing
Valid From	Fri Feb 22 11:00:00 EST 2008
Valid Until	Fri Dec 04 10:59:59 EST 2009
Serial Number	6fb3feb7e2e139918e315b54143bd4c1

Token Codeword :

Tab or Shift-Tab can be used to move around the screen

Java Applet Window



Security features: Rules applying to certificates

- All users must have their own token and RITS digital certificate
- The RITS certificate must be in the user's name (and user logons in RITS e.g. BANK2E01, must also be in the name of the user)
- Users must not share tokens or the Token Codeword
- Each user can only have one logon per Member
- Users who operate in RITS for two related RITS Members need a logon and certificate for each Member (the certificates can be on the same token)
- The same certificate is used for access to RITS Production (live RITS) and RITS Pre-Production



Security features: Session time-out

- After 15 minutes (default setting) of inactivity during a login session, the user is automatically logged out of RITS
- Password Administrator may extend this to 30 or 60 minutes for selected users in **User Privileges**
- Extended settings may impact system performance and security, only selected users should be allocated with extended session time-outs



Responsibilities of the Password/ Certificate Administrators Overview:

- The Password/Certificate Administrator manages the certificates of the users
- Members must assign the responsibilities of 'Password Administrator' and 'Certificate Administrator' to some of its staff.
- The same staff can be responsible for both, or the responsibilities can be separated, for stronger security.



Responsibilities of the Password/ Certificate Administrators Overview:

- The Password Administrator is responsible for:
 - resetting passwords
 - controlling the status of each user
 - the allocation of roles/ functions to users
 - specifying the functions that a user may authorise
 - linking users to branches to perform transactions for those branches
 - assigning the privileges to authorise
 - setting an extended session time-out (if required)



Responsibilities of the Password/ Certificate Administrators Overview:

- The Certificate Administrator is responsible for:
 - activating each user's certificate after they enrol
 - revoking a user's certificate; eg, if they leave the company
- All users have a view-only version of their profiles and privileges



Password Administrator Responsibilities: Resetting RITS Passwords

- A Password Administrator can set a new password for a user in the function **Password Administration**
- This might be required if the user has forgotten the password
- A user that has made 3 failed attempts to log on will be made **inactive**. To re-activate the user, the Password Administrator must:
 - go to the function **User Privileges** and reset the user's status to Active, and
 - set a new password in **Password Administration**



Password Administration screen





RITS - Windows Internet Explorer provided by Reserve Bank of Australia

Reserve Bank Information & Transfer System RBA RTGS Test Environment

09 May 2008 16:28:52 **User** BQLQ2E30 BQLQ2E30, BQLQ2E30 **Member** BQLQ

Current Sessions DAY SWIFTDAY **Sessions Close** DAY 16:30 SCS 17:15 EVE 18:30 REPORTS 19:00
SWIFTDAY 16:30 SWIFFINAL 18:05

Outstanding Auths and Messages
1 Cash Transfer Authorisation(s)
0 General Authorisation(s)
0 Message(s)

RITS Messages RITST-RA    **Logout** 

Main

- ESA Management
 - ESA Position
 - Settled Payments
 - Transaction Enquiry
 - SWIFT Enquiry
 - AIF Enquiry
 - 7:30am Information
- ESA/Credit
 - Queue Mgt
 - Override Status
- Cash Account
 - Queue Mgt
 - Override Status
 - Limit
 - Sub-Limit
 - Enquiry
- Cash Transfers
- Batches
- Batch Admin
- Member Admin
 - Auth by Function
 - Change Password
 - Evening Agreement
 - Password Admin**
 - Roles
 - Unsolicited Advices
 - User Privileges

Password Administration

Select a user BQLQ2E01 BQLQ2E01 UAT MEREDITH MORSE

New Password

Confirm New Password

Rules for RITS Passwords

- Minimum 8 character password. There must be at least one non-alphabetical character included.
- There must be at least one alphabet character included
- Passwords are case sensitive.



Password Administrator Responsibilities: Managing a user's status

The Password Administrator can control a user's access to RITS by changing the user's status in **User Privileges**

- **Active** – Access is available, with a valid certificate.
- **Inactive** – The user may not log on. The user can be re-activated.
- **Inactive/Revoke Certificate** – The certificate is automatically revoked and the user record is removed from RITS. There is no going back.



Password Administrator Responsibilities: Establishing user/branch links

- To conduct transactions for a branch, a user must be first linked to it, eg, WPAC2E, in the function **User Privileges**
- Once linked, a user may:
 - enter, amend, delete, authorise and enquire upon Cash Transfers
 - manage queued transactions at the Cash Account level
 - set an override Cash Account Status
 - set a Cash Account Sub-Limit
 - participate in batches, or be the Batch Administrator, in the RITS batch facility



Password Administrator Responsibilities: Allocating Functions via Roles

- Roles are allocated to users in **User Privileges**, and provide users with the functionality required to operate in RITS
- Newly allocated roles, and roles removed from the user, take effect after the user's next logon to RITS



Password Administrator Responsibilities: Suggested Role Allocations

- It is mandatory that every user has the role called **All Users**. This provides basic functions and access to the menu
- Roles for ESA and liquidity managers
 - Member Enquiries
 - ESA Status Queue Management
 - Override ESA Status – Set Override and
 - ESA Sub-Limit – Set Sub-Limit
- Roles for credit managers
 - Member Enquiries
 - Credit Status Queue Management
 - Override Credit Status – Set Override
 - Cash Account Limit – Set Limit
- Roles for Settlements Authorisers
 - Authoriser
 - Authorise Cash Transfer Entry
 - Member Enquiries



Password Administrator Responsibilities: Suggested Role Allocations

- Roles for settlements staff (not authorising)
 - Cash Transfer Entry
 - Batch Entry (if applicable)
 - Member Enquiries
- Password Administrator role
 - **Password Administrator**
 - and **Activation Code Entry** and **Revoke Certificate** if the user is also a Certificate Administrator
- Certificate Administrator role
 - **Activation Code Entry**
 - **Revoke Certificate**
 - and possibly the **Password Administrator** role
- 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

Password Administrator Responsibilities: Allocating Authorisation Privileges

- To set a user up to authorise Cash Transfers simply allocate the role **Authorise Cash Transfer Entry**.
- For all other authorisations two steps are required
 - Firstly, allocate the role – **Authoriser**.
 - Then, under **User Privileges**, go to the **User Details** screen (by selecting the user), click the **Authorisations** button. Tick the functions to be authorised and Submit.



Password Administrator Responsibilities: Verifying Authorisation Levels

- If a Member requires a function to be authorised, ie, one person to enter, and another to authorise, the RITS Help Desk must be notified
- It is the responsibility of Password Administrators to ensure that authorisation settings have been correctly entered
- To verify, view the function **Authorisations by Function**
- Authorisations on functions can be added or removed by completing the **Member Authorisation Maintenance Form** (available from the Info Facility) and sending it to the RITS Help Desk



Certificate Administrator Responsibilities: Activation Code Entry

- It is the responsibility of the Certificate Administrator to activate a user's RITS digital certificate
- A newly enrolled user must provide the new certificate's 'Activation Code' to the Certificate Administrator for entry in **User Privileges**
- Certificate Administrators should only activate staff authorised to access RITS
- Access to RITS is not available to a user until they are activated



Certificate Administrator Responsibilities: Revoke Certificate

- A Certificate Administrator is responsible for revoking a user's RITS digital certificate
- The facility to revoke a user is found in **User Privileges**, under the **Certificate Administration** button
- Some example circumstances for revoking a certificate
 - User's token has been lost
 - User's token left at home
 - The Token Codeword has been forgotten, or token is locked out
 - The user has moved from the job
 - The Token Codeword has been shared
- Where access to the token is unavailable, and the user still requires access to RITS, the user's certificate must be revoked prior to a new certificate being applied for



User/Member Request Forms

To set up or change access to RITS, the following forms must be used.

- User Access Request (multiple) Form
 - Create a new user/ new users
 - Pre-enrol a user/ users for a RITS digital certificate(s)
 - Obtain supplies of RITS tokens
- Member Authorisations Maintenance Form
 - Add or remove authorisations on functions
- Request to Revoke/ Issue Cert/ Replace Expiring Certificates Form
 - Issue a replacement certificate in anticipation of expiry of the old certificate
 - Revoke a certificate
 - Issue a replacement/ new certificate



User/Member Request Forms

- The following form may be used to request the RITS Help Desk to make urgent changes when the Password/ Certificate Administrators are not available.
- Changes to an Existing User Form
 - Change user status/ links to branches/ roles
 - Change user authorisation functions
 - Activate a RITS digital certificate
 - Reset RITS password
- All forms must be duly signed by two RITS Authorised Signatories
- Send the signed forms to the RITS Help Desk



Obtaining a RITS digital certificate

1. The Member must provide a signed User Access Request Form to the RITS Help Desk
2. The Password/ Certificate Administrator will provide a token to the user
3. The user must **format the token** and **set a Token Codeword**, known only to him/herself
4. The RITS Help Desk pre-enrols the user for a RITS digital certificate and provides the two secret codes to the user: one by email, and the other via telephone to the Password Administrator, who passes it to the user
5. RITS emails the user with instructions and a link to enrol
6. The user inserts the formatted token in the USB port of the PC and clicks the **enrol for a RITS certificate link** in the email



Obtaining a RITS digital certificate

7. The user enrolls by entering their details and the two secret codes. The RITS certificate is loaded onto the iKey token
8. Using the link on the 'enrolment success!' screen, the user goes to Token Administration, finds the certificate 'Activation Code' and passes it to the Certificate Administrator
9. The Certificate Administrator activates the certificate by entering the Activation Code in **User Privileges**
10. At login, the user must enter their username and password (which is the **secret password** passed to the user by the Password Administrator), select the RITS certificate and enter the Token Codeword; the user is prompted to change the password immediately.



Help: The RITS Information Facility

- The “RITS Information Facility” includes information for RITS users that may be read on-line, printed or downloaded:
 - technical requirements for connecting to RITS
 - user guides and training presentations
 - a wide range of other information about RITS
 - User Access Request Forms used to enrol for a RITS certificate (+ other forms for user/Member set-up)



The Role of the RITS Help Desk

- The RITS Help Desk is available while RITS is open to:
 - assist Members with any queries about RITS
 - monitor liquidity
 - deal with requests for session extensions
- The RITS Help Desk will accept duly authorised written requests to:
 - create and pre-enrol users, and supply tokens
 - set up and change Member details, branches, and assign cash accounts to branches
 - place authorisations on functions



Relevant Guides

The following guides in the RITS Information Facility provide information on the topics raised in this presentation:

- *RITS Access and Security* – covers logging on and password management, token management, enrolling for a digital certificate and certificate management
- *Overview of Functionality* – Chapter 15 (Password, Certificate and User Administration), and 16 (Roles and Functions)
- *Member Administration User Guide* – covers the functions User Privileges, Password Admin and Change Password.



Relevant Guides

- *Authorisations User Guide* - covers the function Authorisation by Function
- *Technical Information Paper* – minimum technical requirements for PCs and establishing connectivity
- *Guide to Connectivity Testing* – describes the process of loading the RITS software and testing connectivity

